ISSN: 2587-1218

CYBERPOLITIKJOURNAL
Siber Politikalar Dergisi

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

Winter 2024 -Vol. 9 No. 18

ISSN: 2587-1218

CYBERPOLITIK JOURNAL
Siber Politikalar Dergisi

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

www.cyberpolitikjournal.org

Winter 2024

ISSN: 2587-1218

ABOUT THE JOURNAL

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

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

The Journal
The languages of the Journal are both Turkish and English.

ISSN 2587-1218
Cyberpolitik (CP) aims to publish peer-reviewed scholarly articles and reviews as well as significant developments regarding cyber world, cybersecurity, cyberpolitics and human rights.

Indexing/Endeksler

Cyberpolitik Journal is being indexed by;

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

ISSN: 2587-1218

Issue Referees / Sayı Hakemleri

Prof.Dr. Bilal Sambur

Assoc. Prof.Dr. Mehmet Emin Erendor

Assoc. Prof.Dr. Murat Tümay

Assoc. Prof.Dr. Yusuf Çınar

Assoc. Prof.Dr. Önder A. Afşar

Assistant Prof.Dr. Ayşegül Sili Kalem

Assistant Prof.Dr. Şerife nesimioğlu

Dr. Gül nazik Ünver

Cyberpolitik consists of the following sections:

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

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

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

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

ISSN: 2587-1218

CONTENTS / İÇİNDEKİLER

ISSN: 2587-1218

EDITORIAL PREFACE: REWISITING CYBERSECURITY

Dear Readers,

We are delighted to present the 18th issue of the *Cyberpolitik Journal*, marking another milestone in our ongoing journey, which began nearly a decade ago. It is a privilege for us to continue to explore the complexities and nuances of the digital world, a domain that grows exponentially with each passing day. As new technologies emerge and the digital landscape evolves, we remain committed to examining and understanding these developments within our limitations, seeking insights that help us navigate this ever-expanding sphere.♣

In an era where digital technologies are seamlessly integrated into every facet of our lives, cybersecurity has become a paramount concern. The rapid pace of innovation in cyberspace has brought about unprecedented opportunities, but it has also introduced new vulnerabilities that require urgent attention. As our reliance on interconnected systems deepens, the risks of cyberattacks and data breaches have escalated, posing significant threats not only to individuals but also to organizations, governments, and entire nations. The importance of revisiting and rethinking cybersecurity practices has never been more urgent, as the evolving threat landscape demands that we continuously adapt to new challenges and technologies.

The complexity of modern cyber threats calls for a multifaceted approach to cybersecurity, one that not only addresses technical solutions but also incorporates ethical, legal, and policy considerations. In this issue of the *Cyberpolitik Journal*, we explore the intersection of cybersecurity and artificial intelligence, highlighting how emerging technologies can both enhance and undermine digital defenses. The contributions reflect the growing need for global collaboration and the creation of robust frameworks that promote security while safeguarding privacy and civil liberties. It is clear that cybersecurity is no longer solely a technical issue but one that requires cooperation across disciplines and borders to ensure the safety and resilience of digital infrastructures.

♣ This editorial preface is modtly generated by AI

As digital threats continue to evolve, so too must our strategies for defending against them. This issue underscores the critical importance of reimagining cybersecurity in a rapidly changing world. From nation-state actors engaging in cyber warfare to the increasing sophistication of ransomware attacks, the articles featured here delve into the strategic, ethical, and policy challenges posed by the digital age. By revisiting cybersecurity with a focus on innovation, responsibility, and international cooperation, we can build a more secure and resilient digital future.

This issue brings forth a collection of thought-provoking articles that illuminate various dimensions of the cyber world. From the theory of IR to cyber sovereignty, from cybersecurity to security strategis and from cybersecurity regulations in Malaysia to cyber attacks on Hesbollah's pager explosions.

This issue of *Cyberpolitik Journal* features an engaging array of research articles, opinions, and interviews that address the most pressing and thought-provoking topics in the digital realm. As the digital landscape evolves at a rapid pace, it is essential to critically evaluate the ethical implications of these changes, and our contributors have done so with insight and rigor.

One of the key themes explored in this issue is the intersection of cyberspace and geopolitical conflict. In the article *"Cyberpolitical Spaces in the Contested Narrative of PHL-China Maritime Dispute"*, Santos examine how digital technologies influence international relations and territorial disputes, specifically focusing on the South China Sea. The research highlights the complex relationship between cyberspace and sovereignty, illustrating the growing importance of digital platforms in shaping global political narratives.

In *"What Kind of Theory of International Relations in the Context of Cyberspace?"*, Kurnaz delves into the evolving field of international relations, proposing a new framework for understanding how digital spaces interact with traditional statecraft. This theoretical exploration offers critical insights into how cyberspace is altering power dynamics, diplomacy, and state sovereignty in the modern world.

The article *"Cyberspace and Nation-State: Revisiting Sovereignty"* extends this conversation by revisiting the concept of sovereignty in the digital age. The piece provides a nuanced analysis

of how nation-states navigate the complexities of governing both physical territories and the expansive digital landscapes that transcend borders. Söker in the article challenges traditional conceptions of state control and opens up important discussions about the future of governance in cyberspace.

As digital technologies continue to shape the security landscape, *"AI and Cybersecurity: Navigating the Future of Warfare and Digital Defense"* examines the critical role artificial intelligence plays in modern warfare and digital defense strategies. Karaguezian tries to explore both the opportunities and risks that AI presents to cybersecurity, emphasizing the need for robust ethical frameworks to guide the development and deployment of AI in defense systems.

In *"Digital Diplomacy: The TRNC's Struggle for Recognition in Cyberspace"*, Safa analyzes the role of cyberspace in the diplomatic struggle of the Turkish Republic of Northern Cyprus (TRNC) for international recognition. This research highlights the significance of digital platforms in advancing or hindering diplomatic efforts and underscores the challenges smaller or unrecognized states face in the digital realm.

The article in Turkish, *"Yapay Sinir Ağları ile Güçlenen Güvenlik Stratejileri: Modern Güvenlik Yönetiminde Yapay Zekânın Rolü ve Etkileri"*, provides an in-depth exploration of how artificial neural networks enhance security strategies in modern security management. This work contributes valuable insights into the practical applications of AI in protecting critical infrastructure and mitigating cyber threats.

In the *Opinions* section, *"Cyber Security Act 2024: A Facelift to the Cybersecurity in Malaysia"* offers an overview of recent legislative changes in Malaysia aimed at improving national cybersecurity. The article assesses the strengths and potential shortcomings of the new Cyber Security Act, shedding light on the importance of legislative frameworks in protecting digital infrastructures.

The discussion on *"Sosyal Medya Ekseninde İfade Özgürlüğü"* (Freedom of Expression in the Context of Social Media) explores the complex relationship between freedom of speech and the regulation of content on social media platforms. It addresses the ethical dilemmas surrounding censorship, misinformation, and the role of governments and corporations in moderating online speech.

ISSN: 2587-1218

Our *Article and Book Reviews* section features thoughtful reflections on *Diplomacy in the Digital Age*, which examines how diplomacy has evolved in the face of digital communication technologies and the challenges they pose to traditional diplomatic practices.

Lastly, in the *Academic Interviews* section, *"Siber Saldırılar Asimetrik Savaşın Bir Parçasıdır"* (Cyber Attacks are a Part of Asymmetric Warfare) explores the growing threat of cyber warfare in modern conflicts. This interview provides insight into the strategic use of cyberattacks by state and non-state actors, highlighting the ways in which these new forms of conflict challenge traditional military paradigms.

As we continue to face unprecedented ethical and practical challenges in cyberspace, these articles offer critical perspectives that will aid policymakers, scholars, and practitioners in making informed decisions. The diverse range of topics explored in this issue underscores the importance of interdisciplinary approaches to understanding the ethical implications of digital technologies. We hope this collection of research will spark further dialogue, reflection, and innovation in navigating the evolving digital landscape with integrity and responsibility.

Nezir AKYEŞİLMEN, Ph.D

Editor-in-Chief

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ

CYBERPOLITICAL SPACES IN THE CONTESTED NARRATIVE OF PHL-CHINA MARITIME DISPUTE

Danilo Lorenzo S. Delos SANTOS[*]

Orcid: 0009-0009-4604-1602

Abstract

The ongoing dispute in the West Philippine Sea has proven to be one of the critical geopolitical areas of concern in recent years. After decades of brewing tensions, the two nations have been in a constant war of interest and clout through various forms of media and targeted audiences to garner support and influence in the region and beyond. Over the decades, the game has shifted both ways with the Philippines winning its arbitration case against China under the UNCLOS (United Nations Convention on the Law of the Sea) in 2016 and the eventual and unforeseen policy shift under a pro-China Duterte administration. This paper explores the narrative of the ongoing tensions by comparing the cyberpolitical spaces using Lateral Pressure Theory in discussing how the administration of Rodrigo Duterte shaped, framed, and transformed public opinion and policy within the trajectories of geospatial, environmental, and cyberspace domains.

Key Words: West Philippine Sea, China- Philippines relations, Cyperpolitics, Lateral Pressure Theory

Introduction

The contested waters of the West Philippine Sea or what is also known as the South China Sea has been a hotly debated topic in the last decade. The tensions between the Philippines and China have been escalating for the last two years (Center for Preventive Action, 2024) with various physical altercations with the Chinese Coast Guard as well as the maritime militia (Davidson, 2024) with their cabbage patch strategy (Heydarian, 2019

[*] PhD Student at International Relations at University of Pecs, Pecs-Hungary

The current context of the conflict begs to transpose a question of the current milieu into popular discourse regarding the spillovers of state tensions from the geospatial and environmental domains towards cyberspace that is unbound by physical boundaries and arbitrary rules of conduct. With the nature of cyberspace, the weaponisation of influence is used by state actors as a viable tool to project legitimisation of promoted values and ideas.

International tensions in the West Philippine Sea highlights this spillover that are unforeseen before in major international conflicts. Other than the ongoing one-upmanship between China's coast guard and the Philippine's stand, cyberspace has been a realm in which the Philippines have used to project its domestic policy into a transnational plane. The paper aims to answer the question of how do state actors express national interest through various projections of power and influence in the realm of cyberspace. Also, the exploration of the topic will use the regime under Duterte and how the government cascades national interest in geospatial and environmental nexus through cyberpolitical means as a basis of comparison and using the current tensions of the west Philippine Sea as a case test for the Lateral Pressure Theory.

Overarching Question: "How did the Duterte administration control the narrative of the West Philippine Sea tension within his administration?

Sub-questions:

1. What are the issues framing used by the Duterte administration in advancing the government's agenda across the three domains of cyberspace, geospatial, and environmental nodes?
2. What are the critical narrative nuances created under his administration and how did it impact public opinion?
3. How can the Philippine government promote the national agenda through the lens of Lateral Pressure Theory in the case of the West Philippine Sea tensions?
4.

Literature Review

Lateral Pressure Theory in Retrospect

The advancement of technology has created new landscapes and dynamics of power interaction between actors in international relations. International Relations theorizing has been lagging behind in making sense of the undercurrents surrounding the utilization of technology in the advancement of State agenda and national interest (Foulton & Meibauer, 2024). While the study

of the impact of cyberspace has been a rich field of interest, studies that decrypt and explain the intersection of emerging geopolitics of cyberspace seen in various platforms and mediums.

Lateral Pressure Theory has experienced a resurgence in the literature notably in 2012 as the seminal work on cyberpolitics and the study of international relations was published. Fundamentally, it establishes the relationship between state characteristics and patterns of behaviour in the international level as well as the root and effect of the action in the larger scheme of international relations (Choucri and North, 1989). The looming challenge for International Relations practitioners is to make meaning for the seemingly complex nature of conceptual and definitional basis (Akdağ, 2023). This compounds to the reality that cyber policy and government policies aims to aid its main aim to protect threats from the spread of false information and narratives (Tarhan, 2023).

Focusing commonly on the external effects of state action and its transformative properties outside state territory, it is the initial step in understanding the dynamics of state politics in an outward exogenous direction similar to the economic expansion of Simon Kuznets (Lundberg, 1971). State to state interaction through this understanding is borne from the intersection of interests resulting in engagements that could lead to either cooperation or conflict.

Combining Lateral Pressure Theory and the politics of cyberspace highlights the asymmetric and borderless nature of conflict and warfare with the absence of international law causing a vacuum in cyberspace (Schmitt, 2017). This also is despite past efforts such as the Tallinn Manual that had not resolved the issue (Schmitt, 2013). Due to the lack of a stable international law, states through various non-military means can directly affect another nation-state without accountability due to the lack of legal frame enabling punitive measures to violators.

The complexity surrounding cyberspace is rooted on the seven unique characteristics that it has such as temporality; or the ability to enter high politics, physicality; which is how cyberspace transcends physical limits, permeation; corresponding to its fluidity such as the trait to sustain changes and reconfigurations, participation; that reduces barriers to political expression, attribution; which obscures identity and lastly, accountability; that bypasses existing mechanisms (Choucri, 2012).

As one of the primary theories in explaining the effect of cyberspace to state power and global affairs, Lateral Pressure Theory places itself as the best alternative to assess the current tensions not only seen in tangible physical altercations but what has now translated to online one-upmanship that is discreet, clandestine, and manipulative while at the same time being ubiquitous, unrelenting, and constantly threatening. Illustrating this threat, Choucri advances the theory by anchoring the domains in three categories notably the more traditional geospatial,

the newly surging environmental, and lastly the newest which is the cyberspace spheres (Choucri, 2017).

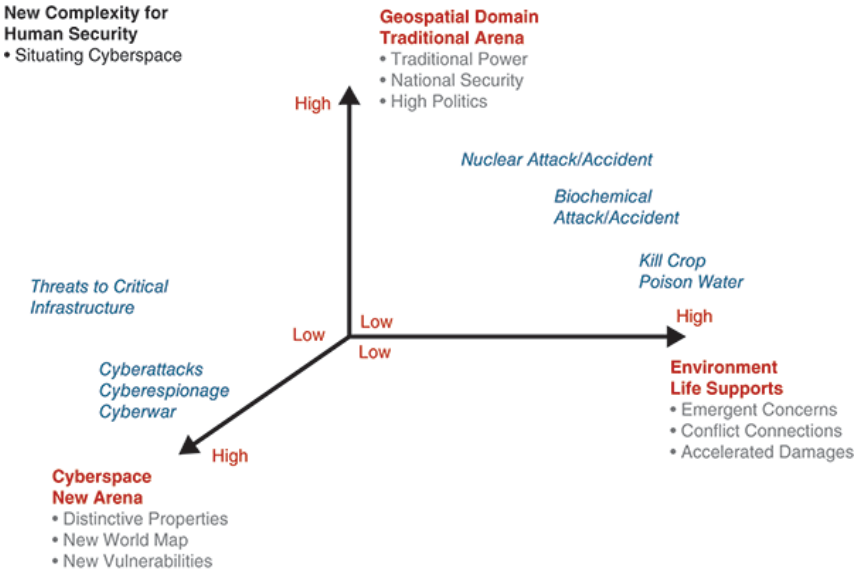


Figure 1: New complexity for human security

Source: Choucri & Agrawal (2017)

Choucri's fundamentals of sustainability & security highlights the anchors of international relations geopolitical space through the three domains that while are static, are considered to be the initial steps for theoretical development in relation to the dynamic change of state affairs and trajectories of interaction. On the other hand, it is also accepted by the proponents that global priorities are also headed towards reversing the arrows into lowering the risks in the premise of co-evolution of international relations and cyberspace. However, the perceived reversal of the arrows is assumed to be a net positive effect and needs further understanding in its application such as with the West Philippine Sea.

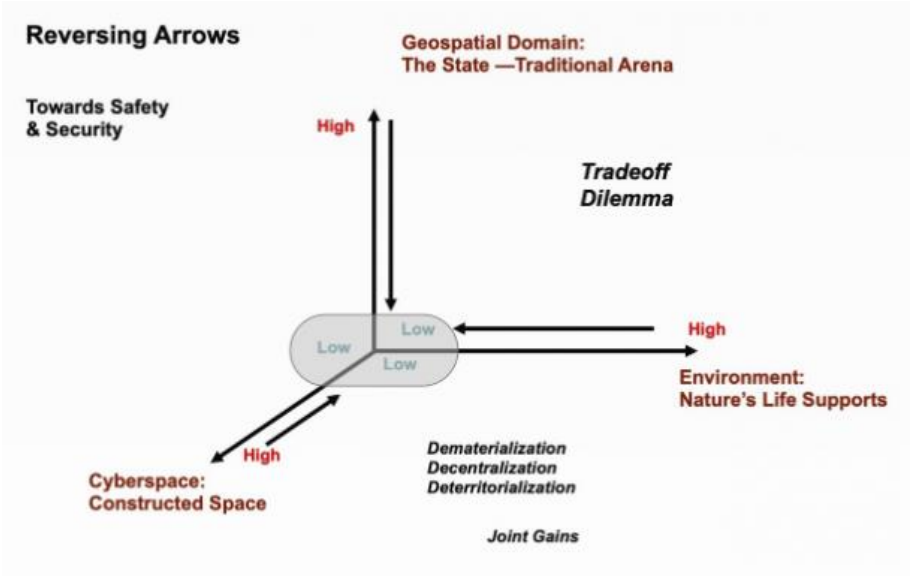


Figure 2: Reversing arrows for human security

Source: Choucri & Clark (2019)

The study advances the literature by using the theoretical lens in understanding the dynamics of lateral pressure across and between the other adjacent domains as well as the domestic effects of lateral pressure to the subjects of the government.

The research intends to test the theory on how cyberspace has been a critical tool for a state to both project national interest and at the same time influence domestic discourse with its framing and issue nuancing to similar result by pivoting external interest and reintroducing it to public discourse.

It posits Choucri's fundamental framing of state profiles that are defined by real and cyber personas necessitating for the development of systems to unlock the paradox if real profiles echo what is seen in cyberspace or as depicted in this study as the issue nuancing that are shown in the government owned and controlled media outlet Philippine News Agency (PNA).

Under the Duterte administration, the government has utilized its primary media resources that spans TV, Radio, Newspapers, and Cyberspace. This paper explores the cyberpolitical realm, and specifically the contents within the Philippine News agency website which is the primary source of government news and information and analyses three major cyberpolitical spaces of geospatial, environmental, and cyberspace domains in Lateral Pressure Theory.

Aquino's Arbitral Win to Duterte's China Pivot

During the early years of the Aquino administration, China has positioned itself as the aggressor in the South China Sea with Chinese Navy vessels seen with building activities in the West Philippine Sea (Lee-Brago, 2011) which was the precursor to various summons and questioning

for the Philippine government over China's ominous presence around the Philippine maritime territory in various incidents and levels of severity (Yann-huei & Zou, 2014). Midway in his leadership on 2012, Aquino sings a new order to rename the South China Sea waters within the Philippine Territory to the West Philippine Sea in a move to establish territorial claims in the islands under considerable threat (South China Sea Morning Post, 2012). These, among many symbolic acts and strategies were a constant item in news outlets during Aquino's tenure and were of considerable importance to the buildup leading to the Philippine's breakthrough in the West Philippine Sea. Aquino's statecraft was tested in the early years of his tenure where the Philippine government was active in accumulating popular support in the region. Mainly Aquino achieved this feat by using both state and non-state actors and track two diplomatic channels (Ibarra, 2024).

It was in 2016 under Aquino's final year of leadership when the Philippines experienced a landmark win in the West Philippine Sea row with an arbitration win concerning the historical rights and claims of China in the disputed islands (Permanent Court of Arbitration, no). The Permanent Court of Arbitration has ruled in favour of the Philippines after three years of initially lodging the proceedings under Annex VII of the United Nations Convention on the Law of the Sea (UNCLOS).

While this decision sets the foundations of the Philippines primary claim, the Aquino administration was able to effectively use existing diplomatic tools and avenues to draw attention to the growing tensions and amass support from its regional neighbours not only in the ASEAN (Ramos, 2018) but also in Asia and the Quadrilateral Security Dialogue (QUAD) through the use of hard balancing strategy using military modernization, alliance building, and the reliance on international law (De Castro, 2024).

During the succeeding 2016 National Elections, it was evident that Aquino's efforts has trickled down to the populace as evidenced with the increased preference of voters towards a leader who will protect the Philippine territory against aggressors as seen in the final pre-election poll regarding the concerns of voters and their preferences on which issues to address (Pulse Asia, 2016).

Comparatively, domestic concerns predominantly were the most urgent worries of the public with local governance issues, social services, and economic balancing were cited. Local security also placed higher in the list with corruption, law enforcement, and illegal gambling all coalesce together under the umbrella of domestic peace and security. Outside threats such as territorial security, overseas worker welfare and climate change preparedness ranked the tail end of the important issues that the public wanted to address after Aquino's tenure. Notably,

8% of the respondents have placed a premium on territorial integrity on the public survey by Pulse Asia running up to the elections.

MOST URGENT NATIONAL CONCERNS FOR A PRESIDENTIAL CANDIDATE TO ADDRESS: OVERALL
January 24 - 28, 2016 / Philippines
(Multiple Response, up to 3 allowed / In Percent)

Base: Registered voters with biometrics

NATIONAL CONCERNS	RP	LOCATION				CLASS		
		NCR	BL	VIS	MIN	ABC	D	E
Improving/Increasing the pay of workers	38	36	35	47	38	27	39	39
Curbing the widespread sale and use of illegal drugs	36	42	32	34	41	34	37	30
Controlling inflation	30	28	32	31	29	28	31	30
Fighting graft and corruption in government	30	26	31	26	34	37	31	24
Reducing poverty of many Filipinos	29	34	31	26	24	25	29	31
Creating more jobs	26	34	28	27	16	23	25	30
Fighting criminality	24	22	23	23	30	33	24	23
Enforcing the law on all whether influential or ordinary people	20	17	21	18	22	19	20	19
Increasing peace in the country	12	9	15	12	10	18	12	13
Curbing the spread of illegal gambling like jueteng	11	7	5	15	18	8	10	15
Stopping the destruction and abuse of our environment	10	7	9	13	10	8	10	11
Defending the integrity of Philippine territory against foreigners	8	9	9	6	7	12	8	8
Preparedness, including giving early warnings for typhoons, floods, landslides and other disasters/calamities	8	13	9	7	5	8	8	7
Protecting the welfare of OFWs	7	8	7	5	7	5	7	5
Speed of responding to the needs of those affected by typhoons and other disasters/calamities	6	7	8	5	5	9	6	9
Preparing to successfully face any kind of terrorism	4	3	4	4	5	5	4	5

Table 1: Issue preferences of voters in the 2016 Philippine National Elections
Source: Pulse Asia (2016)

Though it did not place as one of the highest issues, the emergence of it as one of the primary concerns has been directly borne from the combined efforts of Aquino's line agencies and diplomatic efforts that echoed within public sentiments. The arbitration win has been championed by the international community as a significant cog in the balance of power in Asia as a small island nation has successfully used international law and its channels to defend itself from the aggression and bullying of a rising military power that is China (Campbell, 2016).

The Philippines' victory however was short-lived after the win of the populist candidate Rodrigo Duterte which signalled a drastic turnaround in the narrative with China contrary to his initial claims of a hard-nosed independent foreign policy stance (Wong, 2020).

Built on lofty promises and goals, Duterte's cult of personality signalled a tough stance with China in the initial phases of his campaign such as the infamous promise to use a jet-ski to commute to the disputed island territories and plant the Philippine flag (Politiko, 2016). This stance on the other hand did not last long when Duterte slowly transitioned from a hard-nosed peddler of his own brand of "independent foreign policy" which he notes as "neutrality" by delinking the Philippine foreign policy agenda from the United States towards a familiar bias with China (Valeriano, 2023).

An example of his projected false neutrality is the soft stance of his administration despite the blatant claims of China on the disputed islands by naming it as part of a new administrative district in the Kalayaan group of islands (Rocamora, 2020).

Initially, Duterte's transition were noted as merely a "strategic play" to not further escalate tensions in the West Philippine Sea, however, his dalliance with China had a significant purpose because of its role with his banner project 'Build, Build, Build'. Duterte's major infrastructure push piggybacks with China's aspirations for regional clout through Xi's Belt and Road Initiative (BRI) amounting to $24 Billion which was initially based on 13 government to government contracts and was officially inked just several months after Duterte's official tenure (Fernando, 2020). Other than the Philippines, other ASEAN member states mirrored Duterte's pivot to China such as Laos but it has been widely known that from an economic perspective the China's BRI while connects countries, it largely favours China (Voros & Somsack, 2020).

After grand ambitions of a banner project based on the traditional economic pump-priming model (Department of Budged Management, n.d), Duterte's joint projects with China consequently failed due to various reasons (Baclig, 2022) and most markedly were severely set back by the 2020 pandemic as well as the mercurial relations in the West Philippine Sea that did not find enough clarity under his leadership (Rand Corporation, 2021). Eventually, Duterte's gamble with China failed due to the inefficacy of his own brand of statecraft articulated on hedging and political leveraging with no apparent solid grounding (De Castro, 2022).

Duterte's failed legacy with was obvious at the tail end of this administration after the Philippine public still remained cautious of the territorial disputes with 7% of respondents based on urgent concerns poll of Pulse Asia on June 2022 (Pulse Asia 2022). This result is a testament to the voter's preference of a President that prioritizes national security as part of a candidate's leadership platform and a confirmation to the perception that Duterte's administration has failed to address it within his tenure in office.

Curiously, it also seems to disregard any significant impact that the Duterte government has done in trying to displace the issue from public consciousness with a 7% showing and merely dropping by 1% from its 2016 record.

Issue	**% Change**	**% of Issue Preference in 2022**	**% from 2016**
Inflation	-27%	57%	30%

Increase pays for workers	+7%	45%	38%
Poverty reduction	+4%	33%	29%
Job Creation	+3%	29%	26%
Corruption in government	-20%	20%	30%
Enforcement of the law	-5%	15%	20%
Fighting criminality	-10%	14%	24%
Promotion of peace in the country	-2%	14%	12%
Provision of assistance for livelihood projects due to COVID 19	N/A	14%	N/A
Problem of involuntary hunger	N/A	12%	N/A
Tax reduction	N/A	9%	N/A
Environmental destruction reduction	-3%	7%	10%
Support to small entrepreneurs and businesses	N/A	7%	N/A
Defending the integrity of the territory against foreigners	-1%	7%	8%
Controlling of the spread of COVID-19	N/A	7%	N/A
Protection of the welfare of OFWs	-2%	5%	7%
Prevention of terrorism	-1%	3%	4%

Table 2: Comparison of issue preferences of voters in the 2016 and 2022 Philippine National Elections

Source: Pulse Asia (2016), (2022)

Noticeably, some issue concerns were missing in the 2022 iteration of the survey with drug problem, disaster preparedness was no longer seen as part of major issue concerns with Filipinos and were displaced mainly of issues focused on post-pandemic recovery, COVID-19 control, and hunger.

These new concerns are directly due to the black swan event of the pandemic and were necessary for most Filipinos to solve. Though mainly the list has not changed much and mostly the majority of concerns remain as key issues that are in need to be resolved such as worker pay, inflation, graft and corruption, law enforcement, and worker protection.

The absence of significant changes from the start of Duterte's reign to the end of his leadership on the issue of the West Philippine Sea signals an important space in the literature in answering what the cyberspace strategy employed, how the government framed its agenda, and finally

why is it that there was no significant effect in the issues preferred to be tackled by the voting public at the end of his term.

Re-thinking Cyberpolitical Spaces and Threats

The Philippines as a small island state has largely been considered as an underdog in this conundrum. In recent events, there has been an increasing need to echo the evolution of cyberspace and the importance it has in international relations. The West Philippine Sea tensions exacerbate this point with the convergence of cyber and disinformation activities (Ona, 2024). The threats posed by outside entities can easily derail domestic politics by manipulating popular discourse in legal channels such as, but not limited to applications, media, and the internet.

While cyberspace was formerly considered to be a place where low politics are prevalent and therefore does not affect state position or agenda in the early years of the internet. Choucri's interpretation of the Lateral Pressure Theory has asserted the poignant structure of cyberpolitical affairs, it is argued that the established threats to security nexus have now evolved with the ossification of the geospatial, environmental, and cyberspace spaces. Its illustration and example of this is the Current tensions of the Philippines and China.

A major manifestation of this merger of the geospatial and environmental to the cyberspace front is China's spending on alleged cyber-information operations amounting to $10 billion annually based on the 2021 study of Rand Corporation (Beauchamp-Mustafaga & Hornung, 2021). Through the Strategic Support Force of the People's Liberation Army (PLA) and its affiliate units, China was able to carry on its propaganda efforts beyond the borders of its own territory towards other actors which carry offensive and defensive capabilities.

It was reported that an existence of colloquially called as the 50-cent army are utilized as keyboard trolls and warriors to push propaganda, fight alternative views online, and report on would be dissenters and groups (Lau, 2016). According to various reports, the 50-cent army are composed of 500,000 to 2,000,000 members and are summoned to redirect and deflect critical opinion and promote those that are in line with the state message (Intelligence Insight Group, n.d).

The existence of the 50-cent army emphasizes the need for states to be cautious of cyberspace and with devious forms of non-combative warfare whose damage is intangible and hidden. The war of ideas has now taken cyberspace and the weaponization of the keyboard is in full force with the creation of military units whose full aim is to deceive public opinion to carry-on alien interests that are beyond the targeted state's control or national interest. In this regard, Choucri's differentiation of the three geopolitical spaces no longer hold true as cyberspace now transcends

geospatial and environmental interest with the weaponization of the information in the internet. Duterte's case presents a peculiar case whereby he himself have shown drastic efforts to ease in China's interest within the context of national interest and foreign policy agenda as seen in the official releases of the PNA. This reimagines Choucri's model by inserting traversing arrows from geospatial and environmental domains towards cyberspace as demonstrated by state action and cyber operations.

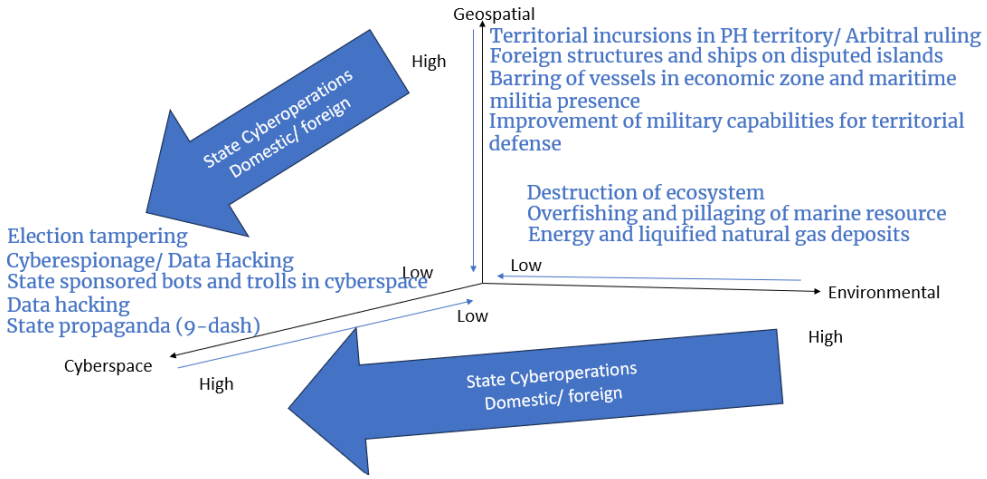


Figure 3: Application of Lateral Pressure Theory in the West Philippine Sea

As it was discussed in the last parts of the research, Duterte's legacy was hinging on China's infrastructure push and therefore inevitably affecting his government's stance on certain issues by branding his government's decoupling from the United States as 'independent foreign policy'. This though did not hold true because his pro-China proclamations were apparent from the start and seemingly did not follow any strategic logic (Strangio, 2024). It therefore, inevitably in the best interest of his administration to align with China's interest and sacrificing domestic interest in the disputed islands by cloaking his pro-China stance as an independent strategy and brand.

A clear display of this partnership is the Philippine Communications Operations Office (PCOO) who serves as the primary media arm of the president has sent numerous media practitioners under their agency to China to learn 'state-media' approach being used under China (Pechora, 2018). With this formal partnership, it is apparent that the government under Duterte's rule wanted to emulate China's strategy in controlling and influencing the populace. Yet, allegedly, Duterte's strategic use of social media manipulation has been widely reported even before he won the presidency with the use of paid online trolls that parallel China's 50-cent army with the use of 400-500 cybertroops (Bradshaw & Howard, 2017). This however does not show a

direct link whether Duterte has had help from China, yet it is highly speculated that Duterte's campaign has had significant help from foreign entities (Reuters,2021). It also does not help that under Duterte's tenure, efforts to diminish the impact of fake accounts and cybertrolls were rejected by himself citing possible constitutional concerns despite it having a potential impact in helping with surveillance and national security (France 24, n.d).

Due to the allegations and apparent linkages with China's influence on Duterte prior and during his tenure as president, it further challenges the literature in how Lateral Pressure Theory sees Duterte's recalibration and re-introduction of foreign interest into domestic public discourse.

The state in this re-conceptualization of Lateral Pressure Theory advances the initial notions and suggestions of Choucri and other proponents of the theory to explore the ongoing relational changes between the geopolitical spaces within cyberpolitics. The application of the Lateral Pressure Theory not only to discuss the extension of state interest in the three spaces but also as a tool of the state to recalibrate national agenda and form it to their own brand casts a new level of analysis and vulnerability in democracies.

Methodology

The study used primarily qualitative research utilizing content analysis through thematic categorization and desk research using primary and secondary data sources. Focusing on government owned and controlled media namely, the PNA over the span of the administration's tenure of governance from 2016-2022. It will not on the other hand include non-government media outlets, sites, and applications or via third party companies, groups, and civilian journalist sources.

Analysis and Discussion of Results

Tale of the Web: Duterte's Strategy in the West Philippine Sea

Based on the extensive thematic research done on over 901 official media releases and articles regarding the West Philippine Sea from 2016-2022 officially posted in the government's official news agency the Philippine News Agency website, it is apparent that the Duterte administration has tried its best to deflect, and reframe the West Philippine Issue towards a more welcoming foreign policy model.

Issue	Promotion of PHL interest	Reinforcement of PHL interest	Neutral	Appeasement towards CHN interest	Promotion of CHN interest	Total
Geospatial						
Territorial incursions in PH territory/ Arbitral ruling	64	47	31	23	79	244
Building of foreign structures and ships on disputed islands	49	26	17	7	11	110
Barring of vessels in economic zone and maritime militia presence	25	13	10	3	15	66
Improvement of military capabilities for territorial defense	63	8	7	4	10	92
Environmental						
Destruction of marine ecosystem	9	6	2	0	4	21
Overfishing and pillaging of marine resources	10	5	2	1	11	29
Energy and liquified natural gas deposits	9	4	5	6	26	50
Cyberspace						
9-Dash line	1		1			2
Data hacking						0
State sponsored bots and trolls in cyberspace						0
Election tampering				1		1
					Total	615

Table 3: Thematic content analysis of articles from 2016-2022 under the Duterte administration tackling the WPS

After an extensive review of the PNA website, out of a total of 901, 615 tackled the core topics and issues in the West Philippine Sea while others are considered to be indirectly linked to the PHL-China issue which ranges from weather reports, local news, holidays pronouncements among other fluff pieces. Among the 615 reports, the top three issues were on the territorial dispute and arbitration dominated the headlines with a total of 244 articles, followed by the building of structures in the disputed islands with a total of 110, and lastly, the improvement of military capability and capacity with 92 posts.

Following these results, the preference remains to push for geospatial narratives having 83.25% followed distantly by the environmental domain with 16.26% and lastly, cyberspace taking in a mere 0.49%.

Domain	Percentage
Geospatial	83.25%
Environmental	16.26%
Cyberspace	0.49%

Table 4. Percentage total per cyberpolitical domain

Further analysing the thematic differences in the articles, it was understood that the Duterte administration has pushed for the pro-China bias significantly in the arbitral ruling specially in the first half of his tenure as president 2016-2019. The core messaging in these articles indicated a stance of appeasement and the delegitimization of the arbitral ruling totalling to 152 articles. On the contrary, the government also have balanced this by publishing articles that pushed for national interest with 297 published pieces that reinforced and promoted Philippines' stance in the region. On the contrary, pro-Philippine messaging was mostly carried out by cabinet officials and leaders while pro-China rhetoric mostly came from the executive branch under Duterte and his office. This division indicates internal factions within as divisive groups clashed on national agenda and positioning on foreign policy despite claiming a supermajority within his administration (Romero, 2016).

The environmental field placed second in the list and were filled with pro-China stance in advancing the possibility of oil and mineral mining partnerships in the disputed territory. Again, this pattern was prevalent in the early years of the administration with repeated calls for partnerships in the WPS which was angled to show how the arbitral ruling should not be given credence and benefit a possible boost to the country's economy. Meanwhile, an issue connected to national security also showed a pro-China slant pertaining to overfishing which shares the common bias with oil exploration positioned as a possible partnership with China and therefore aiming in diluting the Philippines' claim. One vague issue that the government had varying stances on was the marine protection and destruction of the ecosystem with contrasting claims of protection and partnerships proposed with China who was also painted as the primary violators in the area. Given these, the environmental domain shows how the government used the environment as a leverage for economic gain and soften public opinion against China's aggression.

Lastly, cyberspace did not make a significant showing in the overall count however has supported the notion that cyberspace should no longer be seen as a static domain but a variable that boosts other geopolitical spaces in cyberspace. In this case, cyberspace was no longer just a separate issue area but a catalyst to other cyberpolitical spaces.

The application of lateral pressure theory has to be challenged and revisited with the premise that the core definition of the cyberspace area should not be limited to cyberattacks or issues but should also be seen as a variable that boosts other agenda and issue concerns. Cyberspace in this case also has shown that it is now a tool more than just a categorization or an arena where low and high politics coexist.

Due to the increased access to the internet and the lowered barrier of entry, cyberspace has now evolved to a preferred vehicle for influence. No longer is cyberspace confined to illicit acts since now, pushing agenda in the internet does not need to be overt and forced, now, influence can be had if the heads of state are compromised or influenced by external actors. State agenda effects in cyberspace is no longer a one-way exogenous path and should be understood as a reflection of lateral pressure to its citizens.

Domestic Control Through Lateral Pressure

Using content analysis through thematic categorization of content within the PNA, a common strategic model is revealed and created. Within it, the methods on how a state can use lateral pressure not only to project its national agenda but also to recalibrate the issue and reframe existing stances towards drastically polarizing biases.

The study propositions that the Duterte has used three significant facets of media reframing namely under the actions of Curtailment, Constriction and Containment and hereby will be called Lateral Pressure Reframing. It is argued that the Lateral Pressure Theory discounts discontinuity of regimes among democratic countries such as that of the Philippines. With weak party affiliations and ideals, Philippine politics is idealistic and have been in constant state of flux among the leaders it has had in the last two decades. The study espouses the need for the theory to include the state's power to intervene and reframe state agenda to another bias with the use of cyberspace in controlling geospatial and environmental facets of domestic and foreign policy.

Strategy	**Goal**
Curtailment	Curtail public opinion and dissenting voices from gaining popular traction in the populace by framing them as enemies of change, progress, and national security. Application: Often used in geospatial issues, the divisive strategy has been seen in numerous cases by creating division between his supporters and those who are dissenting in his leadership due to the ease of framing geospatial narratives of traitors to the state.

Constriction	Constrict inflammatory issues regarding the government by deflecting accountability through plausible deniability to other agencies, groups or individuals away from the executive branch or the government. Application: The environmental nexus was used in this aspect as it was observed with diplomatic protests which are environmentally related against China whereby former Department of Foreign Affairs Teodoro Locsin Jr. was called upon by the executive branch as the main proponent of the diplomatic protests delinking from the president and his office.
Containment	Control the narrative by using extreme examples that would spread fear and doubt to the populace if an alternative solution was followed which is contrary to his government office. Containment transcends the geospatial and environmental domains since it is also used to ensure constant control of the narrative ensuring a net positive framing in favour of the government and its institutions. Application: Cyberspace was used in this campaign with Duterte projecting a defeatist narrative of 'having no other choice' or face harsher consequences such as that of the threat of war with China in his press releases, personal interviews, and live official pronouncements covering all three domains of geospatial, environmental as well as cyberspace.

Table 5: Lateral Pressure Reframing in application to the West Philippine Issue

The observed application of the theory as studied in the official press releases on the West Philippine Sea has shown a pattern of state strategy that is aimed to reframe public opinion in expense of national interest. A pro-China government such as in the case of the Duterte administration has tried to pivot towards China just to have marginal effect in diminishing the importance of the territorial dispute which will allow China to legitimize its claim in the islands and maritime territory.

With the observed strategy and extension of the Lateral Pressure Theory, it is shown how cyberpolitics and its geopolitics needs to again be recalibrated and extended to include the state as a possible proponent of foreign interest. With Duterte's bias and pro-China stance, it is an example of the fragility of democracies with drastic policy shifts in accordance with the elected personalities in countries with weak political institutions and parties.

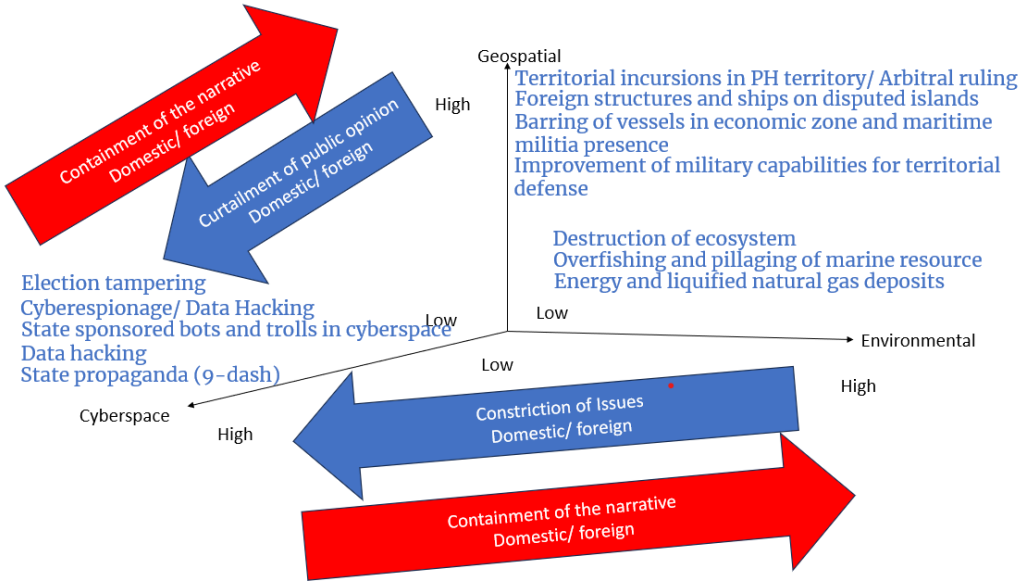


Figure 4: Proposed conceptualization of Lateral Pressure Reframing in the West Philippine Sea

It is acknowledged that further research needs to apply the extension proposed to the Lateral Pressure Theory to test its fundamental integrity and viability in other contexts and cases. Nonetheless, the study commits itself to the need to continually progress the literature in accordance to the demands of the fast-evolving world narratives. The case presented in this study sets the needed foundations for further inquiry and have shown the potential its theory as a means of control not only exogenously as formerly thought but endogenously to pivot its own citizens towards a new direction of governance.

Conclusions

The West Philippine Sea's narrative today under the Marcos regime can be reclaimed again by reengaging the same template of cooperation and statecraft under the Aquino administration. A concerted effort to reframe the geospatial arena as an immediate national threat to security and environmental factors that need to be addressed as a global public good will be a much-needed restart after Duterte's sabotage of the momentum gained from Aquino III's monumental arbitral rule legacy. A coordinated endeavour will be crucial to flip the narrative back to the Philippines and reinstate its rightful and legitimate claim unified with the international community.

References

Akdağ Y. (2023). Cyber AI Technology and International Relations. *Cyberpolitik Journal,* Vol 8, No 16, pp. 149-152

Baclig C. (2022). Targets missed in Duterte's 'Build, Build, Build: What's next?. Philippine Daily Inquirer. 04 April 2022, https://newsinfo.inquirer.net/1578195/targets-missed-in-dutertes-build-build-build-whats-next.

Bradshaw S. & Howard P. (2017). Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. University of Oxford. Working paper no. 2017.12, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2017/07/Troops-Trolls-and-Troublemakers.pdf.

Campbell C. (2016), South China Sea Arbitration Ruling: What Happened and What's Next. https://www.uscc.gov/sites/default/files/Research/Issue%20Brief_South%20China%20Sea%20Arbitration%20Ruling%20What%20Happened%20and%20What%27s%20Next071216.pdf.

Center for Preventive Action (2024), Territorial Disputes in the South China Sea, https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea, (Accessed Time: 29 October 2024.)

Choucri, N., & Agarwal, G. (2017). *The theory of lateral pressure: Highlights of quantification and empirical analysis.* In W. R. Thompson (Ed.), The Oxford Encyclopedia of Empirical International Relations Theory. Oxford University Press.

Choucri, N., & North, R. C. (1989). *Lateral pressure in international relations: Concept and theory.* In M. I. Midlarsky (Ed.), Handbook of war studies (pp. 289–327). Unwin Hyman.

Version: Final published version.

Davidson H. (2024), China Maritime Militia: The Shadowy Armada Beijing Rarely Acknowledges, https://www.theguardian.com/world/article/2024/jun/13/china-maritime-militia-explainer-south-china-sea-scarborough-shoal, (Accessed Time: 30 October 2024).

De Castro R. (2022). The Failure of the Duterte Administration's Pivot to the Non-traditional Partners. https://www.bworldonline.com/opinion/2022/08/30/471526/the-failure-of-the-duterte-administrations-pivot-to-the-non-traditional-partners/, (Accessed Time: 28 October 2024).

De Castro R. (2024), Evolving Grand Strategy in the Face of China's Maritime Expansion: From the Aquino Administration to the Marcos Administration. https://journals.sagepub.com/doi/full/10.1177/18681034241234670, (Accessed Time: 25 October 2024).

Department of Budget Management (n.d). 'Build, Build, Build to generate 1.1 million jobs annually in the medium term'. https://www.dbm.gov.ph/index.php/management-2/773-build-build-build-to-generate-1-1-million-jobs-annually-in-the-medium-term, (Accessed Time: 20 October 2024).

Fernando J. (2020). China's Belt and Road Initiative in the Philippines. https://www.eastwestcenter.org/publications/china%E2%80%99s-belt-and-road-initiative-in-the-philippines, (Accessed Time: 25 October 2024).

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, *45*(3), 426–458.

France 24 (n.d). (2022). 'Philippines' Duterte blocks bill to register social media users. 15 April 2022, https://www.france24.com/en/live-news/20220415-philippines-duterte-blocks-bill-to-register-social-media-users, (Accessed Time: 23 October 2024).

Harold S., Beauchamp-Mustafaga N., & Hornung J. (2021). 'Chinese Disinformation in Social Media'. Rand Corporation. https://www.rand.org/pubs/research_reports/RR4373z3.html, (Accessed Time: 18 October 2024):

Heydarian R. (2019). China's Economic Cabbage Strategy. https://amti.csis.org/chinas-economic-cabbage-strategy/, (Accessed Time: 24 October 2024).

Ibarra, E. J. (2024). "Articulating a Philippine grand strategy: Policy Continuities on the South China Sea". *Asian Politics & Policy*, *16*(3), 317–336.

Intelligence Insight Group (n.d). (2024). 'The 50 Cent Army: Unveilign China's Digital Influence Operations'. https://insightintelligence.com.au/the-50-cent-army-unveiling-chinas-digital-influence-operations/, (Accessed Time: 25 October 2024).

Lau J. (2016). Who Are the Chinese Trolls of the '50 Cent Army'?. O7 October 2016, https://www.voanews.com/a/who-is-that-chinese-troll/3540663.html, (Accessed Time: 23 October 2024).Lee- Brago, P. (2011). China building in Phl waters; DFA summons envoy.

Philippine Star, 02 June 2011, https://www.philstar.com/headlines/2011/06/02/691807/china-building-phl-waters-dfa-summons-envoy, (Accessed Time: 15 October 2024).

Lundberg, E. (1971). "Simon Kuznets' Contribution to Economics". *The Swedish Journal of Economics*, *73*(4), 444–461.

Ona S. (2024), ADRi Special Study: 'The West Philippine Sea and the Convergence of Offensive and Cyber Disinformation Activities. https://adrinstitute.org/2024/03/15/adri-special-study-the-west-philippine-sea-and-the-convergence-of-offensive-cyber-and-disinformation-activities/, (Accessed Time: 16 October 2024).

Parrocha A. (2018). PCOO thanks Chinese state-media for good news about PH. https://www.pna.gov.ph/articles/1054455, (Accessed Time: 17 October 2024).

Permanent Court of Arbitration (nd). The South China Sea Arbitration (The Republic of Philippines v. The People's Republic of China). https://pca-cpa.org/cn/cases/7/, (Accessed Time: 20 October 2024).

Politiko (2016), Duterte to ride jetski to plant flag in Spratlys and challenge China': Suntukan or Barilan, https://politiko.com.ph/2016/04/12/duterte-to-ride-jetski-plant-flag-in-spratlys-and-challenge-china-suntukan-o-barilan/features/, (Accessed Time: 18 October 2024).

Pulse Asia (2016), Nationwide Survey on Urgent National Concerns to be Addressed by Presidential Candidates and Most Important Consideration in Choosing a Presidential Candidate, https://pulseasia.ph/databank/electoral-polls/, (Accessed Time: 17 October 2024).

Pulse Asia (2022). Nationwide Survey on Urgent National Concerns and Issues to be Prioritized by the New President', https://pulseasia.ph/updates/june-2022-nationwide-survey-on-urgent-national-concerns-and-issues-to-be-prioritized-by-the-new-president/, (Accessed Time: 20 October 2024).

Ramos M. (2018). China ignored ASEAN agreement to ease sea tensions, said Aquino. Philippine Inquirer, https://globalnation.inquirer.net/167514/china-ignored-asean-agreement-ease-sea-tensions-says-aquino, (Accessed Time: 16 October 2024).

RAND Corporation (2021). China Has Lost the Philippines Despite Duterte's Best Efforts. https://www.rand.org/pubs/commentary/2021/05/china-has-lost-the-philippines-despite-dutertes-best.html, (Accessed Time: 18 October 2024).

Reuters (2021). Philippines calls allegation on China election influence 'nonsense'. https://www.reuters.com/world/asia-pacific/philippines-calls-allegation-china-election-influence-nonsense-2021-07-12/, (Accessed Time: 13 October 2024).

Rocamora J. (2020). PH 'strongly protests' self-declared Chinese districts in SCS. https://www.pna.gov.ph/articles/1101533, (Accessed Time: 26 October 2024).

Romero A. (2016). Duterte secures 'super majority' in house', Philippine Star, https://www.philstar.com/headlines/2016/06/08/1590856/duterte-secures-super-majority-house, (Accessed Time: 23 October 2024).

Schmitt, Michael N. (Ed.). (2017). *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. Cambridge University Press.

Schmitt, Michael N. (2013). '*Tallinn Manual on the International Law Applicable to Cyber Warfare'*. New York, United States of America: Cambridge University Press.

Song, Yann-huei, and Keyuan Zou. *Major Law and Policy Issues in the South China Sea: European and American Perspectives*. Routledge, 2016.

South China Morning Post (2012)., Philippines renames coast 'West Philippine Sea'. https://www.scmp.com/news/china/article/1035119/philippines-tags-coast-west-philippine-sea, (Accessed Time: 20 October 2024).

Strangio S. (2024). Parsing the Philippines' 'Pivot' to China Under Rodrigo Duterte. The Diplomat. https://thediplomat.com/2024/09/parsing-the-philippines-pivot-to-china-under-rodrigo-duterte/, (Accessed Time: 21 October 2024).

Tarhan K. (2023). "Technology Ethics: A Philosophical Discussion and Readings". *Cyberpolitik Journal*, Vol 8, No 16, pp. 166-171.

Valeriano I. (2023). Duterte's Independent Foreign Policy Delinking the Philippine from the United States. https://postcolonialpolitics.org/dutertes-independent-foreign-policy-delinking-the-philippines-from-the-united-states/, (Accessed Time: 20 October 2024).

Vörös, Zoltán, and Pongkhao Somsack. (2020). "Laos and the belt and road initiative: An Interconnector helping the Chinese needs?" *Foreign Policy Review*, vol. 13, pp. 24–38.

Wong A. (2020), Myth of Rodrigo Duterte's independent foreign policy. Retrieved October 2024, from https://www.lowyinstitute.org/the-interpreter/myth-rodrigo-duterte-s-independent-foreign-policy, (Accessed Time: 20 October 2024).

WHAT KIND OF THEORY OF INTERNATIONAL RELATIONS IN THE CONTEXT OF CYBERSPACE?

İbrahim KURNAZ*

Orcid: 0000-0001-7228-6536

Abstract

Cyberspace, which has found a working ground within the framework of cyber policies on the basis of international relations, constitutes a new field of study in International Relations together with cyber attacks. In today's world, cyberspace, which has such a transformative effect on the communication and interaction of political and social formations with each other, has also attracted the attention of the followers of the International Relations Discipline, which naturally includes human relations, by affecting social, economic and political platforms. Because cyberspace and all the concepts, theories and developments derived from it now affect International Relations on a multidimensional basis. Therefore, how this new field affects international politics within the framework of cyber policies, at what points it has the capacity to transform or erode the discipline and in general how it affects the epistemological, ontological and even methodological dimensions of the discipline are important. Indeed, when it is considered that traditional International Relations theories and theorists are inadequate in explaining the rapid change and transformation in cyberspace, the importance of the study becomes apparent. In this context, this study will focus on the concepts, questions that need to be emphasized in order to evaluate how IR theories explain and understand cyberspace and the assumptions to be developed based on these questions. At the same time, on the basis of all these issues, it will be evaluated how traditional theoretical approaches view cyberspace in the IR plane and on which essential alternative cyber IR theories should be built.

Key Words: Cyberspace, International Relations Discipline, International Relations Theories

Introduction

The discipline of International Relations (IR) deals with all elements of the political field with its interdisciplinary nature. The struggles and interactions of the actors with each other in the

* Dr. Öğr. Üyesi, Uluslararası İlişkiler Bölümü, Selçuk Ünversitesi, Konya-Türkiye, ibrahimkrnz@selcuk.edu.tr

international system are the primary reasons for the diversification of these elements. Cyber security and its reflections, which have found a ground in the context of international security, are making themselves felt in the political arena in terms of changing world conditions. The situation where the struggle for interests is the focal point has risen to the top of the agenda of states that hold the distinction of being the main actors in the power struggle with cybersecurity and related tools.

Of course, information wars and access to strategic information have historical pasts in terms of security and international relations. However, despite the ancient power of information, it can be said that the concepts of cyber power and cyberspace have emerged as relatively new elements of power. Indeed, the literature on the impact of cyber warfare on IR has also begun to form (Choucri, 2012: 1-14; Choucri and Clark, 2019; Foulun and Meibauer, 2024: 426-458). Studies in which cyberspace is addressed and discussed in the context of IR and which now have a working integrity under the name of cyber policies are increasing.[1] No matter how controversial the concepts such as cyber warfare, cyber intelligence, cyber conflicts, cyber deterrence, cyber power, which will be increased in number, are, it is a reality that international actors diversify within the cyberspace and turn into instruments of influence in IR. The cyberspace, which has risen in terms of international politics with the concepts in question and their practical reflections, has also become an option with the concept of deterrence.

It is possible to say that the point that IR followers are most interested in regarding cyberspace is the area where cybersecurity overlaps with national and international security (Burton, 2013: 216-218; Rid, 2012). Especially with the end of the Cold War, the transformation of the perception of security and the replacement of traditional security elements with asymmetric elements have increased the dimensions of the discussions on security. However, as far as can be observed, almost all political and military conflicts have also developed a cyber dimension. Therefore, technological developments affecting inter-state relations as well as social relations have caused relatively radical changes in the discipline of IR (Akdağ, 2023). Security, as the area where these changes are most effective and where erosion is most felt, is taking a different form every passing day. However, traditional IR theories and theorists are inadequate to explain the rapid change and transformation in cyberspace. Therefore, in the cyber age, IR theories need to offer a new perspective in explaining social, political, social and economic events.

*Dr. Öğr. Üyesi İbrahim Kurnaz, Selçuk Üniversitesi Uluslararası İlişkiler Bölümü,

[1] For detailed information on this subject, see: http://cyberpolitikjournal.org/index.php/main/index

In this context, how can a bridge be established between cyberspace and international relations, how can cyber security be reduced to the perspective of international relations and how can this discipline be studied? It is known that MIT (Massachusetts Institute of Technology) has made important publications especially in this interdisciplinary study. Based on these points, this study will focus on the concepts and questions that should be focused on when constructing IR theories related to cyberspace. At the same time, all these issues will be evaluated in terms of how traditional theoretical approaches view cyberspace in terms of IR and on what grounds alternative cyber IR theories should be constructed. In this direction, in the first part of the study, how IR theories are put into practice as a new policy area in cyber policy will be discussed, while in the second part, the approaches of existing IR theories towards cyberspace will be discussed. In the third part, the questions and foundations on which it is possible to produce an international relations theory regarding cyberspace will be discussed.

A New Policy Area for International Relations Theories: Cyber Politics

In today's world where information revolutions have the potential to transform international politics, the increasing impact of information and communication technologies and the internet on many aspects of our daily lives has led to the need to bring cyber-focused approaches and solutions to the challenges encountered. The digital universe has brought the question of how to transfer traditional governance concepts to the new level in cyberspace to states. Because, as mentioned before, developments and reflections originating from cyberspace affect IR in a multidimensional way within IR. Actions and transactions in cyberspace have brought a different dimension to both international relations as a type of relationship or practice, and to IR as a discipline, and therefore have the potential to transform all concepts and sets of theories related to the discipline. Revolutions originating from cyberspace have the potential to affect international relations in three ways in terms of decision-making processes, information sharing and diplomatic processes. First, by increasing and expanding the interests and discourses in the international policy process, they make decision-making processes more complex and reduce the state's control in this process. Secondly, since it brings about the acceleration and cheapening of information about a subject or development, it has an impact on the process and results of managing information. Thirdly, it has also brought about the fast and cheap provision of traditional diplomatic services to individuals, states and other non-state actors (Akyelişmen, 2018: 175-176).

Nazlı Choucri claims that combining Lasswell's "definition of politics as the distribution of values in society through an authority" with David Easton's striking definition of "who gets what, when and how" leads us to the most general and appropriate view of politics, valid in all

contexts, times and places. Choucri, who adapted politics to the cyberspace, stated that with the creation of cyberspace, a new area for the conduct of politics has been shaped and that we are witnessing a new form of politics (Choucri, 2012: 4). The concept of cyber politics is also a concept that is just beginning to be developed and is being worked on. Choucri states that the concept of cyber politics is formed by the merging of two processes or realities. Namely, cyber politics is combined as those that belong to human interactions (politics) surrounding the determination of who will get what, when and how, and those that are possible by using a virtual space (cyber) as a new area of contestation with its own forms and realities (Choucri, 2012: 4). Cyberspace is another arena. It is a space created through technological innovation, allowing users to engage in activities that are put into practice through digital spaces with spatial spaces that exceed traditional regional, social and economic restrictions. Historically, access to and participation in the cyberpolitics space was limited to the most powerful; the nature of the enterprise and its organizational complexity limited the number of players. In contrast, access to cyberspace is becoming available to more and more people around the world. Today, the number of people with Internet access has reached billions (Meibauer et al., 2020: 268-295). This space offers new opportunities for competition, contestation, and conflict as fundamental elements of politics and the pursuit of power and influence.

It is important to understand the sets of concepts and theories that will be necessary to make sense of this new area of politics and the effects of these sets on international politics and IR theories. In this period that is close to the end of the first quarter of the 21st century, cyberspace and international politics mutually affect each other. The IR discipline regarding cyberspace, whose intensity, speed and impact have increased tremendously in this century, has not been able to fully nourish on theoretical and conceptual grounds. Because IR theories under the dominance of positivism have made their foundations on interactions in physical spaces/areas (Dunne vd., 2013: 1-14). Physicality in IR also creates opportunities to expand power and influence in international politics. Any physical space refers to the spheres of interaction that create potential sources of power, influence and hegemony, information and markets in IR. When the actions of one actor threaten the sovereignty, stability or security of other actors, physicality becomes a significant variable in IR. Traditionally, the concept of physical space has been closely linked to territoriality. Physical spaces have been shaped by the exercise of pure physical power combined with competitiveness, innovation and a spirit of adventure. Historically, only the politically and militarily powerful major powers have been able to compete effectively in the conquest of territory and the exploration of outer space (Heywood, 2011: 4-8). These spaces have been marked by the physical spaces in which the quest for power

lies. National prestige, international positioning, wealth gain and strategic advantage in military competition have all been achieved through physical expansion into territory or the atmosphere. Both colonialism and the space race, in their different ways, have controlled rather than leveled the playing field. The space itself has been defined by the few states that can afford to play. It is cyberspace and the new arena of interactions that loosen this relationship (Choucri, 2012; Akyeşilmen, 2018).

However, when observed, threats originating from cyberspace have brought cybersecurity to the top of the national security agenda. Therefore, it is essential to develop a comprehensive and holistic understanding of cyber policy towards cyberspace. Because it is an area that will create a new struggle and competition environment within international relations. In fact, this area brings with it differences in terms of tools, methods and policies, unlike traditional areas. The reflections of these differences on international relations and politics were put into practice in the 2007 Estonia, 2008 Georgia hybrid war, 2010 Stuxnet attack on Iran and 2013 US elections (Russ, 2008; Burton, 2013). Since these developments that will shape international politics originating from cyberspace also bring about transformations, cyber policy is now important.

WHAT KIND OF CYBER THEORY OF INTERNATIONAL RELATIONS?

With the civilianization of cyberspace, the nation state formation that emerged from the Westphalia system was deeply affected (Choucri and Clark, 2019). It is possible to see the traces of nuclear war and conflict in this new era that emerged with the end of the Cold War. The threats that each historical, political and social formation (individuals, states and other non-state actors, etc.) faces from cyberspace and their still unclear boundaries are clearly seen in examples. Cyber attacks against a long-standing security alliance such as NATO and its members in this new security environment provide important clues for the future (Bıçakçı, 2014).

Therefore, it is a matter of curiosity how cyberspace, which manifests itself as a new field for IR, will affect world politics, actors, facts and processes, and how it will affect the epistemology and ontology of the discipline (Akyeşilmen, 2018). Because the concept of cyber feudalism has begun to be frequently mentioned in social sciences in general and in IR in particular. Accordingly, the information revolution in the information age has flattened hierarchies and intensified network organizations. It has been stated that in the information age of the 21st century, centralized bureaucratic administrations will evolve into decentralized organizations in the century in question, and that government functions will be undertaken by private sectors and similar non-organizations (Toffler, 1990; Drucker, 1994). In addition, in the context of

cyber feudalism, other writers have argued that as virtual communities and decentralized organizations develop on the Internet, they will intersect with territorial areas and develop their own governance patterns (Nye and Welch, 2014). Nation states will continue to exist, but their importance will diminish and they will perhaps no longer be central to the life of societies. People will be together through multiple and voluntary contracts and will join and leave communities in a computer environment. These new communities and governance patterns that overlap with each other will be a modern and more civilized world similar to the feudal world that existed before the Westphalian state system became dominant. This world is also described as cyber feudalism (Nye and Welch, 2014: 424). This area is relatively similar to the pre-Westphalian period in terms of its nature and actor structure.

However, although it is an undeniable fact that discussions are being held in cyberspace regarding borders, sovereignty, territoriality, security and many elements related to the state, this situation leaves unanswered the questions of the vision of going beyond the nation state, how the rights claims of virtual and geographical communities will clash and how violence and security issues will be overcome (Nye and Welch, 2014). In this context, there is a need for a theoretical and conceptual framework in the context of IR in order not to leave these questions unanswered and to understand all kinds of outputs originating from cyberspace. In this century, when cyberspace and IR have started to affect each other intensively, there are few and holistic conceptual and theoretical frameworks in order to understand the mutual interaction and processes.

Theorizing cyberspace in the context of IR is relatively new in the sense that cyberspace has difficulty formulating broader policy and theoretical implications for international policy patterns. This is primarily because politics in cyberspace and IR lack the conceptual and theoretical tools to do so. This article argues that conceptualizing and theorizing cyberspace as a policy area that will affect international relations can provide a better understanding of the causal role and effects of the field in IR. Based on these points, it is necessary to present the arguments of traditional IR theories, how these theories approach cyberspace, and the criticisms about how these theories exclude cyberspace. Then, the importance of terminology in creating alternative cyber International Relations theories will be emphasized.

Reading Cyberspace in Terms of Traditional IR Theories

Within this framework, it can be demonstrated that IR theories are compatible or incompatible with cyber policies and cyberspace, both through this terminological plane that has begun to become established and the research topics and questions in question. Of course, the effects of cyberspace on the discipline have only just begun. The issue of how international relations

theories interpret Cyberspace and whether their basic arguments in traditional international politics are now accepted by this field has begun to be discussed. Can cyberspace and the policies implemented in this field really transform international politics? The answers to the question that IR theories will give will also reveal whether they are compatible with the cyberspace environment. First of all, when the realist theory is considered, it is likely that this theory will answer this question negatively. First of all, in order to find answers to these questions, it is necessary to start with the evaluation of realist theory.

Realism, as a theory of IR that has a long history, has become popular especially after World War II. Its important representative Hans Morgenthau stated that international politics is governed by objective and universal laws based on national interests defined in terms of power. He also points to human nature as the source of these laws. He stated that politics is abstracted from moral and ethical values and social and economic aspects and even above them. Because, according to Morgenthau, international politics is a struggle for power (Morgenthau, 1967: 25-26). As can be understood from this introduction, the realist IR theory presents its foundations on power, interest and human nature. Human nature is evil because it is selfish and inclined to evil and thinks only of its own interests (Avcı, 2024: 100). States, similar to people, think of their own interests. This synchronized narrative both sees states as the main actors of IR and reveals the conflicting character of IR.

In realism, power can be defined as the ability of an actor to make another actor do an action that he does not want to do. Therefore, the power of a state can only gain meaning when compared to the power of other states. Since power and power maximization are permanent goals, the distribution of power is also important for realists. Therefore, the balance of power in the international system is a subject that realists focus on. The balance of power is evaluated more in terms of military power, and military alliances are seen as the basic dynamics of creating and maintaining the balance of power. According to realism, this arithmetic defined in terms of power is fixed and unchangeable. Since the realist theory reads IR as state-centered, it argues that the basic norm of IR also acts according to the principle of sovereign equality. The understanding of sovereignty in IR is the principle that shapes the nature of the relations of states, which are the basic actors of the international system, with each other. As a reflection of this expression of sovereignty, an outcome emerges in which states are equal to each other and are not dependent on any higher authority. This is anarchy, one of the basic assumptions of realism (Avcı, 2023: 59-74).

After the 1970s, after criticisms of classical realism, the theory of neo-realism emerged within IR under the leadership of Kenneth Waltz based on the deficiencies of the theory in question.

Neo-realism basically focuses on the structure of the international system and the relative power distribution within the system. Because according to neorealism, the reason for this reading is that the determining element of the international system is anarchy (Avcı and Morçiçek, 2024: 105). So much so that when they read based on this element, they argued that states follow similar policies despite being essentially different. In this respect, states differ from each other only in terms of the capacities they possess. Neorealists, just like classical realism, strongly argue that the system is anarchic (Waltz, 1979). This anarchic structure also reduces the possibilities of cooperation between states. In such a system, states can only rely on themselves. Therefore, states instrumentalize power in order to achieve their goals and ensure their security. According to neorealism, states always try to increase their relative power with the fear that exists in an anarchic environment within the self-help system (Mearsheimer, 2001: 2). According to defensive realism, the balance of power formed by the mutual positioning of material capacities determines state behavior in international relations. At the same time, the distribution of material capacities creates the structure (Waltz, 1979: 97-99). In realist theories, material capacities are the military capacity, which is the source of coercive power, and the economic resources that feed this military capacity.

Therefore, the question asked in this title of the study is whether cyberspace and the policies implemented in this area can really transform international politics, first of all, when the realist theories (both realism and neo-realism) is considered, it is likely that these theories will answer this question negatively. Because according to realism, states are still the main actors. Although the anarchic environment in cyberspace provides opportunities for non-state actors to run rampant, it also increases the power of states. Neo-realists construct cyberspace on a power politics perspective, claiming that, even with new forms of power, struggles for state power will be dominant, despite the fact that cyberspace poses a deep threat to the state system in terms of transcending borders and eroding traditional security paradigms (Steinberg and McDowell, 2003: 197). In this vein, Rothkopf emphasizes that the realist politics of the future should be built on cyberpolitics. According to Rothkopf, the actors are no longer just states, and conventional power should be synthesized or strengthened with information power. The powerful in cyberspace will continue to win, but the resources, tools, and measures of that power will change significantly (Rothkopf, 1998: 326).

In fact, it is argued that the power hierarchy between states is similarly put into practice in cyberspace. In cyberspace, major powers such as the US, China and Russia are at the top of the list both in internet usage and in implementing cyber policies in this area. Although medium or small-scale states have also made significant progress in accessing the information world in

cyberspace, approximately 40% of internet users live in Europe and North America (Statista, 2024). In fact, the digital divide that will support the arguments of classical realists is a reality. Of course, cyberspace has a decentralizing and equalizing effect on states, but will it equalize power between countries? Based on these points and questions, realists can talk about a change of style rather than a transformation originating from cyberspace in world politics. On the other hand, in International Relations, cyberspace, as Choucri puts it, is a new area, but it is an area that traditional practices and theories cannot fully address in terms of conducting politics (Choucri, 2012: 9). In this context, when the cloth of realist theory is evaluated in terms of its basic assumptions, Choucri's argument will be confirmed. Firstly, according to realism, the assumption of being a holistic actor results in the resolution of the differences within the states in a way that allows them to speak with a single voice to the outside world and to be accepted as a single integrated unit against the world (Walker, 2011: 21-39). However, since the cyberspace has a multi-dimensional and multi-actor structure, this basic assumption of realism will not find a response. Another basic argument of realists is the understanding of national security on the level of national interest. Here, again, it is seen that many actors, from the security of individuals to the security of states, are the reference objects of security in cyberspace. At the same time, states cannot ensure their security with the assumptions of traditional security understandings.

The anarchy state of international relations, which is perhaps considered a cornerstone for realism, is quite important. Likewise, even if some theses change in different versions of realism, the anarchy phenomenon does not change. Non-state actors do not have much importance. When observed, the situation does not change for cyberspace either. There is no superior authority. All stakeholders can act freely within an anarchic structure. In other words, an anarchy environment is also valid for cyberspace. However, the most important actor is not only the state. Unlike realism, there are also companies and individuals in the anarchic environment. Cooperation between stakeholders is important for cyber awareness and security against attacks (Tarhan, 2017: 305).

As mentioned above in cyberspace, as in IR, the concept of anarchy is a determining factor. However, their meanings differ from each other. In IR anarchy does not mean an environment of chaos. Waltz defines anarchy as the determining principle of the international structure. Anarchy is the situation where there is no authority only over sovereign states (Waltz, 1979: 88-93). Based on these foundations, realists accept the concept of anarchy as a given in its definitions, where the state actor is the dominant and dominant actor in international relations. On the other hand, in IR, anarchy is a regulating principle between sovereign states, while in

cyberspace, it regulates the relationship between many actors. According to Choucri, cyber anarchy is described as a chaotic environment where states are relatively weak, where the individual, the state and the private sector coexist, and where there is no restrictive and superior authority (Choucri, 2012: 233-236). According to Akyeşilmen, cyberspace is more anarchic than the current physical international system. Because, as the author states, there are institutions in IR that will at least minimize or weaken international anarchy. However, there is no such situation in cyberspace (Akyeşilmen, 2018: 59). In addition, in cyberspace, unlike the single sovereign state actor structure of IR, there is a multi-centered or multi-actor complex structure. Due to this situation, the concept of anarchy has deepened even more with the large number of actors with different qualities in cyberspace.

Another important concept in evaluating the relationship between realism and cyberspace is the phenomenon of power, which also defines national interest. In realism, power is based on physical and material elements such as economy, military force, geographical location and population in the light of the above. Whereas in today's information and technology age, actors seem to resort to methods such as cyber espionage, cyber surveillance, cyber crimes, cyber attacks and cyber warfare to gain power in the international arena. Unlike physicality, cyberspace is man-made. Therefore, it can be changed by humans as Clarke and Kane stated (Clarke and Knake, 2019: 6). The fact that cyberspace is man-made, unlike other areas, changes geographical determination. Areas are no longer just physical structures that need to be dominated. The redesign of the conflict area by humans and its dynamic feature create a multi-layered and cyclical relationship in terms of the concept of power. There is a certain dimensional quality in land, sea and air areas. These areas are also a sovereignty area. Space is not included in this sovereignty area. However, all four areas have fixed qualities. Therefore, the actors who will be in conflict, the attack methods that can be applied, and the weapon capacity that will be effective are certain (Ulu, 2021: 324-343). Continuing from this context, the elements of power are different in both areas. For realists, the elements of power are military/political/strategic, but in cyberspace, power is information (Tarhan, 2016).

One of the essentials of ensuring security and preserving power in cyberspace is to ensure information security. The primary goal of information security is to protect the confidentiality, integrity and accessibility of information (Akyeşilmen, 2018: 13). Because information is, in a sense, the materialization of processed data (Tuomi, 1999:112). Today, cyber power is gaining meaning by states on a more military basis. Here, the cyber power in question stems from processing data with smart strategies and transforming it into artificial intelligence with intellectual capital and infrastructure. Ralph Langner defined cyber power as "Cyber power is

a society's organized capability to leverage digital technology for surveillance, exploitation, subversion, and coercion in international conflict" (Langner, 2016). According to him, a society wielding substantial cyber power can engage in a substantial number of actions: it can economically exploit or undermine other nations; gather political and military intelligence more efficiently than pre-digital espionage; interfere in foreign political discourse online, degrade an adversary's warfighting capabilities; sabotage critical infrastructure and industrial mass production, and even cause mass casualties. All of this can be done through the clever application of digital technology and without necessarily deploying military forces or human spies (Langner, 2016). According to Nye, "cyber power can be used to create desired results within cyberspace or to create desired results in other areas outside cyberspace by using cyber instruments." (Nye Jr., 2011: 123). Nye stated that cyber power can be used by an actor in the hard power or soft power categories if desired. For example, critical infrastructure attacks can be given as an example of hard power application. The ability of states or interest groups to change the preferences of the target actor through social media can be a good example of soft power application. As can be seen, cyber power cannot be measured with material capacities, as in realist theories.

Another traditional IR theory is neoliberalism. Neoliberal theories, like realist theories, see the state as the most fundamental actor in IR and consider power struggles and security as the most important issue in IR. However, unlike realist theories, they argue that the influence of the state has decreased with globalization and interdependence, while non-state actors continue their existence by becoming stronger alongside states (Keohane and Nye, 2011). States are increasingly entering into economic and political interdependence with each other in the globalizing world. On the other hand, states are in governance with non-state actors and multinational corporations in order to use their soft power. Liberals also state that the possibility of war will decrease through trade and economic interdependence (Heywood, 2011: 40-42). Neo-liberals also use the concept of anarchy in a way that is close to the definition of realist theories, but argue that in anarchy, states are in a governance between themselves and other actors, and that even in anarchy, states can cooperate to protect their own interests (Keohane and Nye, 2011:16, Kenneth, 1985:1).

In addition to the foundations they make on the pure power concept of realism, neoliberals have developed the concepts of soft power and smart power. Through soft power, an actor can aim to change the preferences of the other actor by creating attraction (Nye, 2004: 5-7). This attraction is provided by foreign policy, shared political values and culture (Nye, 2011: 83-84). Smart power is the use of soft power and hard power together (Nye, 2004: 32). However, it

thinks that the information universe in cyberspace will increase the role and function of democratic states. Liberal theories believe that there will be a change in the nature of relations between states with the spread of openness, transparency and democracy on this platform. While neorealists see cyberspace as a threat to state power, neoliberals see it as a multi-currency regime for collective governance or cooperation (Steinberg and McDowell, 2003: 216). Liberal theory, just like realists, gives the position of the main actor in world politics to states. However, questions regarding realism also come to mind for liberalism. Will the cyber platform really provide an open market environment? Will non-state actors continue to be active in cyberspace? How will international organizations, which are one of the basic concepts and assumptions of institutional liberalism in solving global problems and in the field of cyber governance, come into being? If they do, what will be the function of the organizations? Will there be a legal system that actors will comply with in cyberspace? (Akyeşilmen, 2018: 184). As can be seen, it is clear that the liberal approach needs to reconsider its theoretical framework within IR in terms of cyberspace.

In fact, liberal approaches can be a driving force in encouraging the development and dissemination of political and social ideas, the existence of civil society, and the development of transnational networks in terms of access to cyberspace. Liberal approaches can be applied to understand international efforts to keep the issue of interstate cooperation on cybersecurity, cyberspace governance, and arms control on the agenda (Eriksson and Giacomello, 2006: 230-233). In addition, liberalism can help explain the behavior of non-international state units such as civil society organizations, ethnic and national groups, cybercriminals, and cyberterrorism. Because, as Eriksson and Giacomello state, cyberspace offers significant communication and networking opportunities for humanity that are borderless and at the same time open to civil society. The cyberspace platform is a pertinent example of complex interdependence and integration through information, communication, and technology.

In addition to all these, the theory that draws the most harmonious portrait of cyberspace among traditional IR theories is constructivism. This theory claims that elements such as identity and culture affect a state's foreign policy. It is assumed that identity and international social structures are mutually constructed and that the outcome of this affects interests. Therefore, constructivism, unlike the two traditional approaches above, refers to social relations and argues that anarchy is also constructed as a result of a social structure (Wendt, 1999).

In terms of cyber space this theory thinks that cyber policies developed in cyberspace have the ground to transform international policies. So much so that, according to Nye and Welch, according to some constructivists, cyberspace brings about the end of the hierarchical

bureaucratic organization that emerged with the industrial revolution. Because this area, which brings a decentralized structure, goes beyond the boundaries of territorial sovereignty areas and develops its own governance mechanisms (Nye and Welch, 2011: 393). Therefore, constructivist theory, which seems more harmonious in terms of developing a cyber theory, should also take some questions as its basis in order to create its theoretical framework. For example, what kind of effect can cyberspace and cyber policies have on the transformation of identity, interests and norms?

All users of cyberspace exist with their identities in the same system with a method that transcends time and space. These actors, who are in communication with each other, affect the flow of history, the determination of the agenda, and the creation of perception on events and facts with the data they upload to the system. The cybersecurity problems of cyberspace, where international actors meet in the same system, lead states to play an active role in this system. The fact that states interact with individuals, groups, organizations and societies in the same universe pushes the discipline of International Relations to investigate the role of the identities and interactions of actors in changing the system. The norms, institutions or theories of the order to be established in cyberspace will be shaped by new approaches to be brought by different disciplines. In this context, while trying to understand perception in cyberspace, benefiting from different perspectives brought by constructivism will continue to contribute to the research on how cyberspace will shape the future of International Relations (Keskin, 2019; 150).

An Indispensable Thing for Cyber IR Theory: Terminology

Terminology is the tool that social scientists have to carry out their research and explain the results they have reached through it. However, when the social scientist moves on to the theory-building process after this first step, terminology (linguistics) becomes a problem. Therefore, terminology is also important for the theory that will be put forward on any political, economic and social issue. At this point, the conceptual or terminological framework should be established as the basis of the theoretical framework regarding cyber policies and cyberspace. Terminology work focuses on the definition of field-specific knowledge structures and how these are transferred in different communicative contexts (Sager, 1990). Therefore, terminology in particular should be considered as a set of linguistic (lexical) units expressing a specific specialized knowledge or field of activity concept that spontaneously takes shape during the emergence and development of a field (Helleklev, 2006). Therefore, terminology generally aims to provide the content of terms in certain fields, their organization and standardization, and the creation of terms for new subject areas. Starting from these points, terminology requires

a set of skills for a field of study. These are; i) the ability to determine terms that define concepts belonging to a subject area ii) the ability to verify the use of terms in a subject area iii) the ability to briefly define concepts iv) the ability to distinguish correct use from inappropriate use v) the ability to suggest or discourage certain uses in order to facilitate open communication and to establish effective communication and dialogue channels in the field of expertise (Condé, 1999: 1-22).

Conceptual infrastructures that can be referenced for knowledge accumulation come into play. Because the conceptual tools needed to classify existing data and make them meaningful also feed theoretical developments in a way. Because there is no integrity between the concept and the fact in the assumptions about social and political phenomena, there is no consistency either. Producing a theory of IR means associating conceptual tools with empirical observations. They believe that this can be achieved best when various conceptual tools are available (Jackson and Nexon, 2013: 550). Because the reality of the historical-political context becomes a knowledge production and element only through concepts. Realities or facts are systematically dressed in a consistent theory, approach and assumption patterns by means of concepts. With this set of concepts, it can have more disciplined communication and dialogue tools based on a common theoretical language and a common set of methods and evaluation standards based on a common meta-theoretical perspective.

In the relations between cyber policy and IR theories, a certain terminological arsenal has also begun to emerge. The first of these concepts is the unique anarchic nature of cyberspace. Just as the international system is read through anarchic nature, the nature of cyberspace is anarchic in terms of both the nature of action and the agency of the actors. Another conceptual arsenal is the issue of actors. As is known, the most important element in international politics is the issue of actors. In this context, although it is a matter of debate today, the international system continues to read a state-centered actor in IR. However, this is not the case in cyberspace. In today's world where cyberspace is rapidly globalizing, cyberspace is developing as a platform where asymmetric threats, conflicts and insecurity will be experienced violently, in the context of the actors and strategies it will bring to the international system. In short, cyberspace is a multi-actor system. Another conceptual arsenal that will feed IR theories within cyber policy is the issue of borders. Borders are flexible in this area. Therefore, cyberspace is the most powerful area that erodes the traditional security paradigm and questions the structures of nation states formed over borders.

Therefore, this conceptual arsenal will be of utmost importance in a cyber theory of IR to be developed through cyber policy. In relation to this, the concept that will be considered important

in developing a cyber theory of IR is sovereignty. Because, as mentioned before, non-state actors are stakeholders in governing on this platform. Again, conflict types originating from cyberspace differ in form from traditional conflict types. IR theories should be re-read in terms of tools, purposes and methods. In addition, conceptual issues such as cyber power and cyber deterrence should also be taken into consideration in a cyber theory of IR to be developed. These two basic concepts of IR are also important for actors when putting forward cyber policy in cyberspace. New power struggles and conflicts are possible in cyberspace devoid of any rule-maker. For this reason, every actor, especially the state, resorts to cyber defense or capacity-building power on this platform or can even form alliances in order to be strong. Theories that will affect new security and defense parameters can be produced through these concepts. Because this environment weakens the hierarchy both at the level of non-state actors and at the level of weak states and makes asymmetric power relations visible.

It is possible to say that the issues that cyber policy researchers in IR are most interested in regarding cyberspace are the points where cybersecurity overlaps with national and international security and the conflict and competition areas exemplified above. Especially following the end of the Cold War, the transformation of the perception of security and the replacement of conventional security and conflict elements with asymmetric elements increased the dimensions of relations and discussions regarding security. As far as can be observed, this has also created a cyber dimension in almost all political and military conflicts. In this context, how will the connections between cyberspace, cyberpolitics, international relations as a practice and IR as a discipline be established, what will be the perception and place of cyberspace as a space in IR, how is it possible to reduce cybersecurity to the perspective of international relations and study it within this discipline? How do classical IR theories and their followers interpret cyberspace and the developments stemming from it from a disciplinary perspective? What kind of dimensions does this field with its unique characteristics add to the discipline? Does the anarchic nature of cyberspace and the anarchic nature of IR have a structural effect on the discipline? How will cyberspace, which erodes borders and shortens time, affect the classical reading of IR based on sovereignty and territoriality? (Akyeşilmen, 2018: 174). Who are the actors, what are their actions and the outcomes of these actions? Who controls cyberspace, where, how and when? What are the types of cyber conflicts and the dimensions of cyber security? What are the types of management and governance in cyberspace? We can start evaluating IR in the cyber age with this set of terminological lenses. Any of these factors is important on its own, but together they provide an important holistic contribution to theory, policy and analysis. Of course, it is a fact that the characteristic features of international

relations and cyberspace are quite different from each other in terms of Temporality, Physicality, Permeation, Fluidity, Attribution and Accountability. Therefore, despite these differences, while establishing a theory of cyber-international relations, it is useful for IR advocates to focus on the following questions through these terminological arsenals.

Within this framework, it can be demonstrated that IR theories are compatible or incompatible with cyber policies and cyberspace, both through this terminological plane that has begun to become established and the research topics and questions in question. Of course, the effects of cyberspace on the discipline have only just begun. The issue of how international relations theories interpret cyberspace and whether their basic arguments in traditional international politics are now accepted by this field has begun to be discussed. Can cyberspace and the policies implemented in this field really transform international politics? The answers to the question that IR theories will give will also reveal whether they are compatible with the cyberspace environment.

Conclusion

The vast majority of discussions on cyberspace in IR are interpreted as a platform where social and political units/actors in this area carry out cyber actions against other units/actors. Again, when the cyber space literature in IR is examined in detail, it is stated that attacks and conflicts originating from this area erode traditional definitions of concepts such as deterrence, security and war and also change IR. Advocates of this idea generally argue that cyberspace has the potential to fundamentally change IR. In the information and technology age of the 21st century, it is indeed discussed that cyberspace has different notions of causality in the context of IR and shapes the actions and foreign policy practices of states in international relations. The literature on this subject has begun to develop theories about the conditions under which cyberspace and cyber policies derived from it are important in IR, how all types of actors effective in this field shape this field, and how cyberspace affects the interaction capacity of actors. This literature is certainly important in terms of the relationship between cyber space and IR, but it has not been able to eliminate two fundamental problems: the relative absence of cyber IR policies as a collective field of study and the fact that IR adherents ignore the politics and theoretical potential of further integrating cyber policies with IR theory and concepts. Most fundamentally, this study attempts to provide a solution to both problems. As emphasized earlier, the construction of the theoretical bridge between cyberspace, cyber policies and IR can be captured in the existing conceptual language to be shared. The study contributes to the literature on cyberspace and IR through cyber policies at three different levels. First, the study contributes to the discussions put forward that IR should be expanded in terms of scope, content and subject.

IR has generally ignored the issue of understanding and making sense of cyberspace and policies, which are a field. From this point on, if IR adherents show an interest in cyber spaces, they can produce theories and concepts that can reveal the empirical reality of social and political realities. Related to this, the second contribution of the study is to provide an awareness and a way to integrate cyber policies and cyberspace into IR as a collective field of study. Because when the literature on this subject is examined, the cyberspace-IR relationship is at risk of being theorized in disconnected ways through a small number of concepts (deterrence, foreign policy tools, etc.). Of course, examining certain developments reflected in the cyberspace or the effects of the cyberspace and the cyber policies of states does not fundamentally create a problem and is also beneficial. On the other hand, on a practical basis, this situation also carries the risk of IR followers who will work on cyber policies moving away from cyberspace and ignoring the collective effects of their research for IR. Discussions on cyberspace in IR have so far been far from a sustainable discussion on the nature or what cyberspace is and its impact on international relations. However, when the economic, political, social and cultural reflections reflected in cyberspace are conceptualized, it can be systematically and generalizably revealed how cyberspace causally affects IR. This conceptualization method can be functionalized in future studies in order to produce theoretical frameworks based on assumptions and inferences in the basic areas of IR. Finally, the research is also close to contributing to policy discussions. Political decision-makers will be able to take cyberspace and cyber policies more seriously through the connection that will be established between cyberspace and IR in the literature. The awareness that will be created in decision-makers regarding cyberspace will eliminate the situation of ignoring cyberspace or confining it to the area of low politics in IR.

References

Akdağ, Y. (2023). "Cyber-AI Technology and International Relations", *Cyberpolitik Journal*, http://cyberpolitikjournal.org/index.php/main/issue/view/16/18, Vol. 8, No. 16, pp. 149-152

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik*. Ankara: Orion Kitabevi

Avcı, Y. and Morçiçek, H. (2024). "Uluslararası İlişkilerde Yapı-Yapan Tartışması ve Eleştirel Gerçekçilik", *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Sayı: 54, s. 102-122.

Avcı, Y. (2024). "Thomas Hobbes ve Uluslararası İlişkiler: Realizm ile Rasyonalizm Arasındaki Leviathan", *Akademik Araştırmalar ve Çalışmalar Dergisi*, Cilt: 16, Sayı: 30, s. 99-120.

Avcı, Y. (2023). Uluslararası İlişkilerde İdealizm-Realizm Tartışması. M. Aksoy (Ed.). Orient Yayınları, Ankara, 55-109.

Bıçakçı, S. (2014). "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, Cilt 10, Sayı 40 (Kış 2014), s. 101-130.

https://www.cybercom.mil/About/History/

Buchanan, B. (2020). *The Hacker And The State: Cyber Attacks And The New Normal Of Geopolitics*. Harvard University Press.

Burton, J. (2013). "Small states and cyber security: The case of New Zealand". *Political Science*, 65(2), 216–238. https://doi.org/10.1177/0032318713508491

Choucri N. and Clark, R. (2019). *Cyberspace and International Relations: The Co-Evolution Dilemma Information Policy*, MIT Press.

Choucri, N. (2012). *Cyberpolitics in International Relations*. The MIT Press

Condé, V. (1999). *A Handbook of International Human Rights Terminology*. Lincoln: The University of Nebraska Press.

Drucker, P. (1994). *21. Yüzyıl için Yönetim Tartışmalar*, (Çev. İ. Bahqlvangil and G. Gorbon), İstanbul: Epsilon Yayıncılık.

Dunne T., Kurki M. and Smith Steve, (2013). *International Relations Theories: Discipline and Diversity*, Oxford University Press.

Eriksson, J. and Giacomello, G. (2006). "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", *International Political Science Review*, Vol. 27, No. 3. 221-244

Foulun, M. and Gustav, M. (2024). "How cyberspace affects international relations: The promise of structural modifiers". *Contemporary Security Policy*, 45(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Helleklev, C. (2006). *Metaphors and Terminology in Social Science A translation and an analysis*. http://www.diva-portal.org/smash/get/diva2:206838/FULLTEXT01

Heywood, A. (2011). *Global Politics*. Palgrave Macmillian

Jackson, P. T. and Nexon, D. H. (2013). International Theory in a Post-paradigmatic era: From Substantive Wagers to Scientific Ontologies. *European Journal of International Relations*, 19(3), 543-565.

Kello, L. (2022). *Striking Back: The End Of Peace in Cyberspace - And How To Restore İt*. Yale University Press.

Kenneth, O. A. (1985). "Explaining Cooperation under Anarchy: Hypotheses and Strategies". *World Politics*, 38 (1), 1-24.

Keohane, R. and Nye, J. S. (2011). *Power and Interdependence.* Pearson.

Kushner, D. (2013). 'The Real Story of Stuxnet', *IEEE Spectrum*, Vol. 50, No.3, 48-53 https://ieeexplore.ieee.org/document/6471059

Mearsheimer, J. (2001). *The Tragedy of Great Power Politics.* New York: W. W. Norton & Company Inc.

Meibauer, G. Desmaele, L., Onea, T., Kitchen, N., Foulon, M., Reichwein, A. And Sterling-Morgenthau, H. (1948). *Politics Among Nations: The Struggle for Power and Peace.* A. A. Knopf.

Nye, J. (2011). 'Nuclear Lessons for Cyber Security?', *Strategic Studies Quarterly*, Vol. 5, No.4, 18-38.

Ralph Langner https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security

Rid, T. (2012) "Think Again: Cyberwar", *Foreign Policy*, 192/81.

Rothkopf, D. (1998) 'Cyberpolitik: the changing nature of power in the information age', Journal of International Affairs, 51: 325-60.

Ruus, K. (2008). "Cyber War I: Estonia Attacked from Russia", *European Affairs*, Vol. 9, No,1,

Sager, J. (1990). *A Practical Course in Terminological Processing*. Amsterdam: John Benjamins Publishing Company.

Snyder, J. (2004). "One World, Rival Theories". *Foreign Policy*. November/December, No: 145, 53-62.

Steinberg, P. E., & McDowell, S. D. (2003). Global Communication and the Post-Statism of Cyberspace: A Spatial Constructivist View. *Review of International Political Economy*, *10*(2), 196–221. http://www.jstor.org/stable/4177458

Tarhan, K. (2017). "Siber Uzayda Realist Teorinin Değerlendirilmesi". *Cyberpolitik Journal*, Vol. 2, No. 3. 105-124.

Toffler, A. (1990). *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, New York: Bantham

Ulu, C. (2021). Uluslararası İlişkilerde Siber Güç ve Yapay Zekâ. Yapay Zekâ: Güncel Yaklaşım- lar ve Uygulamalar. N. Öykü İyigün ve Mustafa K. Yılmaz (Ed.). Beta Basım Yayım, İstanbul, 324-343.

Walker, S. G. (2011). *Rethinking Foreign Policy Analysis*, New York, Routlege.

Waltz, K. (1979). *Theory of International Politics*. Longman Higher Education

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge University Press

https://www.statista.com/studies-and-reports/digital-and-trends

CYBERSPACE AND NATION-STATE: REVISITING SOVEREIGNTY

Çağlar SÖKER♣

Orcid: 0000-0002-7162-3403

Abstract

This study deals with the issue of cyberspace's effects to the sovereignty of nation-state in international relations. First of all, the concept of sovereignty is revisited in IR by mentioning its evolution and definition, explaining its elements and conditions, addressing theories and approaches in short. Secondly, suppositions of "eroding sovereignty" are argued by explaining arguments of various theorists. After that, arguments of "cyberspace's strenghtening effects to state" and "strenghtening state in cyberspace" are evaluated. As a result, the question of whether cyberspace is strenghtening or weakening the state depend on what we mean by "sovereignty". It is concluded that while nation-state is not as "sovereign" as it was before in traditional means; because we still live in a state-centric international system, because states are adapting to changes in cyberspace day by day and because cyberspace is enabling states new tools to control and monitor, there is a risk of "state centralization" of cyberspace.

Key words: Cyberspace, nation-state, sovereignty, international relations.

Özet

Bu çalışma siber uzayın ulus-devletin egemenliğine etkilerini tartışmaktadır. İlk olarak gelişiminden ve tanımından bahsedilerek, bileşenlerine ve şartlarına değinilerek, teorilere ve yaklaşımlara değinilerek egemenlik kavramı ele alınmıştır. Ardından, siber uzayın devlet egemenliğini aşındırdığına dair argümanlar, farklı teorisyenlerin görüşlerine yer verilerek incelenmiştir. Son olarak, "siber uzayın devleti güçlendirici etkileri" ve "siber uzayda güçlenen devlet" savunuları değerlendirilmiştir. Sonuç olarak, siber uzayın egemen devleti güçlendirmesi ya da zayıflatması hususu egemenliğin nasıl tanımlandığına bağlıdır. Çalışmada, ulus-devletin –kavramın geleneksel anlamıyla- eskisi kadar "egemen" olmadığı; ancak devlet-merkezli bir uluslararası sistemde yaşadığımız, devletlerin siber uzaydaki değişikliklere her geçen gün daha iyi adapte olmaları ve siber uzayın devletlere izleme ve kontrol noktasında yeni araçlar sağlaması nedeniyle siber uzayın "devletleştirilmesi" riskinin bulunduğu sonucuna varılmıştır.

♣ Dr. Research Assist, Selçuk University, Department of International Relations, caglarsoker@selcuk.edu.tr

Anahtar kelimeler: Siber uzay, ulus-devlet, egemenlik, uluslararası ilişkiler.

Introduction

Sovereignty has been assumed as one of the fundamental principle of modern international relations which is attributed to nation-state. In relation to that, it has always been an important concept in International Relations (IR) since its establishment. While it seems a highly controversial concept in terms of its definition and scope, some theorists argue even its existence. When we look at the theoretical history of the discipline, we can see range of thoughts from Classical Realism to Poststructuralism. Realism which accepted as the oldest school in the discipline recognize "sovereignty" of nation-state and place it at the very center of international relations. However, in 1970's, with some developments and transformations in international system, sovereignty brought into question especially by liberal scholars. With the rising and strenghtening of constructivism and postmodern theories in 1980's, scholars of IR began to argue sovereignty with its "historical", "changeable" and "disciplining" characteristics.

Community of IR is discussing sovereignty in relation to the cyberspace along with the issues such as globalization, international organizations, human rights, environmental problems. Although there is an inclination to suppose cyberspace is eroding sovereignty of state, some theorists are emphasizing that it is too early to declare the weakening nation-state. This study deals with the issue of cyberspace's effects to the sovereignty of nation-state in international relations. First of all, the concept of sovereignty is revisited in IR by mentioning its evolution and definition, explaining its elements and conditions, addressing theories and approaches in short. Secondly, suppositions of "eroding sovereignty" are argued by explaining arguments of various theorists. After that, arguments of "cyberspace's strenghtening effects to state" and "strenghtening state in cyberspace" are evaluated.

1. What is Sovereignty?

Sovereignty and state are important terms in IR and in international politics both. The concepts of nation-state and sovereignty are central to the study and practice of international relations (Biersteker, 2006:157). And those two concepts are integrative and inseperable in modern international relations. In this context, sovereignty can be defined as "a doctrine that nation-states possess supreme authority and share chracteristics such as territory, authority and

recognition" externally (Jackson, 2013:542) and "the independent and unfettered power of state in its jurisdiction" internally (Weiss, 2016). It is assumed that sovereignty was identified to the nation-state in Westphalian System and no other actor can have this privilage.

Sovereignty, as a concept, was introduced us by Jean Bodin who defined it as "absolute and perpetual power" and in this case, the state is "the highest power of command" (Bodin, 2002:270). Even if this strict definition can be related to the age that Bodin lived, to be a "sovereign state" today, there are also conditions which agreed upon such as: (1) a fixed population, (2) living in a defined territory, (3) having a central government which (4) recognized by other governments (Maier, 1991:241). While those conditions needed juridically, nation-states practice their internal sovereignty by having monopoly of legitimate use of violence as a supreme authority in their territory (Strange, 1999:345) and external sovereignty by practicing two rules: "non-intervention" and "sovereign equality" (Aalberts, 2012:44).

Because it is one of the most used "words" in defining modern international relations, sovereignty has been one of the "founding" concepts of the discipline of IR since it has established. This situatiation can be related to the theoretical schools in the discipline. For example, the oldest tradition of the discipline, realism that is essentially state-centric and assumes the nation-state is the main actor in international politics, accept and use the concept of sovereignty without question (Lewis, 2013:1). However, the narrative of "absolute" sovereignty started to crumble with the recognition of states' coexistence with the transnational actors (Diez, et. al, 2011:217). With 1970's, factors such as globalization, human rights, international organizations, humanitarian intervention and environmental problems began to challenge the sovereignty of nation-state (Havercroft, 2011:37-38). These changes brought the rising of liberal and neoliberal theories in IR. But like realism, sovereignty is fundamental to the international system in liberal theories too and it belongs to the state (Neack, 2007:23).

In realism and liberalism, sovereignty is "given" and "ahistorical" concept. After 1980's, constructivist and postmodern theorists began to question this concept. According to those theorists, sovereignty is historically malleable rather than fixed concept that it was and can be reconceptualized (Prokhovik, 2008: 1-2). For instance, Stephan Krasner described sovereignty as "organized hypocracy" (Krasner, 1999). According to him, nation states' sovereignty has always been breached in history because principles of non-intervention and equality depend on political power rather than being realities. For Thomas Biersteker and Cynthia Weber, sovereignty is socially constructed and it has undergone important change and transformation

throughout history (Biersteker and Weber, 1996:13). The postmodern scholar R. B. J. Walker argued that sovereignty is one of meta-narratives[1] of IR that set binary pairs inside/outside and hierarchy/anarchy in dichotomical sense that serving to design and control the discipline (Walker, 2011).

As a result, sovereignty is a highly controversial concept in international relations. However, "sovereign" nation states are still "main" actors in international relations and in the foreseeable future, they seem to be stay so. The question that most of scholars in social sciences discuss today is whether sovereignty of state is weakening or strenghtening by various factors. For example, it is believed that, especially by liberal theorists, with the globalization, territoriality and rule-making authority of state are being eroded (Hudson, 2004:89). And with the new realities such as "cyberspace", it can be predicted that this discussion is going to widen and deepen.

2. Does Cyberspace Erode Sovereignty of State?: Not as "Sovereign" as It was Before

In 1996, John Perry Barlow, in his "Declaration of the Independence of Cyberspace", as a "person from cyberspace", drew a libertarian picture about cyberspace. He declared that, citizens of cyberspace's virtual selves immune to sovereignty even as they continue to consent to state's rule over their bodies (Barlow, 1996a). According to him, the internet is too widespread to be easily dominated by any single govenment. By creating a seamless global economic zone, borderless and regulatable, the internet calls into question the very idea of nation state (Barlow, 1996b). Although his prediction about the future of cyberspace viewed as "impossible future (Morrison, 2009)" by some scholars and seem "romantic" today, his arguments give us a point of view about early opinions related to cyberspace. Additionally, the question of if cyberspace erode/undermine/weaken the sovereignty of nation-state is still one of the frequently asked questions in IR recently.

Robert Jackson and Georg Sorensen pointed out that there are some activities that can bypass states and render the concept of sovereignty questionable in international relations: ever-

[1] Meta-narratives impose particular worldviews and advance political projects hidden behind a claim to nature and reason, as ideologies based on myths attempting to turn cultural particularities into universal truths (Berensköttter, 2017:7).

increasing international trade and investment; expanding multinational business activity; enlarged NGO activities; increasing regional and global communications; the growth of the internet; expanding and ever extending transportation networks; exploding travel and tourism; massive human migration; cumulative environmental pollution; expanded regional integration; the global expansion of science and technology; continuous downsizing of government; increased privatization (Jackson & Sorensen, 2013:27-28). Effects of those activities to the state and if state can adapt to these changes are fundamental questions in IR especially after Cold War. And as it can be seen, most of them are related to cyberspace implicitly or explicitly. Scholars who believe activities in cyberspace proceed to transcend to nation-state and there is no way for state to adapt to these changes conclude that cyberspace is going to continue to erode the sovereignty of state.

Theorists that claim cyberspace is undermining the sovereignty of nation state day by day focus on restricted effects of cyberspace to the state now that it empowers and enables individuals which is manifested through communication, expressed perceptions and organizations (Choucri, 2012:14). According to David Johnson and David Post, cyberspace cut across territorial borders and in the end weaken the sovereignty of state. Because cyber area constrains "sovereign" governments in terms of power to control over behaviour, legitimacy to enforce rules by destroying the link between territory and governing (Johnson & Post, 1999:3). According to Nezir Akyeşilmen, cyber space is weakening the sovereignty of nation-state because of its anarchical nature, absence of territoriality, anonimity, developing cyber threats and cyber conflicts, strenghtening of non-state actors, variety of asymetrical tools. And as a result, cyberspace challenges the patronizing status of nation-state (Akyeşilmen, 2018:187).

Stephan Kobrin argued that nation-state's unquestionable authority become problematic in that sovereignty is dispersing and getting decentralized over time (Kobrin, 2001). This dispersion and decentralization bring along new conceptual and theoretical approaches. For example governance is one of the most used concept to define cyberspace which require broader and more collective decision-making than in a nation-state and it refers new order that encompassing states and non-state actors; new geographic and functional entities in a power-sharing framework (Weber, 2015:105). So, state is not the sole authority to regulate and control in cyberspace, it is just an actor that is not as powerful as and as "sovereign" as in the physical realm.

So called "governance" in the postmodern world, according to Brian Loader, is characterized by the weakening of the nation-state through the accentuation of the local and global dimensions of human interaction (Loader, 2005:9). So sovereignty is being eroded from up and down both by cyberspace. As Susan Brener argued, sovereignty is becoming much less monolithic and more a matter of negotiation and coordination among lesser, perhaps more specialized entities (Brener, 2014:165). Governance theorists use various labels to name this "polycentric" composition of cyberspace and "networked governance", "new medievalism", "global issues networks", "moebious-web governance", "regime complex", "hypercollective action", "fragmented sovereignty", "quasi constitutionalism" or "new constitutionalism" are some of them (Scholte, 2017:165-184).

Although "governance" of cyberspace is a fact for now, governments are making plans to control and regulate cyberspace or at least trying to become more powerful in there. As Jan Lüdert noted that since they have realized the internet's potential threat to state control reaching in excess of its boundries, all countries –democratic or undemocratic- try to filter, regulate or censor the flow of information in the internet. While they have some success in restricting the flow of information in internet, as new forms of encryption and private networks are deployed, it is obvious that restricting, controlling and filtering are going to become more difficult (Lüdert, 2006:3). Because cyberspace is not territorial or territorially fixed system of rule and it is conditionally inclusive and anarchic in essence (Lüdert, 2006:3), states are not and can not be as "sovereign" as they do in physical international relations. However, these arguements are valid in terms of traditional meanings of sovereignty and if we think the concept in more complex framework we can reach new findings and understandings.

3. Toward a Cyber Sovereignty of Nation-State?: Beware of "State Centralization"

Understanding and defining sovereignty with its traditional meaning is misleading effort in 21st century. Because as it was explained above, traditional concept of sovereignty has never been practiced in international relations. For this reason, as Nazlı Choucri emphasized, sovereignty should be understood with complex logic. She argued that it is a multidimensional concept which can not be defined in territorial terms alone, and may extend beyond territorial bounds; so boundries, shape and qualifications of sovereignty can change (Choucri & Mathieu 2007:403) As a result, it is too early to accept that cyberspace is eroding and is going to weaken sovereignty of nation-state. There are some views hypothesizing that cyberspace provides new venues for state power, gives states new points of control and allows a focus on sovereignty

and territoriality as the ultimate principles on which to justify moves of choice in cyberspace (Choucri, 2012:14).

Jack Goldsmith and Tim Wu rejected the ideas that tell us cyberspace challenges to nation-state. To them, the internet's architecture had been shaped by the whims and obsessions of powerful governments in the United State, China, and Europe. And questions of internet governance had come to be chractarized by clashes among the great powers and their network ideologies (Goldsmith & Wu, 2006: vii, viii). Some scholars thought that states have shared interests in reducing risks from non-state actors, and have shown that sovereign states can work together to deal with challenges that cross borders (McDowell, Nensey & Steinberg, 2014:237). So, it can be inferred that cyberspace is or going to be state-centric. According to Joseph Nye, even if the cyber domain is likely to see an increase in the diffusion of power to non-state actors and network centrality, governments are still the strongest actors. He introduced us the "cyberpower" which is a new dimension to state power (Nye, 2011: 151).

For some theorists, so called concept "governance" has to be questioned in terms of its' decentralized connotations. Because, no matter how "decentralized" it is, the "governance" processes have to interact with the existing international system, national politicians and international organizations which take their authority from nation-states (Mueller, 2002:66-67). When we consider terms such as "cyber sovereignty" which are commonly used in recent years, we can see that cyberspace is not as "decentralized" as it seems. Protecting sovereignty in cyberspace is a task for any government to ensure their "national security" and they are claiming that "sovereignty" should be the guiding principle of cyberspace (Shen, 2016:90). According to Binxing Fang, cyber sovereignty is "natural" extention of state sovereignty in the cyberspace and that's why they continue to (try to) regulate activities in the cyberspace (Fang, 2018:52). And it can be inferred from his thoughts that they have a right to do it. However, "cyber sovereignty" is nothing but a "smoke screen" for the desires of states to monitor and control people to render "fundamentally fragment" internet to "ordered" or "organized" space (Schneier, 2016).

As Klaus Grewlich noted, governments are adopting to the challenges of information society and global network; and questioning long-standing administrative law and regulatory traditions (Grewlich, 1999:130). And this adaptation proceeds in practice, in theory, in discourse and in internet. Ronald Deibert explains the situation in more detailed way:

> "Whereas it was conventional wisdom to believe that the internet's technological infrastructure was immune to control, today states and corporations are applying on ever-increasing level of skill and technological sophistication to precisely that mission… Although it is true that the internet helped unleash non-territorial forces and flows that have helped redefine the landscape of global politics, the internet's architecture is now being hotly contested and an object of competing discources and practices of securitization… Just as the domains of land, sea, air and space have all been gradually colonized, militarized, and subject to interstate competition so too is the once relatively unencumbered domain of cyberspace (Deibert, 2009:333-334).

Conclusion

Since 1970's, lots of scholars from all branches of social sciences have argued the authority of nation-state in international relations. With the addition of the issues such as cyberspace, this discussion has broadened. Some have already declared the "end of nation-state" while others have claimed more moderate conclusions such as "eroding sovereignty of state". However, when modern history from 16-17. century is reviewed, gradual extention of the authority of nation-state can be seen. So it is too early to declare/predict/conclude the "weakening of nation-state". Thoughts that argue cyberspace is undermining "sovereignty of state" because it is borderless; because it contains obstacles to control, regulate or monitor; because it empowers individuals toward state are based on the traditional concept of "sovereignty". However, considering traditional sovereignty is based on territoriality and there is no "territory" in cyberspace, the relation between cyberspace and sovereignty become blurred. Even if it can not be denied that nation-state is not as "sovereign" as it was before in traditional meaning of the term, sovereignty and place of nation-state in international relations in relation to cyberspace should be analyzed in more profound and complex ways. Sovereignty is a malleable and multidimensional concept, it is being transformed depending on political/economic/social changes. That's why, connection between effects of cyberspace to the "sovereignty" of state can not be understood with traditional and basic meaning of the term.

States have the biggest capacity and facilities to adapt the changes of cyberspace. So rather than prejudgementally supposing the "weakening sovereignty" or "end of nation-state" we should try to understand changing dynamics that come along with cyberspace and beware of state's growing control over cyberspace. First of all, because we live in state-centric world, nothing can be free from state's influence. When we consider the terminology we use in terms of

cyberspace, we can see the concepts which are familiar to us from state-centric IR such as "cyber security", "cyber conflict", "cyber threats", "cyber anarchy", "cyber sovereignty" etc. Those concepts are creating ground to construct and (re)produce state-centric cyberspace like international relations. Secondly, it should not be forgotten that governments can adapt the challenges of cyberspace. States are growing their influences on cyberspace and considerations such as "cyberspace is going to end the supremacy of state" can make this process easier by distracting focus from "subject" issue and feeding "need for security" which refer to state. As a result states can have more proper grounds to improve their capacity to control and monitor day by day. They are also revising their regulatory mechanism, technical infrastructure and legislation. So, instead of asking cyberspace's effects to traditional sovereignty, focusing on changing features of sovereignty along with state's growing influence on cyberspace can lead us to more effective understanding.

References

Aalberts, Tanja E. (2012). *Constructing sovereignty between politics and law*. Oxon, The United Kingdom: Routledge.

Akyeşilmen, Nezir. (2018). *Disiplinerarası bir yaklaşımla siber politika & siber güvenlik*. Ankara, Turkey: Orion.

Barlow, John P. (1996a). Declaration of the independence of cyberspace. Retrieved from https://www.eff.org

Barlow, John P. (1996b). Thinking locally, acting globally. Retrieved from https://www.eff.org/pages/thinking-locally-acting-globally

Berensköttter, Felix. (2017). Deep theorizing in international relations. *European Journal of International Relations*, 24(4), 814-840.

Biersteker, Thomas J. & Cynthia Weber. (1996). The social construction of state sovereignty. In Thomas J. Biersteker & Cynthia Weber (Eds.), *State sovereignty as social construct* (pp. 1-21). Melbourne, Australia: Cambridge University Press.

Biersteker, Thomas J. (2006). State, sovereignty and territory. In Walter Carlsnaes, Thomas Risse & Beth A. Simmons (Eds.), *Handbook of international relations* (pp. 157-176). London, The United Kingdom: Sage Publications.

Bodin, Jean. (2002). From six books of the commonwealth. In Chris Brown, Terry Nardin & Nicholas Rengger (Eds.), *International relations in political thought: Texts form the Ancient Greeks to the First World War* (pp. 270-275). Cambridge, The United Kingdom: Cambridge University Press.

Brener, Susan W. (2014). *Cyberthreats and the decline of nation-state*. Oxon, The United Kingdom: Routledge.

Choucri, Nazli & Charlotte Matthieu. (2007). Basic versus complex logic in international relations. In Nazli Choucri et. al. (Eds.), *Mapping sustainability: Konwledge e-networking and the value chain*, Dordrecht, The Netherlands: Springer.

Choucri, Nazlı. (2012). *Cyberpolitics in international relations*. London, The United Kingdom: The MIT Press.

Deibert, Ronald J. (2009). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In Andrew Chadwick & Philip N. Howard (Eds.), *Routledge handbook of internet politics* (pp. 323-336). Oxon, The United Kingdom: Routledge.

Diez, Thomas, Ingvild Bode & Alexandra F. Da Costa. (2011). *Key concepts in international relations*. London, The United Kingdom: Sage Publications.

Fang, Binxing. (2018). *Cyberspace sovereignty: Reflections on building a community of common future in cyberspace*. Beijing, China: Science Press.

Goldsmith, Jack & Tim Wu. (2006). *Who controls the internet?: Illusions of borderless world.* Oxford, The United Kingdom: Oxford University Press.

Grewlich, Klaus W. (1999). *Governance in cyberspace: Access and public interest in global communications*, The Hague, The Netherlands: Kluwer Law International.

Havercroft, Jonathan. (2011). *Captives of sovereignty*. New York, USA: Cambridge University Press.

Hudson, Alan. (2004). Beyond the berders: Globalisation, sovereignty and extra-territoriality. In David Newman (Eds.), *Boundries, territory and postmodernity* (pp. 89-105), Oxon, United Kingdom: Frank Cass Publishers.

Jackson, Robert J. (2013). *Global politics in the 21st century*. New York, USA: Cambridge University Press.

Jackson, Robert J. & Georg Sorensen (2013). *Introduction to international relations: Theories and approaches*. Oxford, The United Kingdom: Oxford University Press.

Johnson, David R. & David G. Post. (1999). The rise of law on the global network. In Brian Kahin & Charles Nesson (Eds.), *Borders in cyberspace: Information policy and global information infrastructure* (pp. 3-47). London, The United Kingdom: The MIT Press.

Kobrin, Stephan J. (2001). Territoriality and the governance of cyberpsace. *Journal of International Business Studies*, 32(4), 687-704.

Krasner, Stephan D. (1999). *Sovereignty: Organized hypocracy*, Princeton, USA: Princeton University Press.

Lewis, Linden. (2013). Sovereignty, heterodoxy and the last desperate Shibboleth of Caribbean nationalism. In Linden Lewis (Eds.), *Caribbean sovereignty, development, and democracy in an age of globalization* (pp. 1-13). New York, USA: Routledge.

Loader, Brian D. (2005). The governance of cyberspace: Politics, technology and global restructuring. In Brian D. Loader (Eds.), *The governance of cyberspace: Politics, technology and global restructuring* (pp. 1-18). New York, USA: Routledge.

Lüdert, Jan. (2006). *Unbundling territoriality in the era of real time cyberspace*. Norderstedt, Germany: Grin Publishing.

Maier, Harold G. (1991). The principles of sovereignty, sovereign equality, and national self-determination. In Paul B. Stephan & Boris M. Klimko (Eds.*), International law and international security: Military and political dimensions* (pp. 241-255). New York, USA: M. E. Sharpe.

McDowell, Stephen D., Zoheb Nensey & Philip E. Steinberg. (2014). Cooperative international approaches to network security: Understanding and assessing OECD and ITU efforts to promote shared cybersecurity. In Jan-Frederick Kremer & Benedikt Müller (Eds.), *Cyberspace and international relations: Theory, prospects and challenges* (pp. 231-252). Berlin, Germany: Springer.

Morrison, Aimee H. (2009). An impossible future: John Perry Barlow's "declaration of the independence of cyberspace". *New Media & Society*, 11(1&2), 53-72.

Mueller, Milton L. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, ABD: MIT Press.

Neack, Laura. (2007). *Elusive security: States first, people last*. Lanham, USA: Rowman & Littlefield Publishers.

Nye, Joseph S. (2011). *The future of power*. New York, USA: Public Affairs.

Prokhovnik, Raia. (2008). *Sovereignty: History and theory*. Exeter, The United Kingdom: Imprint Academic.

Schneier, Bruce. (2016). *Data and goliath: The hidden battles to collect your data and control your world*, New York, USA: W. W. Norton & Company.

Scholte, Jan A. (2017). Polycentrism and democracy in internet governance. In Uta Kohl (Eds.), *The net and the nation state: Multidisciplinary perspectives on internet governance* (pp. 165-184), Cambridge, The United Kingdom: Cambridge University Press.

Shen, Yi. (2016). Cyber sovereignty and governance of global cyberspace. *Chinese Political Science Review*, 1(1), 81-93.

Strange, Susan. (1999). The Westfailure System. *The Review of International Studies*, 25(3), 345-354.

Walker, R.B.J. (2011). *Inside/outside: International relations as political theory*, Cambridge, The United Kingdom: Cambridge University Press.

Weber, Rolf H. (2015). *Realizing a new global cyberspace framework: Normative foundations and guiding principles*, Berlin, Germany: Springer.

Weiss, Thomas G. (2016). *Humanitarian intervention*. Cambridge, The United Kingdom: Polity Press.

AI AND CYBERSECURITY: NAVIGATING THE FUTURE OF WARFARE AND DIGITAL DEFENSE

Sarkis KARAGUEZIAN*

Orcid : 0009-0008-7575-329X

Abstract

The rapid advancements in artificial intelligence (AI) and cybersecurity are reshaping both military and civilian landscapes. This article explores the use of AI in distinguishing military targets and the inherent risks involved in its deployment, particularly regarding ethical issues, misidentifications, and accountability. It also delves into the role of cybersecurity in preventing cyberattacks, focusing on personal experiences in the field of security research. The article reflects on the transformative journey from offensive operations to educational efforts, emphasizing the growing importance of empowering individuals with the tools to protect themselves from cyber threats. The discovery of critical vulnerabilities in widely used software, like Microsoft Outlook, serves as a testament to the importance of ethical and practical measures in cybersecurity. This piece offers a comprehensive understanding of how technology intersects with security concerns and the potential consequences of its misuse in both military and civilian contexts.

Keywords: Artificial Intelligence (AI) in Warfare, Cybersecurity Threats, Ethical Implications of AI in Military, Advanced Military Technology, AI Target Recognition, Cyber Operations (Cyber Ops), Microsoft Outlook Vulnerability.

Methodology

This study employs a qualitative research design, incorporating case analyses, literature reviews, and expert interviews to explore the discovery of cybersecurity vulnerabilities and their ethical implications, as well as the role of AI in military and civilian security. A case study on the Microsoft Outlook vulnerability serves as a focal point, involving a document review of Microsoft's disclosure process and a comparative analysis with other vulnerabilities. Ethical considerations are assessed through a literature review and semi-structured interviews with cybersecurity professionals. Additionally, a systematic review of recent literature on AI technologies in military applications and discussions with experts provide insights into the intersection of AI and cybersecurity. Thematic analysis of qualitative data allows for the identification of key themes, contributing to a deeper understanding of responsible vulnerability disclosure practices and the challenges associated with integrating AI into security frameworks.

Introduction

The rapid development of artificial intelligence (AI) and cybersecurity technologies has had a profound impact on both military and civilian sectors. These technologies have enabled unprecedented advancements in warfare strategies, security systems, and digital communication. However, their integration into military and civilian applications is not without significant ethical challenges and potential risks.

AI, in particular, holds immense promise for revolutionizing military operations. Its ability to process vast amounts of data quickly and make real-time decisions has made it an invaluable tool for defense strategies. AI-powered systems are increasingly being used for target identification, surveillance, and autonomous weapons. Yet, the use of AI in military applications raises critical questions about the accuracy of target identification, the potential for misidentification, and the ethical implications of autonomous decision-making in life-or-death situations (Russell & Norvig, 2020).

In parallel, cybersecurity has become an essential component of modern security strategies, particularly as the digital landscape becomes increasingly vulnerable to malicious actors. With the rise of cyber warfare, the protection of critical infrastructure and national security systems has never been more crucial. Cybersecurity professionals work tirelessly to identify vulnerabilities in systems and protect against cyberattacks, often operating in high-stakes environments where a single oversight could have far-reaching consequences (Healey, 2013).

This article explores the dual themes of AI and cybersecurity, focusing on their applications in military contexts and their broader ethical implications. By drawing on personal experiences in the cybersecurity field, it also reflects on the professional journey from offensive cyber operations to more defensive, educational approaches. Additionally, the article highlights key cybersecurity incidents, such as the discovery of vulnerabilities in major software systems like Microsoft Outlook, underscoring the ongoing need for vigilance and ethical decision-making in the digital age (Schneier, 2019).

Physics Behind Waves and Military Applications

At the heart of understanding AI's role in military technologies lies a fundamental grasp of the physics that governs various forms of wave propagation, including sound waves. The transmission of sound waves through different mediums, for example, reveals how varying densities of materials can affect the speed at which waves travel (Kinsler et al., 2000). In

military applications, the behavior of these waves is integral to various technologies, such as sonar systems, communication devices, and advanced surveillance tools.

The fundamental principles of wave propagation highlight how denser mediums lead to faster transmission speeds; a concept that has been adapted in military technologies to optimize communication in challenging environments (Morse & Feshbach, 1953). Whether it is underwater sonar systems or air-based radar technologies, understanding the properties of wave behavior in different media is crucial for improving detection and communication systems in warfare. These technologies, in turn, rely on AI to enhance their effectiveness, whether it is identifying a submarine via sonar waves or interpreting radar signals from enemy aircraft.

While the foundational principles of wave transmission might seem distant from the daily concerns of military strategists, they play an integral role in the development of technologies that power modern warfare. The use of AI in interpreting these signals, making real-time decisions, and determining the precise nature of potential threats becomes ever more important as the complexity of warfare increases (Russell & Norvig, 2020).

Artificial Intelligence and Military Targeting

One of the most promising applications of AI in modern warfare is in the field of target recognition and identification. AI algorithms are increasingly being used to distinguish between various military targets, such as weapons systems, vehicles, and personnel. This capability can be vital for increasing the precision and efficiency of military operations, especially in scenarios where human decision-making might be slower or more prone to error (Botteldooren, 2018).

For example, AI-powered systems have been used to identify whether an object is a missile or a civilian object, such as a tripod (camera stand). This process, known as object recognition, involves using machine learning algorithms trained on large datasets to differentiate between various objects based on their shape, size, and other distinguishing features (LeCun et al., 2015). However, while the potential of AI in military targeting is significant, it raises important ethical and operational challenges.

One of the central concerns is the possibility of misidentification. AI systems may struggle to differentiate between objects that appear similar, such as a tripod and a missile. In a combat scenario, such a misidentification could lead to the destruction of a civilian object or a failure to engage a genuine threat. The consequences of such errors could be devastating, particularly if they result in unintended casualties or the destruction of valuable infrastructure (Amnesty International, 2019).

Additionally, there are concerns about the ethical implications of autonomous decision-making. If an AI system is responsible for determining whether to engage a target, it raises questions about accountability. Who is responsible for a decision made by a machine? What happens if that decision leads to the loss of innocent lives? These are difficult questions that demand careful consideration as AI becomes more integrated into military systems (Garnett, 2021).

The integration of AI into military targeting systems also presents a challenge in terms of programming. While AI systems can be trained to improve accuracy, they are not foolproof. There is always the possibility that the system will malfunction or fail to recognize an object accurately. This highlights the importance of constant testing, refinement, and oversight of AI systems to ensure they operate as intended and do not cause harm (Cummings, 2017).

Personal Experience in Cybersecurity: Shifting Focus

In addition to AI's applications in the military, the field of cybersecurity also plays a crucial role in modern security strategies. Cybersecurity professionals are tasked with identifying and mitigating risks to digital infrastructures, ensuring that systems remain secure from malicious actors. These professionals often work under immense pressure, facing threats from cybercriminals, hackers, and even state-sponsored actors (Kshetri, 2017).

The author of this article reflects on their own journey in the cybersecurity field, particularly their transition from offensive cybersecurity operations to educational efforts aimed at empowering others. Early in their career, the author was involved in "Cyber Ops" (Cyber Operations), which included targeting government, economic, and media entities. These operations, while intended to protect national security or counteract adversaries, often led to unintended consequences. The author describes how, despite their noble intentions, they realized that the operations they were involved in were not as effective as hoped and, in some cases, caused more harm than good (Holt et al., 2015).

This realization prompted the author to shift their focus. Instead of continuing in offensive operations, they decided to invest their skills in education, teaching others about the importance of offensive cybersecurity techniques. This change in direction marked a significant transformation in the author's professional life. Rather than using their skills to target others, they now sought to empower individuals to protect themselves from cyber threats (Nissenbaum, 2018).

This shift also reflects a broader trend within the cybersecurity community. As the risks and consequences of cyberattacks become more apparent, many cybersecurity professionals are moving away from offensive tactics and focusing on defense, education, and awareness. This

shift is essential, as it empowers individuals and organizations to take proactive steps in safeguarding their digital assets and data (Smith, 2020).

Discovering Vulnerabilities in Microsoft Outlook

One of the most significant moments in the author's career came when they discovered a critical vulnerability in Microsoft Outlook. Outlook is one of the most widely used email programs, with over 100 million users worldwide (Statista, 2021). The vulnerability the author discovered was particularly dangerous because it did not require user interaction to be exploited. Unlike many other types of malwares or cyberattacks, which require users to click on malicious links or download harmful files, this vulnerability allowed cybercriminals to exploit the system without any action on the part of the user (Chen et al., 2019).

The discovery of this vulnerability underscored the importance of ongoing research and vigilance in the cybersecurity field. Vulnerabilities like the one discovered in Outlook can go unnoticed for long periods, potentially affecting millions of users (CISA, 2022). The author worked closely with Microsoft to report the flaw, and the company acknowledged the discovery, recognizing its significance. The author's efforts were not only a personal achievement but also highlighted the broader need for cybersecurity researchers to identify and address such vulnerabilities (Verizon, 2021).

Challenges and Ethical Implications

The discovery of vulnerabilities in systems like Microsoft Outlook highlights the broader ethical issues in cybersecurity. While discovering and reporting vulnerabilities is an essential part of the job for many cybersecurity professionals, it raises questions about responsibility and accountability. When a vulnerability is discovered, should it be reported immediately, or should the researcher first assess the potential risks associated with its disclosure?

In the case of the Outlook vulnerability, the author chose to report the flaw to Microsoft, allowing the company time to address the issue before it was publicly disclosed. However, this decision was not without its own set of challenges. The author had to navigate the complexities of responsible disclosure, ensuring that the vulnerability was addressed before it could be exploited by malicious actors (Bishop & Gates, 2020). This process highlights the importance of ethical decision-making in cybersecurity, as well as the need for cooperation between researchers, organizations, and governments to mitigate cyber threats (Cavusoglu et al., 2020).

Conclusion: A Call to Action

As AI and cybersecurity continue to evolve, they will play increasingly significant roles in shaping both military operations and civilian security infrastructures. AI has the potential to revolutionize the way military forces identify and engage targets, enhancing operational efficiency and decision-making capabilities. However, its deployment must be handled with caution due to the ethical and operational challenges associated with AI in military applications, including potential biases, accountability issues, and the risk of unintended consequences (Lin et al., 2021). These challenges underscore the need for rigorous oversight and continuous improvement to ensure that AI systems are effectively managed and aligned with ethical standards. Furthermore, the integration of robust cybersecurity measures is essential to protect AI technologies and the data they rely on, ensuring resilience against cyber threats.

References

Amnesty International. (2019). Slaughter in Syria: The Use of Indiscriminate Weapons in Civilian Areas. Amnesty International.

Botteldooren, D. (2018). "Artificial Intelligence for Military Applications: Insights and Implementation". *Defence Science Journal*, 68(5), 457-463.

Bishop, M., & Gates, C. (2020). "The Ethics of Vulnerability Disclosure: A Case Study Approach". *IEEE Security & Privacy*, 18(4), 72-79.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2020). "The Role of Ethical Considerations in Vulnerability Disclosure". *Journal of Cybersecurity*, 6(1), 1-15.

Center for Internet Security (CISA). (2022). The Importance of Vulnerability Management in Cybersecurity. Retrieved from CISA.gov

Chen, Y., Gu, L., & Wang, Y. (2019). "Understanding The Impact of Zero-Day Vulnerability Promotions on Cybersecurity". *Web Intelligence*, 17(2), 91-101.

Cummings, M. L. (2017). "Artificial Intelligence and the Future of Warfare". *Strategic Studies Quarterly*, 11(3), 25-51.

Garnett, J. (2021). "Autonomous Weapons and the Future of Warfare: The Legal and Ethical Implications". *Naval War College Review*, 74(2), 1-25.

Healey, J. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

Holt, T. J., Blickle, W., & Byram, J. (2015). "Rethinking the Offensive Cyber Warfare Dilemma: From Simply "Hacker" to Serious Threat". *The RUSI Journal*, 160(2), 40-48.

Kinsler, L. E., Frey, A. R., Coppens, A. B., & Sanders, J. V. (2000). *Fundamentals of Acoustics* (4th ed.). John Wiley & Sons.

Kshetri, N. (2017). "Cybersecurity and Cybercrime: What the Information Society Should Know and Why". *Information & Computer Security*, 25(4), 386-398.

LeCun, Y., Bengio, Y., & Haffner, P. (2015). "Gradient-Based Learning Applied to Document Recognition". *Proceedings of the IEEE*, 86(11), 2278-2324.

Lin, P., Abney, K., & Bekey, G. (2021). *Robot Ethics: The Ethical and Social Implications of Robotics*. MIT Press.

Morse, P. M., & Feshbach, H. (1953). *Methods of Theoretical Physics*. McGraw-Hill.

Nissenbaum, H. (2018). "Digital Privacy and the Ethics of Surveillance: The Need for a New Cybersecurity Paradigm". *Ethics and Information Technology*, 20(3), 181-192.

Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

Schneier, B. (2019). *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World.* W. W. Norton & Company.

Smith, J. (2020). "Defensive Cybersecurity: Strategies and Practices for Modern Challenges". *Cybersecurity Review*, 6(1), 55-70.

Statista. (2021). Number of Microsoft Outlook Users Worldwide from 2012 to 2025. Retrieved from Statista.com

Verizon. (2021). Data Breach Investigations Report. Retrieved from Verizon.com

DIGITAL DIPLOMACY: THE TRNC'S STRUGGLE FOR RECOGNITION IN CYBERSPACE

Ramazan SAFA*

ORCID: 0000-0002-1629-5283

Abstract

This paper investigates the digital diplomacy initiatives of the Turkish Republic of Northern Cyprus (TRNC), focusing on its efforts to engage with the international community through online platforms despite lacking formal recognition. The TRNC's strategy includes official websites, social media presence, and advocacy groups. Official TRNC websites provide comprehensive information on governance, policies, and diplomatic activities, enhancing transparency. However, social media efforts are hindered by inactive English versions and outdated content, limiting global reach. Advocacy groups play vital roles in raising awareness and advocating for international recognition. These groups leverage social media to educate and mobilize support, emphasizing the Turkish Cypriot perspective on the Cyprus issue.

The study highlights the diplomatic efforts of TRNC President Ersin Tatar and advocates for a shift towards cyber diplomacy to enhance global presence, reduce diplomatic costs, and engage with the Turkish Cypriot diaspora. Challenges such as resource limitations, social media policies, and global skepticism persist but can be mitigated through strategic collaborations, particularly with Türkiye, and by amplifying the Turkish Cypriot narrative.

Keywords: TRNC, Political Recognition, Digital Diplomacy, Cyber Engagement, Advocacy Groups

Dijital Diplomasi: KKTC'nin Siber Alanda Tanınma Mücadelesi

Özet

Bu makale, Kuzey Kıbrıs Türk Cumhuriyeti'nin (KKTC) dijital diplomasi girişimlerini inceleyerek, resmi tanınma eksikliğine rağmen uluslararası toplumla çevrimiçi platformlar aracılığıyla etkileşim kurma çabalarına odaklanmaktadır. KKTC'nin stratejisi, resmi web siteleri, sosyal medya varlığı ve savunuculuk gruplarını içermektedir. Resmi KKTC web siteleri, yönetişim, politikalar ve diplomatik faaliyetler hakkında kapsamlı bilgiler sağlayarak

* PhD Candidate, Political Science and Public Administration, Adam Mickiewicz University, Poznan – Poland, Ramsaf1@amu.edu.pl

şeffaflığı artırmaktadır. Bununla birlikte, sosyal medya çabaları, İngilizce versiyonların aktif olmaması ve güncel olmayan içerik nedeniyle küresel erişimi sınırlamaktadır. Savunuculuk grupları, farkındalık yaratmada ve uluslararası tanınma için savunuculuk yapmada kritik roller oynamaktadır. Bu gruplar, sosyal medyayı kullanarak eğitim vermekte ve destek sağlamayı, Kıbrıs meselesinde Türk Kıbrıslı perspektifini vurgulamayı amaçlamaktadır.

Çalışma, KKTC Cumhurbaşkanı Ersin Tatar'ın diplomatik çabalarına dikkat çekmekte ve küresel varlığı artırmak, diplomatik maliyetleri azaltmak ve Türk Kıbrıslı diasporasıyla etkileşimi artırmak için siber diplomasiye geçişin gerekliliğini savunmaktadır. Kaynak kısıtlamaları, sosyal medya politikaları ve küresel şüphecilik gibi zorluklar devam etmektedir. Ancak, bu zorluklar özellikle Türkiye ile stratejik işbirlikleri ve Türk Kıbrıslı anlatının güçlendirilmesiyle hafifletilebilir. Sonuç olarak, KKTC'nin dijital diplomasi çabaları, uluslararası izolasyonu kırmayı ve Kıbrıs sorunu konusunda daha dengeli bir küresel anlayışı teşvik etmeyi hedeflemektedir.

Anahtar kelimeler: KKTC, siyasi tanınma, dijital diplomasi, siber iletişim, savunma grupları

Introduction

The Turkish Republic of Northern Cyprus (TRNC) was established on November 15, 1983, following significant geopolitical strife in the northeastern region of Cyprus (Isachenko, 2012). TRNC has faced international non-recognition and political isolation since its inception. In 1974, a coup d'état by Greek nationalists led to a military intervention by Türkiye, dividing the island into two distinct territories (Hannay, 2005).

In an era of rapid technological advancement, cyberspace plays a significant role in diplomacy by revolutionizing communication and information exchange (Dorn & Webb, 2008). Diplomatic missions and international organizations use digital platforms like email, social media, and video conferencing to engage in real-time dialogue and share official information with global audiences. This allows diplomats to maintain constant contact and respond swiftly to evolving situations. The digital landscape has revolutionized public diplomacy, allowing governments and diplomats to connect with foreign audiences directly through online platforms (Holmes, 2015). Social media tools like Twitter, Facebook, and Instagram facilitate direct communication, cultural exchange promotion, and national achievement showcasing. Digital advocacy campaigns use various multimedia formats to convey diplomatic messages effectively and shape perceptions on key policy issues. However, cyberspace also brings diplomatic challenges to cybersecurity. Diplomatic missions and government agencies face a range of cyber threats, emphasizing the need for strong cybersecurity measures to protect

sensitive communications and national interests. Cyberspace has become a platform for digital diplomacy initiatives focused on conflict resolution and peacebuilding (Lanz et al., 2021). Online dialogue forums, virtual peace negotiations, and collaborative digital platforms enable diplomatic engagement between conflicting parties in an interconnected world. As diplomats navigate the complexities of cyberspace, adherence to diplomatic protocol and ethical considerations remains paramount.

Understanding the TRNC's digital diplomacy efforts holds significant implications for its diplomatic standing, economic development, and prospects for international recognition. By examining the challenges encountered and proposing practical solutions, this study contributes to a deeper understanding of how unrecognized states navigate diplomatic complexities in the digital age. Furthermore, it offers insights into the broader trends in digital diplomacy relevant to unrecognized or partially recognized states, providing valuable lessons for policymakers and practitioners in the field. There is a universality phenomenon in cyberspace because all people living in the world are included in the unlimited area (Tarhan, 2017). Cyberspace disrupts the conventional understanding of sovereign nation-states by establishing a modern, tangible social contract rooted in the interconnected framework of hardware, firmware, and software. At the same time, it opens up fresh opportunities and avenues for advancement for some nations (Lancelot, 2020). So, there are unlimited opportunities for the unrecognized states with a new social contract.

This paper analyzes the strategies used by the TRNC in using cyberspace to promote its political and economic interests, despite lacking international recognition. It examines approaches such as social media campaigns, official websites, digital public relations, virtual events, e-government services, and cybersecurity measures to shed light on TRNC's efforts to engage with the global community.

The paper will focus on how the TRNC uses cyberspace for its objectives, including social media campaigns, digital public relations, and virtual diplomacy. It will explore challenges such as geopolitical resistance, resource constraints, and cybersecurity threats. Additionally, the paper will offer insights into the implications of the TRNC's digital diplomacy efforts for its diplomatic standing, economic development, and prospects for international recognition. Additionally, the paper explores practical solutions to address key challenges, including resource constraints, social media restrictions, and skepticism from global audiences.

The Unrecognized Status of the TRNC

The journey to the establishment of the Turkish Republic of Northern Cyprus (TRNC) is rooted in a history of conflict and aspirations for self-determination. During the period of British colonial rule from 1878 to 1960, Cyprus underwent a substantial change. The island, previously under the control of the Ottoman Empire, was leased to Britain and subsequently incorporated into British territory in 1925. The Greek Cypriot majority's desire for union with Greece (Enosis) was opposed by the Turkish Cypriots, who preferred either staying under British rule or splitting the island (Taksim). The period following independence witnessed growing tensions between the Greek and Turkish Cypriot communities. Upon gaining independence in 1960, Cyprus established a power-sharing government under a new constitution. Nevertheless, this delicate equilibrium deteriorated rapidly. President Makarios' suggested constitutional changes in 1963 sparked violence between the two communities. As a result, Turkish Cypriots disengaged from the government, leading to an informal division of the island. The situation became so unstable that UN peacekeepers were sent in 1964 to restore order. The situation escalated dramatically in 1974 when a coup d'état by Greek Cypriot nationalists, aimed at Enosis, prompted Turkey to intervene. On July 20, 1974, Turkey, invoking its rights as a guarantor power, launched a military operation to protect the Turkish Cypriot community. This intervention resulted in the occupation of the northern part of the island and significant population exchanges, with Greek Cypriots fleeing south and Turkish Cypriots moving north.

In reaction to these changes, Turkish Cypriots aimed to establish their self-governing status. This was made official on February 13, 1975, when they announced the establishment of the Turkish Federated State of Cyprus in order to express their wish for a federal resolution that would safeguard their security and political entitlements. Nevertheless, due to ongoing stalemate and little advancement towards a federal agreement, they took a more decisive action. The Turkish Republic of Northern Cyprus was established on November 15, 1983, following significant geopolitical strife in the northeastern region of Cyprus (Isachenko, 2012). Since its establishment, the TRNC has faced international non-recognition and political isolation. Despite numerous attempts to address the Cyprus problem through discussions and peace proposals, a comprehensive resolution remains difficult to attain. The island remains split, with the TRNC overseeing the northern region and the internationally acknowledged Republic of Cyprus governing the southern area. Turkish Cypriot views concentrate on attaining an equitable and enduring agreement that recognizes their rights and ambitions.

Since its establishment, TRNC is not recognized by the UN or most of the international community (Hoffmeister, 2006). The TRNC has its governmental structures and economy, but it heavily relies on Türkiye for support due to a lack of global recognition. Efforts by the United

Nations to resolve the Cyprus conflict have not led to a comprehensive settlement yet. The Republic of Cyprus's accession to the EU in 2004 complicated the TRNC's status due to the unresolved division (Hoffmeister, 2006). The unrecognized status brings significant geopolitical implications involving regional powers like Greece and Türkiye. Addressing the aspirations and concerns of both communities is crucial for a sustainable settlement.

Diplomatic isolation is a major challenge for entities like the TRNC due to a lack of formal recognition from the international community (Dolunay & Kasap, 2020). This leads to barriers to participating in forums, negotiating agreements, and engaging in diplomatic initiatives, limiting their influence on global affairs. Non-recognition compounds economic challenges and development obstacles for unrecognized entities, leading to limited access to international financial institutions, foreign aid, and investment opportunities. This hinders regions like the TRNC from achieving economic growth, reducing poverty, and promoting sustainable development. Additionally, it results in restricted market access, trade limitations, and financial sanctions that perpetuate cycles of dependency and underdevelopment (Peksen, 2023). The lack of international recognition also creates legal ambiguity and juridical uncertainty within unrecognized territories' governance structures and legal frameworks. Entities like the TRNC face legal uncertainty and lack international oversight, which undermines stability, erodes confidence in institutions, and hinders efforts to establish effective governance (Grzybowski, 2019). Non-recognition exacerbates human rights concerns and humanitarian challenges within unrecognized territories. Humanitarian assistance and relief efforts may face challenges due to logistical constraints, funding shortages, and political obstacles. These factors worsen vulnerabilities and exacerbate humanitarian crises. Lack of recognition contributes to geopolitical tensions and conflict dynamics in contested regions, perpetuating cycles of instability and insecurity. Unresolved territorial disputes, competing sovereignty claims, and geopolitical rivalries fuel inter-state tensions and regional instability, posing risks to peace and security (Söderbaum & Hettne, 2016). Entities like the TRNC remain ensnared in protracted conflicts without formal recognition or diplomatic engagement, hampering peacebuilding efforts due to entrenched divisions and competing interests.

Cyberspace as a Platform for Recognition

In the international sphere, the information revolution emerged in the 2000s. Throughout the information age, there was an optimistic dialogue about how knowledge would drive the progress of nations (Tarhan, 2022). Technological developments, especially in the field of information and communication, have forced those carrying out diplomatic activities to shift to

cyberspace and the digital world (Orhon, 2022). International relations are becoming increasingly complex and intricate with each passing day. As a result, traditional strategies and policies may sometimes prove ineffective. A key feature of the international system is that it is structured around the physical borders and jurisdictions of states. In contrast, cyberspace is decentralized and anarchic, lacking clear boundaries, jurisdiction, or a single dominant actor shaping the system at a global level (Akyeşilmen, 2016). Digital diplomacy involves the use of digital technologies and communication platforms by various diplomatic actors to engage with foreign audiences and pursue diplomatic objectives in the online space (Manor, 2017). It includes activities such as advocacy, public diplomacy, cybersecurity, and conflict resolution, significantly influencing modern international relations.

Digital diplomacy uses digital technologies like social media, websites, email, and video conferencing to improve diplomatic communication and engagement (Bjola & Holmes, 2015). It includes public diplomacy, cultural diplomacy, economic diplomacy, and crisis communication, and involves official and unofficial diplomatic actors. Digital diplomacy enables real-time communication and information exchange between diplomatic actors, foreign governments, and global audiences, transcending geographical barriers (Adesina, 2017). It empowers diplomats to engage directly with foreign publics and promote national interests through targeted messaging and interactive strategies. This plays a crucial role in crisis response and conflict resolution efforts by coordinating humanitarian assistance, disseminating timely information, and engaging in virtual negotiations to promote dialogue in conflict-affected regions. Digital platforms facilitate cultural exchange, educational programs, and people-to-people diplomacy. They contribute to building social networks and projecting influence through digital storytelling, cultural initiatives, and virtual exchange programs (Formica et al., 2021). In addition to these roles, in an era of increasing cyber threats, digital diplomacy efforts also focus on safeguarding diplomatic communications and mitigating cybersecurity risks through encryption protocols, intelligence sharing, and cooperation. Furthermore, digital technologies enable multilateral diplomacy by providing virtual platforms for international conferences, summit meetings, and diplomatic negotiations which help diplomats collaborate on transnational challenges (Adesina, 2017). Digital diplomacy reaches beyond traditional diplomatic channels to involve diaspora communities, non-governmental organizations, and civil society actors. It utilizes online networks and social media advocacy campaigns to gather support for diplomatic initiatives and amplify marginalized voices on the global stage. In our modern, interconnected world, digital diplomacy is essential for diplomats, governments, and international organizations to handle the intricacies of global relations. Using digital

technologies and social media platforms, enables better communication, public engagement, crisis response, cultural exchange, cybersecurity cooperation & multilateral diplomacy. This redefines diplomatic practice in the digital age (Jay, 2018). In recent years, Ministries of Foreign Affairs have accelerated the digitalization of diplomacy. So much so that even digital embassies have started to be established. Denmark has opened a digital embassy to facilitate communication between the government and major technology companies such as Facebook, Google, Apple, Twitter, and Amazon (Kaplan, 2021).

Cyberspace offers unrecognized states new opportunities to engage with global audiences and further their interests, despite lacking formal international recognition (Shen, 2016). By strategically using digital technologies and online platforms, these states can navigate diplomatic limitations and amplify their voices in the digital domain. Unrecognized states can use cyberspace for global diplomatic outreach and advocacy efforts through social media, official websites, virtual conferences, and other digital platforms to disseminate information, share perspectives, and connect with foreign governments as well as civil society actors. By strategically implementing digital diplomacy efforts, unrecognized territories can increase awareness about their goals, gain international backing, and influence public opinion on the world stage. The online realm provides a space for promoting culture and projecting soft power for these entities (Iosifidis & Wheeler, 2016). Utilizing digital narratives, cultural exchange initiatives, and virtual exhibitions allows unrecognized states to highlight their heritage, customs, and accomplishments to global viewership (Selmanović et al., 2020). This fosters mutual understanding between cultures and cultivates favorable perceptions internationally. By using digital media and creative content, unrecognized states can increase their influence and visibility in the digital age. Cyberspace supports economic development and investment promotion in unrecognized states (Sauer, 2014). Digital platforms enable e-commerce, online entrepreneurship, and virtual trade initiatives, providing access to global markets, attracting foreign investment, and stimulating economic growth (Ablyazov & Rapgof, 2019). Leveraging digital technologies for economic diversification, innovation, and job creation helps unrecognized states mitigate diplomatic isolation's adverse effects while enhancing resilience against economic challenges (Solberg et al., 2020). Unrecognized states can use cyberspace for virtual diplomacy and conflict resolution. Online forums, negotiations, and mediation platforms provide channels for diplomatic engagement and trust-building between conflicting parties (Doelker, 1989). By facilitating virtual interactions, unrecognized states can mitigate tensions and explore solutions to conflicts, paving the way for sustainable peace in contested regions (Bramsen & Hagemann, 2021). Cyberspace allows unrecognized states to gather humanitarian

aid and organize crisis response efforts during emergencies. Online platforms help with fundraising, emergency appeals, and relief initiatives, enabling these states to mobilize resources, coordinate assistance efforts, and support vulnerable populations affected by conflicts or natural disasters (Hoskins, 2020). Through digital networks and social media engagement, unrecognized states can improve their ability to handle humanitarian crises and ease suffering in regions facing crises.,

In conclusion, cyberspace provides unrecognized states with new opportunities to assert their presence, engage globally, and pursue diplomatic objectives in the digital age. By leveraging digital technologies and online platforms, unrecognized states can overcome constraints and advance their interests on the international stage. Despite challenges, strategic use of cyberspace can empower unrecognized states to navigate diplomatic complexities and contribute to peace, stability, and development in contested regions worldwide.

Digital Lobbying: TRNC and Cyber Advocacy

The TRNC has taken steps to use the Internet for diplomatic purposes, even without formal international recognition. In its early efforts in digital diplomacy, the TRNC has concentrated on using online tools and platforms to improve communication, connect with global audiences, and advocate for its interests internationally (Isachenko, 2012). The TRNC government institutions' official websites offer detailed information about its governance, policies, and diplomatic efforts. Visitors can find official documents, press releases, and statements from TRNC authorities to promote transparency in the digital realm. The websites acts as central platforms for domestic and international stakeholders to stay informed about the TRNC's governance and diplomatic activities. For example, the TRNC Presidency's official website provides updates on events, diplomatic initiatives, documents, reports, and publications. The TRNC Presidency website provides a wide array of documents and sections aimed at educating the public and international stakeholders about the historical, political, and economic dimensions of the TRNC. It presents comprehensive details on the "Cyprus Issue," offering a historical analysis from 1960 to 2016 that chronicles major events and advancements. The site showcases "Joint Statements of Leaders" as evidence of cooperative diplomatic initiatives, along with segments dedicated to the "United Nations" and "Security Council Resolutions," emphasizing global engagements and influential decisions affecting the TRNC. Additionally, the website provides information about the "European Union," including details about relationships and regulatory measures such as the "Direct Trade Regulation," "Financial Aid Regulation," and "Green Line Regulation Council Decision." It also discusses compliance with

the "Copenhagen Criteria" and "Maastricht Criteria," which are crucial for understanding the TRNC's adherence to European standards. The section on "Presidential Publications" contains various reports and documents issued by the presidency, while "100 Days at the Presidency" offers insights into the initial achievements and initiatives of the administration. This extensive collection of documents illustrates TRNC's commitment to transparency, articulation of its position on critical issues, and interaction with the global community through digital diplomacy. It also provides detailed information regards to President's daily activities and international trips (TRNC Presidency, 2024).

The TRNC has a presence on significant social media platforms like Facebook and Twitter. However, various factors greatly hinder the effectiveness of these platforms in fostering global acknowledgment. The inactive English versions of their websites restrict accessibility for non-Turkish speakers. Furthermore, there has been no recent activity on Twitter since 2017 and the last post on Facebook dates to 2019. Additionally, its absence from Instagram is noteworthy as this platform holds substantial importance for digital interaction and outreach efforts. The lack of activity and outdated material on the TRNC's social media profiles indicates a deficiency in strategic planning and resource management for maintaining a strong digital presence. It is essential to have active and consistently updated social media accounts for effectively connecting with global audiences, distributing information, and influencing public opinions. The absence of recent content suggests that the TRNC has missed chances to convey its story, exhibit its culture, and spotlight its accomplishments to an international audience. English is the lingua franca of international diplomacy, and having an active, well-maintained English-language digital presence is essential for effectively communicating with the global community. The TRNC's failure to use Instagram and TikTok highlights its limited utilization of digital resources. Instagram is especially useful for visually narrating stories, engaging with younger demographics, and promoting cultural diplomacy. By not making use of Instagram, the TRNC overlooks chances to visually showcase its cultural legacy, natural landscapes, and social progressions, which could aid in creating a favorable international image.

The Young Turkish Cypriots (YTC) is an international collective dedicated to educating the public about the history and contemporary issues of Cyprus. YTC platform plays a significant role in advocating for international recognition of the TRNC. Operating across multiple social media platforms, including Facebook, X (formerly Twitter), Instagram, and TikTok, YTC focuses on educating about Cyprus's history and current issues. It promotes a two-state solution and Turkish Cypriot independence while highlighting President Ersin Tatar's efforts in advocating this stance internationally. Additionally, YTC aims to raise awareness about the

hardships experienced during the war period in Cyprus to foster empathy among global audiences. The name 'Young Turkish Cypriots' is influenced by the Young Turks movement from the Ottoman Empire and criticizes support for EOKA in South Cyprus as it suggests that coexistence is unfeasible. YTC promotes the direct flights from UK to Northern Cyprus through an online petition. It is a strategic initiative that significantly contributes to the international recognition of the TRNC. By leveraging cyberspace, YTC can mobilize global support, raising awareness about the political and economic isolation faced by the TRNC. This digital activism facilitates broader engagement with international audiences, including the Turkish Cypriot diaspora and global allies, fostering a sense of community and collective effort. Comprised of young Turkish Cypriots from around the globe, including regions such as the UK, Türkiye, Australia, and the United States, YTC's mission extends beyond education. It seeks to reconnect the Turkish Cypriot diaspora with their cultural roots and identity while fostering a sense of community and visibility for Turkish Cypriots. Through their posts and educational content, YTC aspires not only to inform but also to unite and empower the Turkish Cypriot community worldwide. Despite its unofficial status, YTC effectively educates an international audience about TRNC's position and historical context with content available exclusively in English. However, challenges such as maintaining consistent engagement and broader collaboration are encountered but deemed necessary to maximize impact through digital diplomacy efforts (Young Turkish Cypriots, 2024).

'North Cyprus Exists' (NCE) is a group dedicated to promoting and preserving the cultural identity of Turkish Cypriots. Initially formed as a lobbying group, it has evolved into a platform aiming to reach a wider audience and highlight the struggles of the Turkish Cypriot community on X (Twitter), Facebook, Instagram, and their website. The organization advocates for the Turkish Cypriot community through letter-writing campaigns and engagement with influential stakeholders to challenge discriminatory policies, focusing on ending international isolation and economic embargoes imposed on the TRNC. North Cyprus Exists was created to address the international community's treatment of Turkish Cypriots. The organization aims to promote and highlight the struggles of Turkish Cypriots, preserving and recognizing their cultural identity while ensuring that their voice is heard. The main goal of NCE is to work towards a TRNC that is free from embargoes and international isolation (North Cyprus Exist, 2024). Despite its significant past contributions, NCE has been inactive on Instagram, Twitter, and its website since 2022. This lack of recent activity suggests that the organization is not currently active in its advocacy efforts. Additionally, it operates independently without support from the TRNC government, reflecting its grassroots nature. While its inactivity may limit its current

impact, the organization's past actions remain a testament to the determination of Turkish Cypriots to confront suppression and demand recognition, highlighting the importance of continued efforts towards a more equitable future.

Another advocacy group is Freedom and Fairness for Northern Cyprus, dedicated to promoting the recognition of the TRNC as a sovereign, independent, and democratic nation state equal in opportunity, rights, and status to the Greek Cypriot South. The organization highlights historic injustices faced by Turkish Cypriots and advocates for international recognition for TRNC through a two-state solution endorsed by President Ersin Tatar in 2020 (Freedom And Fairness For Northern Cyprus , 2024). The organization runs a media center that disseminates news, reports, and summaries of annual meetings to offer valuable insights into the current status and advancements in TRNC. They actively engage in advocacy by correspondingly with UK and UN officials concerning TRNC issues, as well as arranging lobbying activities to gain backing for their objectives. The group also maintains a strong presence on social media platforms such as Twitter and Facebook, where they share information and rally support for their initiatives. Their endeavors are focused on addressing past injustices and striving for international recognition and equality for Turkish Cypriots through advocating for a two-state solution that aims to bring lasting peace and stability to the island.

Similarly, Embargoed! is a human rights group working to end the international isolation of North Cyprus and restore the political, economic, and social rights of the Turkish Cypriot people. Founded in September 2004 by Bulent Osman, Gulfem Veziroglu, and Ipek Ozerim with twenty initial signatories, it has since grown into a formidable force with thousands of supporters. Operating as an independent non-profit membership association primarily from London, Embargoed! mobilizes non-violent action through peaceful means to raise awareness about the plight of Turkish Cypriots and advocate for change. They aim to facilitate democratic dialogue between both sides without endorsing any specific political solution for Cyprus. Ultimately motivated by a commitment to human rights and justice for all, Embargoed! seeks to end unjust isolation imposed on the people of North Cyprus (EMBARGOED, 2024). Embargoed! differs in its focus on championing the rights of Turkish Cypriots and working to eliminate international isolation against North Cyprus from a human rights standpoint, rather than adopting a nationalist position. In contrast to other groups, it abstains from supporting or advocating for any particular peace proposal, instead maintaining an impartial stance as it seeks justice and equality for the Turkish Cypriot community.

Not as an advocacy group but as a media entity CyprusScene.com is a platform dedicated to advocating for the recognition of the TRNC. The platform aims to draw attention to the actions

of international entities like the UN, EU, UK, and others in maintaining the current state of the Cyprus Issue and not providing international acknowledgment and fairness to the TRNC. Its main goal is to advocate for TRNC rights, shed light on the continuing difficulties encountered by the Turkish Cypriot community, and ultimately work toward a fairer resolution of the Cyprus Issue (Cyprusscene, 2024).

TRNC President Ersin Tatar has made extensive diplomatic efforts, involving visits to various countries such as Türkiye, Gambia, Australia, Germany, the USA, the UK, Azerbaijan and Kyrgyzstan. Despite the considerable physical and financial demands of these trips highlighting their significance; there is a need to prioritize utilizing online platforms for many interactions in order to minimize these challenges. While certain events like the Organization of Islamic Cooperation's 15th Summit in Gambia or meetings with potential recognizing states like Azerbaijan and Kyrgyzstan require in-person participation; numerous other engagements could be efficiently conducted online.

Cyber initiatives offer a cost-efficient and effective option for upholding diplomatic ties and advancing the international acknowledgment of the TRNC (Cucos, 2012). But cyberspace is becoming more competitive, fragmented, and chaotic. Similar to the physical world, order in cyberspace does not emerge on its own (Barrinha & Renard, 2020). Engaging with local entities, communities, universities, and conferences in Türkiye can take place using virtual channels. This strategy not only saves resources but also enhances the scope and regularity of diplomatic endeavors. This reality makes digital diplomacy more appealing to governments, Ministries of Foreign Affairs, and embassies for promoting their activities, as it does not strain their budgets (Rashica, 2018). By forming a specialized government body for leading cyber diplomacy efforts, the TRNC could develop a lasting and influential online profile.

Investing in cyber diplomacy could also enable ongoing interaction with the Turkish Cypriot diaspora in the UK and Australia, along with other important global participants. Employing virtual meetings and webinars can guarantee consistent engagement and backing from the diaspora, promoting deeper connections and collaborative initiatives for acknowledgment. Additionally, a specialized cyber diplomacy entity could assist scholars and researchers concentrating on TRNC-related concerns by offering funding and materials to advance scholarly endeavors that support recognition of TRNC while addressing its imposed isolation policies. The strategic utilization of online platforms can increase the TRNC's presence and impact on global stages. By executing well-planned digital campaigns, engaging in social media interactions, and participating in virtual events, the TRNC is able to efficiently convey its story, exhibit its cultural legacy, and emphasize its political ambitions to an international audience.

This online visibility has the potential to draw attention from international media outlets, shape public perceptions, and establish partnerships with supportive countries and organizations (Adesina, 2017).

Ultimately, although President Tatar's individual diplomatic trips are praiseworthy, a coordinated and united approach to cyber diplomacy has the potential to increase the TRNC's influence on the world stage. By reallocating resources to establish a strong cyber strategy, the TRNC can pursue a more enduring and influential route toward global recognition and an end to isolation policies. This tactical change not only conforms with contemporary diplomatic norms but also guarantees that the TRNC's pursuit of recognition receives backing from a comprehensive and cooperative endeavor.

Challenges for TRNC in Cyberspace

Unrecognized states encounter numerous difficulties as they strive to practice digital diplomacy, seeking to interact with the global community despite not having official recognition (Ker-Lindsay, 2015). The lack of formal acknowledgment from other nations presents a significant challenge to the success of digital diplomacy for unrecognized states. This absence of diplomatic status hinders their participation in international forums and discussions, severely limiting their use of digital communication as a diplomatic tool. The absence of recognition reduces their impact on world events and constrains their involvement in diplomatic activities, weakening the effectiveness of digital outreach efforts. Proposals can be suggested to address the challenges stemming from TRNC's lack of global recognition in the realm of digital diplomacy. Despite not being officially recognized as a state internationally, the President of the TRNC can continue these efforts under the title of "Leader of the Turkish Cypriot Community" (Duckett, 2010). For instance, in negotiations regarding the Cyprus issue, the President of the TRNC participates as the leader of the Turkish Cypriot community and leads the discussions. This approach enables the TRNC to effectively engage in digital diplomacy, taking into account its non-recognition status. The President of the TRNC, acting as the leader of the Turkish Cypriot community, can represent the Cyprus issue on international platforms and advocate for the TRNC's position. Consequently, the TRNC can maintain its presence on the international stage, effectively utilizing digital channels to advance its interests. Unrecognized states frequently face challenges due to a lack of financial and technical resources, which hinders their ability to establish and sustain a strong online diplomatic representation (Ker-Lindsay, 2015). Insufficient funding and expertise make it difficult for these entities to effectively compete in the digital sphere, limiting their capacity to promote

their perspectives and narratives (Nielsen & Cherubini, 2022). The resource disparity exacerbates existing diplomatic inequalities, further marginalizing some states in the digital sphere (Norris, 2001). While it's true that unrecognized states like TRNC often face constraints in terms of financial and technical resources, it's important to consider the support they receive from other entities, particularly in the case of TRNC, Türkiye has consistently provided comprehensive support across various domains, and it's reasonable to assume that this support extends to the realm of digital diplomacy as well. TRNC policymakers could potentially alleviate their resource limitations by initiating a project aimed at increasing visibility in digital diplomacy and seeking assistance from Türkiye. TRNC could leverage Türkiye's expertise and resources to mitigate economic challenges by collaborating on initiatives to enhance digital diplomacy efforts. Additionally, the utilization of digital diplomacy could lead to a reduction in the need for physical diplomatic travel, resulting in cost savings (Adesina, 2017). These cost savings could then be reallocated to establish a dedicated budget for further advancements in digital diplomacy. Therefore, while resource constraints may pose challenges, strategic collaboration with supportive entities like Türkiye and the efficient use of digital platforms offer viable solutions for enhancing TRNC's presence and effectiveness in digital diplomacy.

The policies of social media platforms can limit the portrayal of unrecognized states, making it difficult for them to use these channels for diplomatic communication (Ker-Lindsay, 2018). Entities that are not officially recognized must carefully work within these restrictions, weighing their wish to connect with global audiences against the possibility of censorship by the platform. Restrictions on online engagement hinder their capacity to communicate their messages and influence public opinion, thereby restricting their digital diplomacy efforts. While it's acknowledged that social media platforms may impose certain restrictions on the representation of non-recognized entities, such as limitations on using location data or national flags, these constraints do not significantly hinder the TRNC from enhancing its effectiveness in digital diplomacy. Despite these minor issues, the TRNC can still leverage social media platforms to effectively communicate its diplomatic messages and engage with international audiences. The restrictions imposed by social media platforms may pose challenges, but they do not fundamentally undermine the TRNC's ability to expand its digital diplomatic outreach.

Unrecognized states face a major obstacle in persuading global audiences and official decision-makers (Toomla, 2016). Lacking formal diplomatic recognition, these entities encounter difficulties in attracting attention and obtaining reactions from important stakeholders, hindering their ability to advocate for their interests and pursue their goals. In the case of the TRNC, the primary reason for this skepticism is the lobbying and diplomatic efforts conducted

by the Greek Cypriot side. As a recognized state in Cyprus, the statements and warnings issued by the Greek Cypriot side are often regarded as more credible by the international community. Therefore, one crucial step that the TRNC needs to take is to provide a stronger response to these efforts by the Greek Cypriot side. The Cyprus issue should be presented more from the perspective of the Turkish Cypriots, both in the digital world and in diplomatic efforts.

In conclusion, unrecognized states such as the TRNC encounter various obstacles in digital diplomacy due to their lack of formal acknowledgment. Nevertheless, there exist practical methods to surmount these challenges. Although traditional states persist in their pursuit of power and security, they often work to identify the most effective resolution to a conflict through multilateral diplomacy (Verrekia, 2017). Using the position of the TRNC President as the "Leader of the Turkish Cypriot Community" and actively engaging in diplomatic dialogues can enable the TRNC to effectively utilize digital platforms to advocate for its interests internationally. Additionally, strategic partnerships with supportive entities like Türkiye can help mitigate resource constraints and bolster digital diplomacy endeavors. Despite encountering limitations on social media platforms and skepticism from global audiences, the TRNC can address these hurdles by concentrating on amplifying its diplomatic messages and presenting a perspective of the Cyprus issue from that of the Turkish Cypriots.

Conclusion

In summary, the Turkish Republic of Northern Cyprus encounters considerable difficulties arising from its lack of recognition in the global community. Although it was founded in 1983 and has since progressed in governance and economic aspects, the TRNC still struggles with isolation on diplomatic fronts, financial limitations, and intricate geopolitical circumstances. The separation of Cyprus in 1974 as a result of a coup d'état and subsequent military involvement led to long-standing tensions and impeded endeavors for a comprehensive resolution.

In addressing these difficulties, the TRNC is trying to adopt digital diplomacy as a strategy to advance its political and economic objectives worldwide. Through utilizing diverse online platforms such as official websites, social media channels, and digital advocacy organizations, the TRNC aims to interact with global audiences, influence narratives, and promote recognition and equality. Nevertheless, deficiencies like inactive social media accounts and restricted multilingual communication impede the impact of these endeavors. Despite these challenges, grassroots advocacy organizations such as the Young Turkish Cypriots, North Cyprus Exists, Freedom and Fairness for Northern Cyprus, Embargoed!, and CyprusScene.com are essential

in promoting the TRNC's viewpoint and defending the rights of Turkish Cypriots. Using online activism, they garner support, raise consciousness, and confront unjust policies while emphasizing the strength and persistence of the Turkish Cypriot population.

President Ersin Tatar's extensive diplomatic travels are praiseworthy; however, the TRNC must modernize its approach by embracing cyber diplomacy. Leveraging online platforms provides a cost-effective method to maintain diplomatic relationships and further the TRNC's pursuit of international recognition. Establishing a specialized government department for cyber diplomacy would enable the TRNC to cultivate a strong online presence that complements traditional diplomatic endeavors. Investing in digital initiatives ensures continual engagement with important stakeholders, such as the Turkish Cypriot diaspora and global academics, fostering deeper connections and cooperative efforts. Thoughtful online campaigns and virtual gatherings can effectively present the TRNC's perspective, garner international media attention, and form partnerships with sympathetic nations.

Moving forward, the TRNC needs to focus on improving its digital diplomacy strategy by enhancing its social media engagement, broadening multilingual communication efforts, and utilizing visual storytelling platforms such as Instagram and TikTok. Furthermore, increased collaboration between the TRNC government and grassroots advocacy groups has the potential to enhance their combined influence and bolster the TRNC's standing in global affairs. The ongoing dedication to promoting the rights and acknowledgment of Turkish Cypriots is highlighted by the combined actions of government bodies, advocacy organizations, and diaspora communities. Utilizing digital diplomacy and working together collaboratively will enable the TRNC to address diplomatic obstacles and facilitate discussions towards a fairer future for Turkish Cypriots in Cyprus.

REFERENCES

Ablyazov, T., & Rapgof, V. (2019). Digital platforms as the basis of a new ecological system of socio-economic development. In IOP Conference Series Materials Science and Engineering (Vol. 497, p. 12002). IOP Publishing. https://doi.org/10.1088/1757-899x/497/1/012002

Adesina, O S. (2017, January 1). Foreign policy in an era of digital diplomacy. https://doi.org/10.1080/23311886.2017.1297175

Akyeşilmen, N. (2016). Cybersecurity and human rights: Need for a paradigm shift? Cyberpolitik Journal, 1(1), Summer 2016

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. International Affairs, 96(3), 749–766. https://doi.org/10.1093/ia/iiz274

Bjola, C., & Holmes, M. (2015, March 24). Digital Diplomacy. https://doi.org/10.4324/9781315730844

Bramsen, I., & Hagemann, A. (2021). The missing sense of peace: diplomatic approachment and virtualization during the COVID-19 lockdown. In International Affairs (Vol. 97, Issue 2, p. 539). Oxford University Press. https://doi.org/10.1093/ia/iiaa229

Cucos, R. (2012, November 13). Virtual diplomacy – a new way of conducting international affairs?.https://blogs.worldbank.org/digital-development/virtual-diplomacy-a-new-way-of-conducting-international-affairs

Cyprusscene. (2024, 05 26). cyprusscene.com. Retrieved from About CyprusScene: https://cyprusscene.com/about/

Dolunay, A., & Kasap, F. (2020, July 23). Still Unrecognized State "Turkish Republic of Northern Cyprus" in the Context of the Cyprus Negotiations: Status of the TRNC' Court Decisions. https://doi.org/10.5539/jpl.v13n3p1

Doelker, R. E. (1989). Mediation in academia: Practicing what we preach. In Mediation Quarterly (Vol. 7, Issue 2, p. 157). Wiley. https://doi.org/10.1002/crq.3900070207

Dorn, A W., & Webb, S. (2008, August 13). Cyberpeacekeeping: New Ways to Prevent and Manage Cyberattacks. https://www.walterdorn.net/273

Duckett, B. (2010). Historical Dictionary of Cyprus. In Reference Reviews (Vol. 24, Issue 7, p. 61). Emerald Publishing Limited. https://doi.org/10.1108/09504121011077516

EMBARGOED. (2024, 05 26). Who We Are - EMBARGOED! - Campaigning for Turkish Cypriots, Embargoed since 1964. Retrieved from embargoed.org: https://www.embargoed.org/about/

Kaplan E., "Politik Psikoloji Bağlamında Diplomaside Dijital Dönüşüm: Antalya Diplomasi Forumu," Cyberpolitik Journal, Vol. 6, No. 11 (2021)

Freedom And Faırness For Northern Cyprus . (2024, 05 26). Freedom and Faırness for Northern Cyprus Has One Aim. Retrieved from freedom-and-fairness: https://freedom-and-fairness.org/about/

Formica, E., Kavanagh, C., Lanz, D., & Eleiba, A. (2021, June 9). Social media in peace mediation: a practical framework - World. https://reliefweb.int/report/world/social-media-peace-mediation-practical-framework

Grzybowski, J. (2019, October 8). The paradox of state identification:de factostates, recognition, and the (re-)production of the international. https://doi.org/10.1017/s1752971919000113

Hannay, D. (2005, January 1). Cyprus: The Search for Solution

Hoffmeister, F. (2006, July 1). Legal Aspects of the Cyprus Problem. https://doi.org/10.1163/ej.9789004152236.i-290

Holmes, C B M. (2015, March 27). Digital Diplomacy | Theory and Practice | Corneliu Bjola, Marcus Holme. https://www.taylorfrancis.com/books/edit/10.4324/9781315730844/digital-diplomacy-corneliu-bjola-marcus-holmes

Hoskins, A. (2020, April 1). Media and compassion after digital war: Why digital media haven't transformed responses to human suffering in contemporary conflict. https://doi.org/10.1017/s1816383121000102

Isachenko, D. (2012, January 1). The Making of Informal States. https://doi.org/10.1057/9780230392069

Iosifidis, P., & Wheeler, M. (2016). Public Diplomacy 2.0 and the Social Media. In Palgrave Macmillan UK eBooks (p. 149). Palgrave Macmillan. https://doi.org/10.1057/978-1-137-41030-6_7

Jay, R. (2018, February 13). Digital Diplomacy: From Tactics to Strategy | Richard C. Holbrooke Publication. https://www.americanacademy.de/digital-diplomacy-tactics-strategy/

Ker-Lindsay, J. (2015, March 1). Engagement without recognition: the limits of diplomatic interaction with contested states. https://doi.org/10.1111/1468-2346.12234

Ker-Lindsay, J. (2018, July 23). The Stigmatisation of de facto States: Disapproval and 'Engagement without Recognition'. https://doi.org/10.1080/17449057.2018.1495363

Lancelot, J. F. (2020). The deconstruction of nation-state power and the materialization of cyber-states. Cyberpolitik Journal, 5(9), July 13, 2020

Lanz, D., Eleiba, A., Formica, E., & Kavanagh, C. (2021, June 7). Social Media in Peace Mediation: A Practical Framework. https://edoc.unibas.ch/83433/

Manor, I. (2017, January 1). The Digitalization of Diplomacy- Toward Clarification of a Fractured Terminology. https://www.academia.edu/34179587/Digital_Diplomacy_Working_Paper_The_Digitalization_of_Diplomacy_Toward_Clarification_of_a_Fractured_Terminology

Nielsen, R. K., & Cherubini, F. (2022). Born in the Fire: What We Can Learn from How Digital Publishers in the Global South Approach Platforms.

https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-10/Nielsen_%20and_Cherubini_Born_in_the_Fire.pdf
Norris, P. (2001). Digital Divide. https://doi.org/10.1017/cbo9781139164887
North Cyprus Exist. (2024, 05 26). North Cyprus Exists. Retrieved from Who we are: https://www.north-cyprus-exists.com/about-us/who-we-are
Orhon, Ö. (2022). Geleneksel diplomasiden siber diplomasiye geçiş: Aktörler ve süreçler. Cyberpolitik Journal, 7(14), Winter 2022.
Peksen, D. (2023, June 23). The human right effect of economic sanctions. https://www.eastasiaforum.org/2023/06/23/the-human-right-effect-of-economic-sanctions/
Rashica, V. (2018). The benefits and risks of digital diplomacy. SEEU Review, 13(1), 75. https://doi.org/10.2478/seeur-2018-0008
Sauer, N. (2014, January 14). The politics of getting online in countries that don't exist. https://theconversation.com/the-politics-of-getting-online-in-countries-that-dont-exist-21399
Seki, T., Çimen, F., & Dilmaç, B. (2023). The effect of emotional intelligence on cybersecurity: The mediator role of mindfulness [Duygusal zekânın siber güvenliğe etkisi: Bilinçli farkındalığın aracı rolü]. Bartın University Journal of Faculty of Education, 12(1), 190–199. https://doi.org/10.14686/buefad.1040614
Selmanović, E., Rizvić, S., Harvey, C., Bošković, D., Hulusić, V., Chahin, M., & Šljivo, S. (2020). Improving Accessibility to Intangible Cultural Heritage Preservation Using Virtual Reality. Journal on Computing and Cultural Heritage (Vol. 13, Issue 2, p. 1). https://doi.org/10.1145/3377143
Shen, Y. (2016, March 1). Cyber Sovereignty and the Governance of Global Cyberspace. https://doi.org/10.1007/s41111-016-0002-6
Solberg, E., Traavik, L. E. M., & Wong, S. I. (2020). Digital Mindsets: Recognizing and Leveraging Individual Beliefs for Digital Transformation. In California Management Review (Vol. 62, Issue 4, p. 105). SAGE Publishing. https://doi.org/10.1177/0008125620931839
Söderbaum, F., & Hettne, B. (2016, April 1). Regional Security in a Global Perspective. https://doi.org/10.4324/9781315566115-8
Tarhan, K. (2017). Siber Uzayda Realist Teorinin Değerlendirilmesi [Evaluation Of Realist Theory In Cyberspace].Cyberpolitik Journal, 2(3), 1-17, http://cyberpolitikjournal.org/index.php/main/article/view/66
Tarhan, K. (2022). Historical development of cybersecurity studies: A literature review and its place in security studies. Przegląd Strategiczny, 15, 1-23. https://doi.org/10.14746/ps.2022.1.23

Toomla, R. (2016, September 1). Charting informal engagement between de facto states: a quantitative analysis. https://doi.org/10.1080/13562576.2016.1243037

TRNC Presidency. (2024, 05 25). Presidency of the Turkish Republic of Northern Cyprus. Retrieved from KTTCB: https://www.kktcb.org/tr

Verrekia, B. (2017). Digital diplomacy and its effect on international relations. Independent Study Project (ISP) Collection, (2596). https://digitalcollections.sit.edu/isp_collection/2596

Young Turkish Cypriots. (2024, 05 24). https://youngturkishcypriots.org/social-media/. Retrieved from youngturkishcypriots: https://youngturkishcypriots.org/

YAPAY SİNİR AĞLARI İLE GÜÇLENEN GÜVENLİK STRATEJİLERİ: MODERN GÜVENLİK YÖNETİMİNDE YAPAY ZEKÂNIN ROLÜ VE ETKİLERİ

Yasin TURNA[*]

Orcid: 0000-0003-2153-2797

Kaan Doğan ERDOĞAN[**]

Orcid: 0000-0002-8552-7965

Nurettin DOĞAN[***]

Orcid: 0000-0002-8267-8469

Özet

Modern güvenlik anlayışı, geleneksel askerî tehditlerin ötesine geçerek çok boyutlu ve karmaşık riskleri içermektedir. Bu çalışma, değişen güvenlik riskleri karşısında yapay zekâ ile özellikle yapay sinir ağlarının güvenlik stratejilerinde kullanımını ve bunun etik, yasal ve toplumsal etkilerini ele almaktır. Literatür incelemesi ve çeşitli uygulama örneklerine dayanan araştırma, yapay zekânın büyük veri analizi, tahmin ve gözetim yetenekleriyle kamu güvenliği, asayiş ve askerî operasyonlarda proaktif çözümler sunduğunu ortaya koymaktadır. Yapay zekâ tabanlı teknolojilerin güvenlik alanlarında verimliliği artırırken, otoriter rejimlerde toplumsal alanın kontrolünü kolaylaştırıcı rolü de vurgulanmıştır. Güvenlikte dönüştürücü rolü büyük olan yapay zekâ ve yapay sinir ağları teknolojilerinde kullanılan büyük veri setleri ile kullanıcıların önyargılı tutumlarından kaynaklanan manipülasyon, veri önyargısı ve mahremiyet ihlalleri, düzenli denetim ve mevzuat düzenlemelerinin gerekliliğini ortaya koymaktadır. Çalışma, disiplinlerarası işbirliği ve şeffaf veri yönetimi sayesinde, güvenlik ile özgürlük arasında sağlıklı denge kurmanın mümkün olduğunu göstermektedir.♣

Anahtar kelimeler: Güvenlik Stratejileri, Yapay Zeka, Yapay Sinir Ağları, Proaktif Risk Yönetimi, Mahremiyet ve Etik Düzenlemeler

[*] Dr. Öğretim Üyesi, Bandırma Onyedi Eylül Üniversitesi, E-mail: yasinturna@bandirma.edu.tr

[**] Öğr. Gör., Selçuk Üniversitesi, E-mail: kaan.erdogan@selcuk.edu.tr

[***] Prof. Dr., Selçuk Üniversitesi, E-Mail: nurettin.dogan@selcuk.edu.tr

♣ Bu çalışmada, Yasin TURNA kavramsallaştırma, yöntem, düzenleme, özgün taslak yazımı, gözden geçirme ve yapay zekâ kavramının güvenlik bağlamında ilişkilendirilmesi konularında değerli katkılar sağlamıştır. Kaan Doğan ERDOĞAN, kavramsallaştırma, yöntem, gözden geçirme süreçlerinin yanı sıra yapay zekâ teknolojilerinin güvenlik stratejileri üzerindeki etkilerini analiz ederek çalışmaya önemli katkılarda bulunmuştur. Nurettin DOĞAN ise yapay zekâ, yapay zekâ uygulamaları ve alt dallarıyla ilgili danışmanlık sağlamış; kavramsallaştırma sürecine uzman görüşleriyle destek olmuştur.

SECURITY STRATEGIES EMPOWERED BY ARTIFICIAL NEURAL NETWORKS: THE ROLE AND IMPACTS OF ARTIFICIAL INTELLIGENCE IN MODERN SECURITY MANAGEMENT

Abstract

The modern understanding of security extends beyond traditional military threats to encompass multidimensional and complex risks. This study examines the use of artificial intelligence (AI), particularly artificial neural networks (ANNs), in security strategies and explores their ethical, legal, and societal implications. Based on a literature review and various application examples, the research highlights how AI, with its capabilities in big data analysis, prediction, and surveillance, provides proactive solutions in public safety, law enforcement, and military operations. While AI-based technologies enhance efficiency in security domains, their potential role in facilitating societal control in authoritarian regimes is also emphasized. The transformative role of AI and ANN technologies in security is underscored by the challenges of manipulation, data bias, and privacy violations arising from the use of large datasets and user biases, highlighting the necessity for regular oversight and regulatory frameworks. The study demonstrates that a balanced approach between security and liberty is achievable through interdisciplinary collaboration and transparent data management practices.

Keywords: Security Strategies, Artificial Intelligence, Artificial Neural Networks, Proactive Risk Management, Privacy and Ethical Regulations

Giriş

Güvenlik kavramı, tarih boyunca politik ve toplumsal dinamiklere göre değişim geçirmiştir. Başlangıçta askeri savunma odaklı güvenlik politikaları, günümüzde ulusal sınırların ötesine geçerek bireylerden dünya çapına kadar geniş bir çerçeveyi kapsamaktadır. Bu değişim, modern toplumların karşı karşıya kaldığı tehditlerin çeşitlenmesi ve karmaşıklaşmasıyla doğrudan ilintilidir. Her ne kadar güvenlik stratejileri, ulus devletlerin sınırlarını ve egemenliğini korumak üzerine kurgulansa da günümüzde güvenlik tehditlerinin askeri saldırılarla sınırlı kalmayıp; terörizm, salgın hastalıklar, siber saldırılar ve çevresel felaketler gibi giderek artan küresel tehditleri de barındırmaktadır. Bu nedenle, güvenlik alanında daha geniş ölçekli yaklaşımlar benimsenerek askeri stratejilere ek olarak disiplinlerarası ve küresel işbirliğine dayanan daha kapsamlı bir yaklaşım benimsenmiştir.

20. yüzyılın sonlarından itibaren teknolojik ilerlemeler ile devlet dışı aktörlerin güvenlik algısını dönüştürmesi, risklerin önlenmesi için güvenlik stratejilerindeki değişimi gerekli kılmıştır. Küreselleşme ve dijitalleşmenin hız kazanmasıyla birlikte klasik güvenlikçi yaklaşımın ötesine geçen yenilikçi ve teknoloji tabanlı güvenlik çözümleri geliştirilmiştir. Bu

süreçte, devletlerin güvenlik politikalarında, yapay zekâ (YZ) ve yapay sinir ağları (YSA) gibi teknolojik araçların güvenlik stratejilerine dahil edilmesi ile yeni bir dönem başlamıştır. YZ destekli güvenlik uygulamaları, gelişen güvenlik tehditlerini hızlı analiz eden ve etkili müdahale imkanları sağlama yeteneğine sahip güvenlik sistemlerini destekleyerek yeni bir dönemi başlatmıştır. Örneğin, yüz tanıma sistemleri, koku detektörleri ve siber güvenlik çözümleri gibi YZ tabanlı uygulamalar ile güvenlik hizmetleri sunumunda verimliliği artırmıştır.

Geleneksel güvenlik anlayışından farklı olarak YZ destekli uygulamalar, büyük veri analizi ve makine öğrenimi algoritmalarını kullanarak büyük veri kümelerini yorumlama ve tehdit eğilimlerini tahmin etme kabiliyetini geliştirmektedir. Bu sayede, YSA insan hatalarından kaynaklanan handikapları azaltarak daha etkin ve hızlı çözümlemeler yapılmasını güçlendirmektedir. Ayrıca yalnızca olayların reaktif değil, riskleri önceden öngörme ve proaktif bir müdahale imkânı da sunmaktadır. YZ destekli güvenlik kameraları ve geçmiş olaylardan hareketle öngörücü güvenlik önerileri sunan YSA uygulamaları ile tehditler henüz gerçekleşmeden önlenebilmektedir. Nitekim YZ destekli güvenlik sistemleri kaynakların daha etkili kullanılarak güvenlikleştirme süreçlerine katkı sağladığı görülmektedir.

Bu çalışmada araştırmanın temel problemi, YZ ve YSA teknolojilerinin güvenlik sahasında giderek yaygınlaşmasının avantajlarını kadar etik, yasal ve toplumsal etkilerine de odaklanmaktadır. Bu teknolojiler, gözetim ve verimlilikte önemli katkılar sağlasa manipülasyon, veri önyargısı ve mahremiyet ihlalleri gibi sorunları da beraberinde getirmektedir. YZ ve YSA teknolojilerinin geleneksel güvenlik stratejilerini yeniden şekillendirerek daha etkili ve verimli hâle getirdiğini dünyadaki örnekleri ile analiz edilmesiyle, modern güvenlik sorunlarına hangi çözümlerin sunulduğunu incelenmiştir. Dolayısıyla bu çalışma, YZ tabanlı güvenlik sistemlerinin tehditleri tespit, analiz ve müdahale etme kapasitesi ile güvenlik stratejilerindeki rolünü çok yönlü biçimde incelerken, modern risklere karşı sürdürülebilir yaklaşımlar geliştirmeye yönelik güçlü bir temel sunmayı hedeflemektedir.

1. Güvenlik Tehditlerinin Tarihsel Süreç İçerisindeki Değişimi

Modern çağda güvenlik politikaları önemli değişiklikler yaşamıştır. 19. yüzyılın sonlarından 20. yüzyılın ilk yarısına kadar süren erken dönemde, güvenlik politikaları ve uygulamaları ulusal güvenliğe yönelik askerî stratejiler ve geleneksel kolluk faaliyetlerine odaklanmıştır. Ancak 20. yüzyılın ikinci yarısından itibaren güvenlik tehditlerinin küreselleşmesi, yeni teknolojik atılımlar ve değişen siyasi dinamikler nedeniyle bu politikalar köklü bir dönüşüm geçirmiştir. Artık, daimî orduların idamesi, tahkimat ve stratejik ortaklıklar gibi geleneksel askerî yöntemlerin yanı sıra sosyal ve siyasi kaygılar da gözetilerek ulusların korunmasına

öncelik verilmiştir. Bu eylemler, devlet egemenliğini ve toprak bütünlüğünü korumaya odaklanarak dış tehditleri caydırmak için uygulanmıştır.

Ulus-devletlerin kurulması ve jeopolitik dinamiklerin değişmesiyle birlikte askerî gücün önemi devam etse de güvenlik taktiklerinin yelpazesi genişlemeye başlamıştır. Genellikle fiziksel tehdit ve çatışmaları kapsayan güvenlik riskleri giderek terörizm, siber saldırılar ve çevresel tehlikeler gibi geleneksel vurgunun ötesindeki konuları da kapsayacak şekilde genişlemiş ve böylece modern risklerin karmaşık doğası kabul edilmiştir (Collective, 2006: 444-445).

Geleneksel askeri tehditlerden daha kapsamlı bir dizi güvenlik sorununa geçiş, Soğuk Savaş'ın sona ermesiyle hız kazanmıştır. Tehlikelerin doğası ekonomi, teknolojik atılımlar, çevresel sorunlar ve değişen siyasi ortamlar nedeniyle dönüşüme uğramıştır. Küreselleşmenin etkisiyle güvenlik kavramı, geleneksel askerî mülahazaların ötesine geçerek geniş bir sorun yelpazesini kapsar hâle gelmiş ve bu durum, güvenlik kaygısı olarak kabul edilen konuların çerçevesini farklı boyutlara taşımıştır. Bu yaklaşım, modern güvenlik kaygılarının inceliklerini daha kapsamlı bir şekilde ele almak amacıyla, askerî yeteneklere ve devlet merkezli bakış açılarına yapılan önceki vurgudan ayrılmıştır. Artık geleneksel güvenlik yaklaşımı aşılmış, devletler güvenlik çalışmalarında konuyu kitlesel göç, küresel sağlık, gıda, enerji, siber güvenlik ve insan hakları gibi alanlara genişleterek devlet merkezli bakış açısını benimsemiştir. Bu yaklaşım, güvenlik çalışmalarının, devletler, alt devlet grupları, bölgeler ve hatta biyosfer gibi farklı unsurları içeren yeni bir paradigma ile yeniden yapılandırılması gerektiğini savunmaktadır (Vennesson, 2019:495-496).

Güvenlik anlayışındaki bu değişime cevap olarak liderler ve politika yapıcılar, yalnızca ulus devletlerden gelen saldırıları değil, aynı zamanda devlet dışı aktörlerden gelen tehditleri, siber saldırıları ve terörizm, organize suç ile insan kaçakçılığı gibi ulusötesi endişeleri de kapsayan güvenlik planlarının gerekliliğini dikkate alarak çok boyutlu stratejiler geliştirmek zorunda kalmıştır. Buna ek olarak, modern güvenlik politikalarının iklim değişikliği, salgın hastalıklar ve siber savaş gibi artan endişeleri de dikkate almaya başlaması, neyin tehlike olarak görüldüğüne dair değişen anlayışı ortaya koymaktadır. Daha kapsamlı bir anlayışa ulaşmak için, riskler devlet sınırlarının ve geleneksel güvenlik çerçevelerinin ötesine geçtiğinden, disiplinlerarası işbirliğine ihtiyaç duyulmuştur. Böylece güvenlik anlayışı, asimetrik tehditlere maruz kalan bireyler, doğal çevre ve veriler gibi korunması gereken varlıklara yönelik tehditlerin önlenmesi ve risklerin yönetilmesini amaçlayan bir yaklaşıma sahip olmuştur (Senn, 2017:605-606).

İnsanlık tarihinin geldiği bu noktada ortaya çıkan yeni risklere karşı klasik güvenlikçi yaklaşımın çözüm üretemeyeceği açıktır. Tehditlerin farklılaşmasıyla birlikte sunulan çözüm

önerilerine ve güvenlik stratejilerine ilişkin yaklaşım, hiç şüphesiz teknolojik ilerlemeden istifade etmek olacaktır. Buradan hareketle, son dönemde hemen her alanda kullanım alanı yaygınlaşan YZ temelli teknik ilerlemelerin güvenlik stratejilerine eklemlenmesi kaçınılmaz bir zorunluluktur. Nitekim dünyada güvenlik konseptlerine entegre edilmeye başlanan bu teknolojiler, yüz tanıma, izinsiz giriş tespiti ve siber güvenlik gibi uygulamaların oluşturulmasını kolaylaştırarak güvenlik sistemlerini dönüştürmüştür. YZ'nin güvenlik uygulamalarına entegrasyonu, tehditleri tanımlama, verileri analiz etme ve koruma mekanizmalarını güçlendirme becerilerini destekleyerek güvenlik yöntemlerine yeni bir bakış açısı getirmiştir.

YZ uygulamalarının sunduğu hızlı tehdit tanımlama, izleme ve gelecek riskleri öngörebilme becerisi, karar verme süreçlerini güçlendirerek güvenlik yöntemlerinde adeta bir devrim yaratmıştır. Makine öğrenimi algoritmalarının, tehditlerle mücadelede faydalı olabilecek büyük veri kümelerindeki eğilimleri tespit etme yeteneğine sahip olması, güvenlik süreçlerinin proaktif bir şekilde yönetilmesine olanak tanımaktadır. Geçmişteki tehdit verilerini analiz eden bir YZ sistemi, potansiyel riskleri belirlemede analiz imkânı sunarken; YZ destekli gözetim sistemleri gibi anlık izleme araçları ile güvenlik ihlallerine daha hızlı tepki verilmesi mümkün hâle gelmektedir. Bu teknolojiler, ortaya çıkan tehditleri öngörmek, engellemek ve ele almak için araçlar sağlayarak düzen ve devamlılığı sürdürülebilir kılmakta kaçınılmaz bir potansiyele sahiptir.

2. Modern Güvenlik Stratejilerinin Geliştirilmesinde Yapay Sinir Ağlarının Kullanımı

Modern güvenlik stratejilerinin biçimlenmesi, tarihsel süreç içerisindeki çeşitli stratejik ve teknolojik evrimin nihayetinde gerçekleşmektedir. Geleneksel askeri tehditlerle başlayan güvenlik stratejileri asimetrik tehditlere odaklanarak dönüşmektedir. İç ve dış güvenliğin sağlanmasında, karmaşık tehditlerin tespit edilmesi ve önlem alınmasına yönelik yaklaşımlar genişlemekte; bu dönemde, özellikle teknolojik araçların hızlı ve etkili tespit olanaklarından yararlanılmaktadır. Teknik araçlar, bilgi edinme, izleme ve müdahale etme aracı olarak kullanılarak güvenlik operasyonlarını destekleyen vazgeçilmez birer güvenlik aparatına dönüşmektedir. Güvenlik anlayışında dönüşümün en büyük devrimlerinden biri, YZ ve YSA gibi ileri düzey tekniklerin uygulanmasıyla gerçekleşmiş; bu teknolojiler güvenlik stratejilerinin temel dinamiklerini yeniden tanımlamıştır.

YSA, insan beyninin bilgi işleme biçimini taklit etmek üzere tasarlanmış ve biyolojik sinir ağlarından ilham alan hesaplama modelleridir. YSA'lar, sinir yapısını oluşturan ve ağırlıklarla birbirine bağlanan yapay veya işlem birimlerinden oluşur (Kustrin ve Beresford, 2000:718-

719). YSA temelinde geliştirilmiş uygulamalar, geleneksel bilişim uygulamalarından farklı olarak davranış göstermek, tepki vermek, kendini yeniden organize etmek, öğrenmek, genelleştirmek ve unutmak gibi kavramları öne çıkarmaktadır. İnsan beyninin sinir yapısını model alan bu teknoloji, basit işlem birimlerinden oluşur ve bu birimler karmaşık bir iletişim ağı ile birbirlerine bağlıdır. Bu karmaşık iletişim ağı sayesinde de zorlu problemlerin çözülmesi sağlanmaktadır (Kumar ve Sanwan, 2015: 1086-1087). YSA'nın güvenlik teknolojilerin entegrasyonu ile kazandırdığı yetenekler sayesinde tehdit algılama, risk analizi ve önleyici stratejileri geliştirmede çığır açıcı bir dönüşüm sağlamıştır.

Teknik araçlar, bilgi edinme, izleme ve müdahale etme aracı olarak kullanılarak güvenlik operasyonlarını destekleyen vazgeçilmez birer güvenlik aparatına dönüşmektedir. Teknik kapasitenin yanı sıra, YZ teknolojilerinin sunduğu hem fiziksel hem de siber güvenlik alanında proaktif çözümler, güvenlik yaklaşımlarının daha verimli ve etkin hâle gelmesine katkı sağlamaktadır. Bu doğrultuda, özellikle YSA desteğiyle otomatikleştirilmiş ve entegre edilmiş güvenlik sistemleri; veri analizi, tanıma ve tahmin yapma yetenekleriyle güvenlik stratejilerinde önemli bir rol oynamaktadır. Bu teknolojiler, karmaşıklaşan çeşitli güvenlik tehditlerine karşı kritik önleyici mekanizmalar sunmaktadır (Marciniak, 2023: 451-454).

YZ teknolojisinin bir parçası olan YSA destekli mekanizmalar, günümüzde büyük veri setlerinden anlam çıkarma, tehdit tespiti, risk analizi, yüz ve nesne tanıma gibi güvenlik uygulamalarında yaygın biçimde kullanılmaktadır. Geleneksel güvenlik yöntemlerinin ötesine geçen bu teknolojiler, görüntüleme ve "elektronik burun" gibi araçlarla elde edilen verileri algoritmalar aracılığıyla analiz ederek şüpheli faaliyetleri tespit edilebilmekte; daha önce yaşanmış olaylardan oluşan veri setleri ve sensör verileriyle de olası riskleri ve gelecekteki muhtemel tehlikelere yönelik öngörücü çözümler sunmaktadır. Bu teknolojilerin uygulanması için gereken verilerin işlenmesi, altyapı yatırımları, geliştirme ve bakım süreçleri ile uzman personel istihdamı gibi süreklilik arz eden maliyetlere rağmen; insan hatalarını azaltması, kamu hizmeti operasyonlarının verimliliği ve etkinliğinin artması sayesinde kamu düzeni ve güvenliğinin sağlanması desteklenmektedir (Wirtz & Müller, 2019: 1084).

YZ destekli güvenlik araçları, geleneksel güvenlik yöntemlerinin sahip olduğu yüksek işletme giderleri ile insan kaynağı ve işgücü gibi handikapların aşılmasına olanak tanımaktadır. Zira geleneksel yöntemde, suçun ya da tehdidin gerçekleşmesi sonrasında toplanan deliller kanıt olarak kullanılır ve uzun prosedürlerin ardından müdahalede bulunulur. Güvenlik güçlerinin kullandığı gözetim sistemleri de reaktif bir yaklaşımla sınırlı kaldığı için önlemden ziyade, olaylardan sonra yorumlanması gereken kanıtları belgeleyebilmektedir. YZ destekli teknolojiler ise anormal eylemleri aktif bir biçimde tespit etme ve yanıt verme kabiliyetini

sahiptir. Bu bakımdan, geleneksel güvenlik araçlarının sınırlılıklarını aşan ve YSA ile desteklenen akıllı sistemler, kanıtların kayda geçirilmesinden öte proaktif bir güce sahiptir. Söz konusu sistemler, risk ve tehditleri meydana gelmeden önce belirlemek için özellikle derin öğrenme teknolojisini kullanarak verileri gerçek zamanlı olarak analiz etmekte; böylece güvenlik yönetimine ve suçların önlenmesinde avantajlar sağlamaktadır (Sung & Park, 2021: 34298-34299).

Güvenlik teşkilatlarının yönetim ve operasyonlarında ana hedef, stratejilerin geliştirilmesi, tehditlerin tespiti ile hızlı ve etkili müdahalede bulunma unsurları optimal şekilde uygulamaktır. İnsan unsurunun etkisiyle değişkenlik gösteren bu uygulamalar, YZ, makine öğrenimi algoritmaları ve büyük veri yazılımlarının desteğiyle kapsamlı güvenlik yönetimi imkânına kavuşmaktadır. Bilgi işleme hızını artırarak devlet kaynaklarının daha etkili bir şekilde kullanılmasını ve kaliteli hizmet sunumunu iyileştiren bu teknolojiler, kamu kaynaklarının da verimli biçimde kullanılmasına önemli ölçüde katkı sağlamaktadır. Wirtz ve Müller (2019: 1085)'in YZ uygulamalarından yararlanarak kamu hizmetinin sunumuna ilişkin araştırmalar, iş tamamlama hızında %20 ila %200 arasında artış potansiyeli olduğunu ortaya koymaktadır. Şüphesiz, işlem hızının artırılması artan vaka yükünü hafifleterek kaliteli hizmet sunumunu da güçlendirecektir.

Dünyada kentsel kamu güvenliği yönetişimi ve kriz yönetiminde devreye alınan çok sayıda YSA destekli uygulama, veri işleme ve tahmine dayalı algoritmaların birleşmesiyle olası riskleri azaltabilen uyarı sistemlerinin başarılı sonuçlar ürettiğini göstermektedir. Toplumsal hayatta karşılaşılan riskleri önlemek veya muhtemel tehditlere ilişkin senaryolar oluşturarak belirsizlikleri etkili bir yönetmek için geçmiş olay verileriyle ve kurallarla eğitilmiş YSA modelleri; video ve fotoğraflardan ardışık çıkarımlar yapma, nesne algılama ve davranışları tanımlama gibi yöntemler kullanarak proaktif risk yönetimine önemli katkılar sunmaktadır (Nguyen, Cai, & Chen, 2017: 616, 621; Alawad, Kaewunruen, & An, 2020: 102815-102816; Khosravinia, Perumal, & Zarrin, 2023: 52985). Doğru karar alma süreçlerini hızlandırarak müdahale sürelerini azaltan bu teknolojiler, emek yoğun güç ihtiyacını düşürdüğü gibi ulusal güvenliğin korunmasında da dikkate değer bir kapasiteye sahiptir. Bu teknolojiler, kentsel güvenlik ve kriz yönetiminden küresel ölçekte nükleer tehditler gibi daha makro düzeydeki karmaşık risklerin dahi yönetiminde etkili olabilecek bir kapasiteye sahiptir.

YZ teknolojilerinin hızlı çözümleme gücü ve doğru karar vermedeki etkinliği, yanlış bilgiyle hareket etmenin ya da savaş durumu gibi telafisi mümkün olmayan krizlerin önüne geçmek için muazzam fırsatlar sunmaktadır. Örneğin Soğuk Savaş döneminden kalma "karşılıklı garantili imha" (Mutually Assured Destruction) veya "ikinci vuruş yeteneği" (Second-Strike Capability)

doktrinlerinin, nükleer saldırıya anında başka bir nükleer saldırı ile karşılık verme üzerine kurgulu olması, nükleer savaş tehdidine dair endişeleri uzun süre güçlendirmiştir. Nitekim, erken uyarı sistemlerinin verdiği yanlış alarmlar neticesinde nükleer savaşın başlamasını, askeri uzmanların ve siyasi liderlerin son anda yaptığı müdahaleler engellemiştir. Bu vakadan hareketle Cox ve Williams (2021)'ın araştırması, YZ araçlarının benzer riskleri en aza indirebileceğini göstermektedir. Onlara göre, uzay araçları veya ateşli silahların taşınması için kullanılan roketlerin fırlatma türlerine özgü davranış kalıpları ile eğitilmiş YZ araçları, büyük veri analitiğindeki bilgileri harmanlayarak geçmişte tesadüfi bir şekilde atlatılan nükleer savaş riski gibi durumların fiilen önlenmesini sağlayacaktır.

Güvenlik alanında YZ teknolojilerini en yoğun şekilde kullan kurumların başında silahlı kuvvetler gelmektedir. Bu teknolojiler; radar ve uydu görüntülerindeki anomalilerin tespitinden, denizaltı mayınlarının tespiti ve sınıflandırılmasını sağlayacak sonar sistemlerine entegre edilmesinde; saldırı algılama sistemlerinin ağ trafiğini analiz ederek siber güvenliği desteklemesinden, savunma sistemlerinde kritik bir rol oynayan insansız hava araçlarının hedef algılama ve görev planlamasına kadar modern askeri sistemleri güçlendirmektedir (Bistron ve Piotrowski, 2021: 3-8). Bu işleviyle YZ tabanlı sistemler, orduların savunma yeteneğini ve operasyonel etkinliğini büyük ölçüde güçlendirmektedir.

Askerî ve kolluk faaliyetleri, doğrudan operasyonel süreçler kadar önleyici hizmetlere odaklanan proaktif bir yaklaşıma da dayalıdır. Bu yaklaşım, kamu düzeni ve devamlılığının sağlanmasını desteklendiği gibi kaynakların da verimli kullanılmasına katkı sunmaktadır. Bu doğrultuda, güvenlik kurumlarının karmaşık doğası gereği başa çıkmada en çok zorlandığı ve toplumun zarar gördüğü terörle mücadelede YZ teknolojileri önemli fırsatlar sunacaktır. Uddin ve arkadaşlarının (2020) simülasyon tabanlı tahminlere dayalı çalışması, bir terör saldırısının hangi yöntemle olabileceği, kullanılabilecek silah türlerini ve hedef alınabilecek bölgeler gibi unsurları analiz eden YSA gibi derin öğrenme modellerinin, geleneksel makine öğrenmesi algoritmalarına göre %95'in üzerinde doğruluk oranıyla karmaşık örüntüleri anlamada ve gelecekteki saldırıları tahmin etmede etkin bir araç olabileceğini ortaya koymaktadır.

YSA teknolojilerinin yaygın biçimde kullanılmaya başlandığı bir diğer alan ise, kamu düzeni ve güvenliğini sağlamada kuşkusuz bir öneme sahip asayiş faaliyetleridir. Kolluk faaliyetlerinde YZ'nın kullanımıyla, kamu güvenliğinin sağlanmasında iyileşmeye kaydedildiği ve kolluk kuvvetlerinin kaynaklarının daha verimli kullanılarak suç oranında bir düşüş sağlandığını gösteren bir çalışmada (Van 't Wout ve diğ., 2021); geçmiş suç verilerine ilişkin bilgileri içeren veri kümelerini analiz eden YSA destekli sistemler, suç davranışlarını tahmin ederek önleyici polislik yaklaşımını güçlendirdiği ve bu sayede suç oranlarını

düşürmede başarılı çözümler ortaya koyduğu gözlemlenmiştir. Bir başka ifadeyle, YSA ve diğer makine öğrenimi algoritmaları, demografik, coğrafi ve zamansal eğilimler gibi çeşitli faktörlerle eğitilerek olağanüstü tahmin yeteneklerine ulaşmaktadır; böylece geçmiş asayiş olaylarının analiz edilmesini mümkün kılmaktadır. Bu sayede suç faaliyetlerine karışma olasılığı daha yüksek olan bireylere ve bölgelere yoğunlaşarak gelecekteki vakalara ilişkin daha isabetli öngörülerde bulunma imkânına kavuşulmaktadır (Van 't Wout ve diğ., 2021: 1044-1046).

YSA teknolojileri, kamu güvenliğini sağlamada spesifik sorunlara çözüm getirmenin ötesinde, makro ölçekte planlama gerektiren bölgesel ve ulusal sorunlara ilişkin de çözümleyici fırsatlar sunmaktadır. Kent güvenliği çerçevesinde, farklı unsurların ve karmaşık olay örgülerinin yönetilmeye çalışıldığı bölgelerde olduğu gibi, ulusal çapta etkiye sahip güvenlik sorunlarıyla başa çıkmada da bu teknolojiler önemli katkılar sağlayabilir. Özellikle geniş çaplı güvenlik yönetimi uygulamalarında, riskle mücadelede etkili bir sonuç elde edebilmek için farklı kamu kurumlarının ve hatta sivil toplum kuruluşlarının işbirliği zorunlu hâle gelmektedir. YZ tabanlı araçlar, kamu güvenliğini sağlayan kurumlar arasındaki işbirliğini artırarak karmaşık durumlara ve değişen koşullara uyum sağlama kapasitesini yükseltmektedir. Ayrıca, YZ teknolojilerinin kullanımı sayesinde farklı kurumlar arasındaki güç dengesizliği, örgütsel kültür farklılıkları, öncelik çatışmaları ve bilgi paylaşımındaki engeller gibi işbirliğini güçleştirecek hususları aşmak daha kolay hâle gelecektir (Malyjurek, 2022: 1200-1201). YSA'nın farklı veri kaynaklarına entegre edilmesi, kriz anlarında hangi adımların atılacağını planlamak ve bu planlara dair projeksiyonlar oluşturulmasına olanak sağlamakta; karşılaşılabilecek zorluklara dair öngörüler geliştirerek sorunlara yönelik stratejik çözümlerin üretilmesine destek vermektedir.

3. Güvenlikte Yapay Zeka Teknolojisinin Sınırlılıkları ve Tehlikeleri

Dünya tarihinde icatlar ve teknolojik gelişimin ilk yansımaları, şüphesiz güvenlik alanında belirgin bir biçimde kendini göstermiştir. Kilit ve anahtar sisteminden biyometrik tanıma sistemlerine, atlı arabalardan drone ve insansız hava araçlarına, telgraf ve telefondan radarlara kadar pek çok icadın evrimi, gündelik hayatta insanların yaşam kalitesini arttırmaktan çok devletler açısından güvenlik stratejilerini şekillendirmede benzersiz bir öneme sahip olmuştur. Bilhassa YZ ve makine öğrenimi sayesinde, devletlerin bilgi gücünü emsali görülmemiş bir şekilde kullanma kapasitesine eriştiği günümüze dek, teknolojinin toplumsal iyilik için mi yoksa daha fazla kontrol sağlamak amacıyla mı kullanıldığı sorusu daima tartışılmalıdır.

Günümüzde algoritmalar aracılığıyla kişiler hakkında toplanan bilgiler ve gözetim aygıtları, insanların gündelik yaşamlarını kapsayan kent yönetimi, kamu hizmetleri, eğitim gibi pek çok

alanda önemli iyileştirmeler sağlamaktadır. Fakat bu aygıtlar toplumsal alanı baskılama gücünü artırma amacıyla da kullanılabilmektedir. Örneğin dijital teknolojileri etkin biçimde kullanarak adeta 21. yüzyılın "gözetim devletini" kuran Çin'de, toplumsal düzenin muhafaza edilmesi kolaylaşırken, muhalif hareketlerin önceden tespit edilmesi de mümkün hâle gelmiştir. Keza bu teknolojiler, Çin Komünist Partisi'nin siyasi ve sosyal kontrolü güçlendirilmesinde etkili bir araç olarak kullanılmaktadır. Yüz tanıma sistemleri ile bireylerin hareketlerini izleme, protestoları önceden tahmin etme ve kimlik tespiti gibi uygulamalar sayesinde, Çin'in güvenlik ve istihbarat kapasitesi son derece güçlenmiştir. 2013 yılından itibaren Çin'de YZ tabanlı güvenlik teknolojilerinin kamu hizmetine sunulması için çeşitli ihaleler yapılmaktadır. Öyle ki, yalnızca 2018 yılında gerçekleşen bir ihale kapsamında, Heilongjiang eyaletinde yaşayan 30 milyon kişinin yüz tanıma verilerinin işlenmesi için bir anlaşma imzalanmıştır. Böylesine kapsamlı bir gözetim ve veri işleme kapasitesi güvenlik güçlerinin kabiliyetini arttırmakla birlikte kamu huzuruna yönelik endişeleri de beraberinde getirmiştir. Zira YZ destekli gözetim sistemleri, bireysel özgürlükler üzerinde kısıtlayıcı bir etkiye sahip olabildiği gibi, bu sistemler tarafından elde edilen verilerin saklanması ve işlenmesiyle oluşabilecek mahremiyet ihlalleri, siyasi ve sosyal istikrarsızlıklara yol açabilecek meşruiyet krizi riskini de beraberinde taşımaktadır. Nitekim YZ destekli yüz tanıma sistemi üretiminde Rusya ile birlikte dünya lideri olan Çin'in, bu teknolojileri ihraç ettiği ülkelerin başında otokratik rejimlerin gelmesi, YZ'nin antidemokratik uygulamalara elverişli olduğuna dair endişeleri güçlendirmektedir (Beraja, Kao, Yang, & Yuchtman, 2023: 1395-1397).

Çin'in YZ teknolojilerinden sağladığı kazanımları sadece sınırları içinde değil, bu teknolojileri ihraç ettiği ülkelerden elde ettiği veriler sayesinde de katlayarak artırmaktadır. 2030 yılına kadar dünyanın en büyük YZ inovasyon merkezi olmayı hedefleyen Çin, bu doğrultuda geliştirdiği teknolojileri ihraç ederek diğer ülkeler üzerinde politik ve ekonomik bir etki gücüne sahip olmanın yanı sıra, söz konusu etkiyi sürdürülebilir kılacak istihbarî bilgiye de erişmektedir. Afrika ülkelerinde hayata geçirilen yüz tanıma ve telekomünikasyon sistemleriyle siyasi nüfuzunu arttıran Çin, aynı zamanda YZ algoritmalarını eğitecek biyometrik veriler de toplamaktadır. Buna karşılık, dünyanın önde gelen yüz tanıma firmalarından Microsoft ve IBM'in ABD'deki etnik çeşitlilik sayesinde Çinli firmalara göre avantajlı bir konumda bulunsalar da, siyahi bireylerin yer aldığı yüz tanıma süreçlerinde hâlâ yeterince istikrarlı sonuçlar elde edememektedir. Nüfus yapısı büyük ölçüde homojen olan Çin ise Afrika'daki faaliyetleri ile adeta bir laboratuvar ortamı sağlayarak, yüz tanıma sistemlerinin farklı ırklarda daha başarılı çalışacak seviyeye erişmesine imkân tanımaktadır (Gravett, 2020: 154).

Siber teknolojilerin dünya geneline yayılması birlikte, pek çok ülkede özellikle muhalif hareketlerin kontrol altına alınmasının kolaylaştığı yönünde değerlendirmeler yapılmaktadır. Bu teknolojilerin, bireylerin hareketlerini izlenebilir hale getiren gözetim ve kontrol mekanizmalarıyla, baskıcı rejimlere güç kazandırdığı ileri sürülebilir (Akyeşilmen, 2019: 275-276). Ses tanıma teknolojileri, mobil ağların taranması, yurttaşların GPS üzerinden takip edilebilmesi ve mesajlarının izlenebilmesi gibi yetkinliklerin, kamu düzenine sağladığı avantajlar kadar birey mahremiyetine yönelik riskler (Dragu ve Lupu, 2021: 992-996) taşıdığına dair tartışmalar devam etmektedir. Benzer biçimde, geleneksel medyayı aşan bir güce sahip olan internet uygulamaları üzerinden propaganda faaliyetinde bulunan organizasyonların web sitelerine DDoS saldırıları düzenlenerek erişimlerine kısıtlama getirilmesi gibi durumlar, internet özgürlüğünün engellenebileceği ihtimalini gündeme getirmektedir. Ortadoğu ülkelerinde de örneklerine rastlandığı gibi YZ algoritmaları, rejim karşıtı eylemlerin kontrol altına alınmasında ve propaganda faaliyeti yürütmek amacıyla kullanılmaktadır. Sosyal medya platformlardaki belirli anahtar kelimeleri taramak için geliştirilen YZ tabanlı sistemler, botnetleri muhalif söylemleri manipüle etmek üzere harekete geçirebileceği gibi, çevrimiçi faaliyetlerin büyük veri analitiğiyle incelenmesi sayesinde hükümet karşıtı olarak görülen birey ya da grupların tespit edilmesini de sağlamaktadır (Uniacke, 2020: 996-996).

YZ destekli güvenlik teknolojilerinin kullanım amacı kadar, tehdit algısını biçimlendiren veriler de en az bu amaç kadar önemlidir. Makine öğrenimi sırasında kullanılan verilerdeki önyargılı yaklaşımlar, pek çok hak ihlaline sebep olabilmektedir. Özellikle YZ destekli iç güvenlik uygulamalarında, YSA'yı şekillendiren veri setlerinde yaş, cinsiyet, eğitim seviyesi, gelir durumu, daha önce işlediği suçlar gibi pek çok veri unsurunun yanı sıra ırksal özellikler ya da içinde bulunduğu sosyal sınıf gibi bilgiler de kullanıldığı için YSA'nın avantajları kadar potansiyel tehlikeleri ve etik sonuçları da gözeterek dengeli bir yaklaşım benimsemek gerekir. Bu bakımdan verilerin tarafsız biçimde kayıt altına alınması, sistemin isabetliliğini arttıracağı gibi YZ'nin toplumsal değerleri tehlikeye atabilecek tercihlerde bulunmasının da önüne geçecek tedbirler gerekmektedir (Wirtz & Müller, 2019: 1087; Van't Wout ve diğ., 2021: 1046-1048). Zira Çin'de Uygur Türklerinin ırksal özellikleri ile eğitilmiş YZ araçlarının özel olarak ayrımcı uygulamalara imkân veren bir silah vazifesi görmesi; ABD'de de polis teşkilâtı tarafından kullanılan yüz tanıma sistemlerinin, siyahi insanları tanımlamadaki yüksek hata payı nedeniyle çok sayıda mağduriyete sebebiyet vermesi (Gravett, 2020: 159, 162) gibi olumsuz örnekler bulunmaktadır.

YZ sistemlerinin istikrarlı çalışmasında en etkili faktör, sahip olduğu büyük veridir. Bu verinin önyargılı olmasının yanı sıra manipüle edilmesi neticesinde doğabilecek risklere de dikkat

etmek gerekir. Görsel, işitsel ya da algoritmik verilerden hareketle çıktılar üreten bu teknolojiler, siber saldırılar, derin sahtecilik ve görüntü sahteciliği ile yanıltılarak derin öğrenme modelleri üzerinde ciddi güvenlik riskleri doğurabilmektedir (Cox ve Williams, 2021: 80-81). YZ'nın yüksek güvenle yanlış tahminde bulunmasını sağlayacak adversarial örnekler, FGSM (Fast Gradient Sign Method) tekniği ve DeepFool algoritmaları kullanılarak oluşturulabilir (Lai, Huo, Hou ve Wang, 2022). Ayrıca otonom araçların yol işaretlerini yanlış okumasına sebep olabilen küçük etiketlerle yanlış hız limitlerine göre hareket ettirecek LiDAR saldırıları; insan kulağının işitemeyeceği frekansta ses dalgaları oluşturularak sesli asistanlara yanlış komutları gönderilmesini ve cihazların kullanıcısından bağımsız işlemler yürütebilmesini sağlayan Dolphin saldırıları gibi dijital ve fiziksel dünyada manipüle edilebilecek güvenlik sorunlarını da barındırmaktadır (Ren ve diğ., 2021: 3331-3334). Bu sebeple YZ destekli güvenlik uygulamalarının, düzenli olarak iyi eğitilmiş personeller tarafından kullanılması ve denetlenmesi mühim bir öneme sahiptir. Son yıllarda, güvenlik yarışında geri kalmamak adına bu uygulamalar hızla güvenlik alanına entegre olmaktadır. Bu alandaki özel firmaların da kamu personelini destekleyecek uzmanları sağlaması teşvik edilmelidir.

Geleneksel uluslararası hukuk, siber teknolojilerden kaynaklanan insan haklarını korumada yetersiz kaldığından, bu alanda yeni bir küresel hukuk düzenine duyulan ihtiyaç giderek artmaktadır (Akyeşilmen, 2019: 278). Bu nedenle YZ teknolojilerinin kullanımında karşılaşılan teknik, sosyal ve siyasi sorunların aşılmasında, uzmanların görüşleri kadar toplumsal paydaşların da bu uygulamalara yönelik bilgi sahibi olması hayati önem taşımaktadır. Bu teknolojilere yönelik gelişmiş demokratik devletlerde "güvenlik ve özgürlük dengesi" konulu tartışmalar giderek çoğalması ihtiyaç duyulan düzenlemeler için zemin hazırlamaktadır. Örneğin, toplumsal hayatı kuşatan gözetim ağının tetiklediği protestolar neticesinde, ABD polisinin kullandığı Amazon'un "Rekognition" yüz tanıma sisteminin kullanımı durdurulmak zorunda kalınmıştır (Gravett, 2020: 162). Bu bağlamda, demokratik rejimlerde toplumsal paydaşların baskısı ile YZ algoritmalarının yol açtığı sorunlar kısmen giderilmeye çalışılmakta; hükümetler de yurttaşların çıkarlarını koruyacak farklı tedbirler almaya başlamaktadır. Nitekim AB ve Kanada'da mevzuat düzenlemeleri ve etik kullanım için kurullar oluşturulmuş, YZ uygulamalarına demokratik kısıtlamalar getirilmiş ve temel hakların korunmasına ilişkin geniş çaplı düzenlemeler yapılmıştır. Ancak YZ'nın toplum üzerindeki olumsuz etkilerini en aza indirmeyi ve teknolojik faydayı en üst düzeye çıkarmayı amaçlayan bu yaklaşım, YZ üretiminde lider konumda bulunan ABD ve Çin gibi ülkeler arasındaki yoğun rekabet nedeniyle hâlen oldukça sınırlı kalmaktadır. Hükümetlerin, stratejik bir hedef olarak gördükleri YZ

inovasyonunu teşvik etmek amacıyla esnek politikalar uygulaması (Papyshev ve Yarime, 2023: 86-90), bu teknolojilerin muhtemel etkilerine yönelik endişeleri daha da güçlendirmektedir.

Şüphesiz günümüzde devletlerin güvenliği sağlamada YZ'dan istifade etmemesi büyük bir sorundur. Bununla birlikte, kamu hizmetlerinin iyileştirilmesi için büyük bir zorunluluk hâline gelen YZ araçlarının hâkimiyeti, çeşitli demokratik endişeleri de beraberinde getirmektedir. Bu teknolojilerin ağırlıklı olarak dünyanın en büyük şirketlerinin kontrolü altında olması, demokrasi açısından mülhem sorunlar barındırmaktadır. Yüksek teknolojili YZ araçlarının üretildiği ülkelerde, devlet eliyle üretici şirketlerin önünün açılması; belirli şirketlerin elinde bulunan veri gücünün şirketokrasiyi doğurma riskini artırmaktadır. Demokratik değerler açısından bir diğer endişe de enformasyonun şirketlerin elinde yoğunlaşmasına rağmen hükümet temsilcileri ve bürokratların yeterince bilgi birikime sahip olmamasıdır. Ayrıca kullanılacak teknolojilerin kapsamı hakkında toplumun aydınlatılmaması, geniş halk kesimlerinin görüşlerine başvurulmaması ve şirketlerin lobi gücünün, devletlerin uluslararası rekabette öne geçme isteğiyle birleşmesi, gelecekte yeni etik ve demokratik sorunları doğurma ihtimalini güçlendirmektedir. Bu sebeple, etik kurallar ve yönetmeliklerle çevrelenmesi gereken bu teknolojileri kullanma ve geliştirme kapasitesine sahip eğitimli kamu personeli oranını arttırmaya, vatandaşların bu teknolojilere yönelik farkındalığını yükselterek hak ve özgürlükler konusundaki kaygılarını gidermeye büyük önem verilmelidir.

Sonuç

Güvenlik alanındaki teknolojik evrim içerisinde, YZ ile YSA gibi ileri teknolojiler, güvenlik politikalarının kapsamını genişletmekte ve modern stratejilerin biçimlenmesinde belirgin bir rol oynamaktadır. YZ teknolojileri, modernleşmeyle büyüyen tehditlere karşı geleneksel güvenlik konseptlerinin aşamadığı sorunlara hızlı ve etkili çözümler sunarak, güvenlik operasyonlarının vazgeçilmez araçları hâline gelmiştir.

Ulusal sınırlar, bireysel güvenlik, toplumsal bütünlük ve kamu düzeni gibi unsurların korunmasına yönelik yeni yaklaşımlar sunan YZ teknolojileri, tehditleri yalnızca kayıt altına almakla kalmayıp, aynı zamanda riskleri önceden tespit etme ve müdahale etme kapasitesine de sahiptir. Bu uygulamaların sahip olduğu yüz ve nesne tanıma, tehdit tespiti, risk analizi ve suç tahmini gibi yetenekler; asayiş hizmetleri, kent güvenliği, kitlesel göç, doğal afetler, terör ve siber saldırılar gibi operasyonlarda kullanılmaktadır.

YZ teknolojileri, sunduğu fırsatların yanı sıra önemli sınırlılıkları ve tehlikeleri de beraberinde getirir. Özellikle YZ sistemlerinin etkin çalışması için gerekli olan büyük veri setlerinin manipüle edilmesi ve siber saldırılara maruz kalması, kişisel güvenlik risklerini ve hak ihlallerini doğurabilmektedir. Ayrıca makine öğretimi süreçlerinde kullanılan veri

kümelerindeki önyargılı yaklaşımlar, adaletsiz uygulamalara neden olabilmektedir. Bu sebeple YZ destekli güvenlik uygulamalarının geliştirilmesi ve uygulanmasında etik kuralların göz önünde bulundurulması ve iyi eğitilmiş personel tarafından sürekli denetlenmesi hayati öneme taşımaktadır.

Dünyada kamu düzeni ve güvenliğinin sağlanmasında YZ teknolojilerinin uygulanmaya başladığı ülkelerdeki çarpıcı örneklere rağmen, bilhassa otokratik rejimlerde bireylerin mahremiyetini ihlal etme ve özgürlükleri kısıtlama aracı olarak kullanabilme riskini de taşıdığı da görülmektedir. Örneğin Çin'de yüz tanıma sistemleri ve diğer izleme araçları, bireylerin hareketlerini takip etme ve toplumsal hareketleri önceden tespit etme amacıyla kullanılabilmektedir. Bununla birlikte demokratik rejimlerde de YZ uygulamalarının etkisine ilişkin bilgi ve bu sistemlerin denetimi sınırlı kalmaktadır. Bu teknolojilerin toplum üzerindeki olumsuz etkilerini asgari düzeye indirmek için yasal düzenlemeler ve etik kurallar getirilmesi gerekliliğini ortaya koymaktadır. Bu bağlamda, araştırma ve uygulama alanlarına yönelik çıkarımlar arasında politika oluşturma süreçlerinde sivil toplum, uzmanlar ve ilgili kamu kurumlarının etkin katılımı gerekmektedir.

Bu araştırmanın sınırlılıkları arasında, istatistiksel verilerin ve saha çalışmalarının daha derinlemesine incelenememesi sayılabilir. Gelecekteki çalışmalar, farklı ülke ve kurumların YZ tabanlı güvenlik sistemlerini karşılaştırarak ampirik veriler üzerinden daha kapsamlı sonuçlar elde etmeye odaklanabilir. Ayrıca, etik ve toplumsal kabule ilişkin etkilerin izlenmesi, bu teknolojilerin güvenlik uygulamalarındaki meşruiyetini ve sürdürülebilirliğini değerlendirmek açısından değerli olacaktır. Böylece araştırma, teknolojik yeniliklerin toplumsal faydaya dönüştürülmesi yolunda karar alıcılara ve akademik çevrelere önemli katkılar sunmaya devam edecektir.

Kaynakça:

Agatonovic-Kustrin, S., & Beresford, R. (2000). Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research. Journal of Pharmaceutical and Biomedical Analysis, 22(5), 717–727. doi:10.1016/s0731-7085(99)00272-1

Akyeşilmen, N. (2019). New debates brought about by cyberspace in human rights. *Cyberpolitik Journal*, 4(8), 274–286.

Alawad, H., Kaewunruen, S., & An, M. (2020). A deep learning approach towards railway safety risk assessment. *IEEE Access*, 8, 102811–102826. https://doi.org/10.1109/ACCESS.2020.2997946

Beraja, M., Kao, A., Yang, D. Y., & Yuchtman, N. (2023). AI-tocracy: The mutual reinforcement of artificial intelligence and autocratic regimes. *The Quarterly Journal of Economics*, 138(3), 1349–1402. https://doi.org/10.1093/qje/qjad012

Bistron, M., & Piotrowski, Z. (2021). Artificial intelligence applications in military systems and their influence on sense of security of citizens. Electronics, 10(7), 871. https://doi.org/10.3390/electronics10070871 (Erişim tarihi: 4 Eylül 2024).

Collective, C. A. S. E. (2006). Critical approaches to security in Europe: A networked manifesto. *Security Dialogue*, 37(4), 443–487. https://doi.org/10.1177/0967010606073085

Cox, J., & Williams, H. (2021). The unavoidable technology: How artificial intelligence can strengthen nuclear stability. *The Washington Quarterly*, 44(1), 69–85. https://doi.org/10.1080/0163660X.2021.1893019

Dragu, T., & Lupu, Y. (2021). Digital authoritarianism and the future of human rights. *International Organization*, 75(4), 991–1017. https://doi.org/10.1017/S0020818320000624

Gillham, P. F. (2011). Securitizing America: Strategic incapacitation and the policing of protest since the 11 September 2001 terrorist attacks. *Sociology Compass*, 5(7), 636–652. https://doi.org/10.1111/j.1751-9020.2011.00394.x

Gravett, W. H. (2020). Digital coloniser? China and artificial intelligence in Africa. *Survival*, 62(6), 153–178. https://doi.org/10.1080/00396338.2020.1851098

Hörnqvist, M. (2004). The birth of public order policy. *Race & Class*, 46(1), 30–52. https://doi.org/10.1177/0306396804045513

Khosravinia, P., Perumal, T., & Zarrin, J. (2023). Enhancing road safety through accurate detection of hazardous driving behaviors with graph convolutional recurrent networks. *IEEE Access*, 11, 52983–52995. https://doi.org/10.1109/ACCESS.2023.3280473

Kumar, D., & Sangwan, H. (2015). Research paper on basic of artificial neural network. International Journal of Innovative Research in Technology, 1(12), 1086–1089. https://doi.org/10.2349/6002

Lai, J., Huo, Y., Hou, R., & Wang, X. (2022). A universal detection method for adversarial examples and fake images. *Sensors*, 22(3445). https://doi.org/10.3390/s22093445

Malyjurek, K. (2022). Interpretive structural modelling of inter-agency collaboration risk in public safety networks. *Quality & Quantity*, 56(3), 1193–1221. https://doi.org/10.1007/s11135-021-01172-0

Marciniak, D. (2023). Algorithmic policing: An exploratory study of the algorithmically mediated construction of individual risk in a UK police force. *Policing and Society*, 33(4), 449–463. https://doi.org/10.1080/10439463.2022.2144305

Nguyen, H., Cai, C., & Chen, F. (2017). Automatic classification of traffic incident's severity using machine learning approaches. *IET Intelligent Transport Systems*, 11(10), 615–623. https://doi.org/10.1049/iet-its.2017.0051

Papyshev, G., & Yarime, M. (2023). The state's role in governing artificial intelligence: Development, control, and promotion through national strategies. *Policy Design and Practice*, 6(1), 79–102. https://doi.org/10.1080/25741292.2022.2162252

Ren, H., Huang, T., & Yan, H. (2021). Adversarial examples: Attacks and defenses in the physical world. *International Journal of Machine Learning and Cybernetics*, 12(11), 3325–3336. https://doi.org/10.1007/s13042-020-01242-z

Senn, M. (2017). The art of constructing (in)security: Probing rhetorical strategies of securitisation. *Journal of International Relations and Development*, 20(3), 605–630. https://doi.org/10.1057/jird.2016.7

Sung, C. S., & Park, J. Y. (2021). Design of an intelligent video surveillance system for crime prevention: Applying deep learning technology. *Multimedia Tools and Applications*, 80(26), 34297–34309. https://doi.org/10.1007/s11042-021-10809-z

Uddin, M. I., Zada, N., Aziz, F., Saeed, Y., Zeb, A., Ali Shah, S. A., … Mahmoud, M. (2020). Prediction of Future Terrorist Activities Using Deep Neural Networks. Complexity, 2020, 1–16. doi:10.1155/2020/1373087 (Erişim Tarihi: 04.09.2024)

Uniacke, R. (2020). Authoritarianism in the information age: State branding, depoliticizing and 'de-civilizing' of online civil society in Saudi Arabia and the United Arab Emirates. *British Journal of Middle Eastern Studies*, 48(5), 979–999. https://doi.org/10.1080/13530194.2020.1737916

Van 't Wout, E., Pieringer, C., Torres Irribarra, D., Asahi, K., & Larroulet, P. (2021). Machine learning for policing: A case study on arrests in Chile. *Policing and Society*, 31(9), 1036–1050. https://doi.org/10.1080/10439463.2020.1779270

Vennesson, P. (2019). Is strategic studies rationalist, materialist, and a-critical? Reconnecting security and strategy. *Journal of Global Security Studies*, 5(3), 494–510. https://doi.org/10.1093/jogss/ogz032

Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review*, 21(7), 1076–1100. https://doi.org/10.1080/14719037.2018.1549268

OPINIONS / YORUMLAR

CYBER SECURITY ACT 2024: A FACELIFT TO THE CYBER SECURITY IN MALAYSIA

Sonny ZULHUDA*

Orcid: 0000-0003-0192-1971

1. Introduction

Digitalization has permeated all aspects of life, with many critical activities now dependent on digital systems. Their disruption could severely impact citizens' well-being and essential services. The G20 recently emphasized the importance of digital connectivity for inclusion and transformation, stressing the need for a secure online environment to build trust in the digital economy (ITU, 2024). However, this vision faces challenges including digital divides, privacy concerns, intellectual property issues, online safety, disinformation, and cybersecurity threats. The World Economic Forum report highlighted technological risks as a key global concern, including widespread cybercrime, critical infrastructure breakdown, digital inequality, and adverse outcomes of new technologies (World Economic Forum, 2024). Weak cybersecurity infrastructure exacerbates these issues, potentially leading to misinformation, social cohesion erosion, supply chain collapse, and even social conflicts. Therefore, strengthening cybersecurity policies is crucial for addressing these challenges and ensuring a resilient digital future.

Cybersecurity is the process of protecting information by preventing, detecting and responding to attacks. It is a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets (ITU, 2008). Such organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyber environment. The aim of cybersecurity is to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment.

* Assoc. Prof. Dr.Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia. E-mail: sonny@iium.edu.my

Furthermore, we can summarise that the objectives of cybersecurity are to achieve the three components, namely, availability, integrity which may include authenticity and non-repudiation and confidentiality. Pertaining to the cyber system or digital assets of any country, therefore, three components are crucial, namely:

1. The confidentiality of cyber system. This aspect of security focuses on the need to ensure only relevant persons would have access to every type of the digital assets. Measures must be taken to prevent unauthorised hands or eyes from entering the restricted space or accessing confidential information. There are incidents we heard from many parts of the globe where confidentiality of digital assets was compromised, such as leaks of military and official secrets, massive breach of personal data that impacted the public at large or an illegal interception of confidential communications systems.
2. The integrity of the cyber system. This second aspect of the CIA-triangle aims at preventing malicious or negligent disruption to the accuracy, completeness or truth of the system. Threats such as illegal intrusion ("hacking") of digital systems, unauthorised modification to the digital system, data theft as well as disinformation and misinformation are incidents that compromise with the integrity of a cybersecurity system. When threats such as these happen, the owner of the critical information system must be prepared to embrace the worst scenario of cybersecurity attacks. Therefore, access restriction and data preservation mechanisms must take place and must be enforced by law to ensure abuses can be effectively prevented or prosecuted.
3. The availability of system's security. This third objective of cybersecurity perceives that any interruption to the smooth working of digital system of a country or an organisation must be prevented, quickly detected or otherwise responded to. This is because such interruption will not only stop or slow down the system's function, but certainly when it comes to the CII, this may cause disturbance to public service delivery and may therefore create massive disturbance to public safety or economic chaos. Thus, threats such as sabotage and shutting down of the system, malicious downtime and the denial of services (DOS) should be perceived as serious disturbances to national security.

2. Threat to Cybersecurity and Critical Infrastructure in Malaysia

Malaysian cyberspace has never been a quiet zone. The country's National Cyber Security Agency (NACSA) under the National Security Council, Prime Minister's Office, revealed that the cyberattack trend has been increasing between 2016 and 2022. The trend includes

Distributed Denial of Service (DDoS), intrusion malware infection, malware hosting and advance persistent threats. NACSA reported 7192 incidents of cybersecurity in 2022, an increase from 5575 reported a year earlier.[2]

In the beginning of 2024, the Government of Malaysia initiated the Central Database Hub ("PADU") system as a key part of the country's digital transformation. The citizen data repository is an integrated socio-economic database that combines data from various government departments to provide a fair representation of each household's status in Malaysia (Prime Minister's Office Website, 2024). According to the release, PADU aims to ensure government services reach deserving recipients and prevent leakage in aid distribution and would therefore put an end to the issues of subsidy misappropriation, which currently costs the government RM80 billion. Barely three months after the announcement, we were informed that PADU has attracted a huge amount of cyberattacks. The Economic Affairs Minister revealed that there were two million weekly cyberattack attempts were put up against PADU database (*The New Straits Times*, 11 March 2024). Meanwhile, the defense minister warned that there were over 3000 cyberattacks made daily against the Malaysian cyberspace (*The New Straits Times*, 30 March 2024). These are perhaps just a tip of an iceberg we can never be sure of. But we know that the Malaysian cyberspace is never a quiet and peaceful playfield.

If this phenomenon is allowed to proceed, we may certainly end up losing. Public trust erodes, businesses slow down, privacy loses its meaning and our global competitiveness suffers. The most tangible impact will be felt by our national critical information infrastructure (CII). CII are those computer or information systems that are so critical that their disruption may cause detrimental impact on the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the government functions.

Take for example two incidents affecting the system of public transport. In Malaysia, Kuala Lumpur International Airport ("KLIA")'s Total Airport Management System (TAMS) was disrupted by a technical glitch that caused system network failure on August 21, 2019. The system failure lasted for several days, affecting multiple systems including flight information display, check-in counters, WiFi availability, baggage-handling system and immigration process. This had in turn created dozens of flight delays and long passenger queues in both international terminals. Malaysia's Transport Minister reportedly refuted any elements of sabotage and told the members of parliament that the outage was because the 21-year-old core network switches (CNS) system that was never changed since KLIA began operations in 1998

[2] This is what was reported by the Government in the Parliament back in March 2024 (Hansard Dewan Rakyat, DR 27/3/2024, p. 37).

(Malay Mail, 2019). In a separate and a more recent incident, a series of disruptions occurred to Prasarana Malaysia's LRT signalling system for more than a week in November 2022. In one of the incidents, the operator company revealed that some trains "disappeared" intermittently from the monitoring screen of the LRT operation and control centre, posing a huge hazard (The Star, 2022).

The incidents mentioned highlight the vulnerability of Critical Information Infrastructure (CII) to a wide range of cybersecurity threats, stemming from both intentional attacks and unintentional system failures. Essential sectors including government operations, telecommunications, utilities, public transport, financial systems, and healthcare facilities have all faced significant cybersecurity challenges. Malaysia, like many other countries, has experienced a series of incidents affecting the cybersecurity of its CII in recent times. To address these challenges, a multi-faceted approach incorporating tools, measures, policies, and laws is necessary to prevent, detect, and respond to cybersecurity threats effectively. Particularly crucial are well-crafted policies and robust legal frameworks, which are essential for equipping the nation to navigate the complex and evolving cyber landscape. These elements form the foundation of a comprehensive strategy to safeguard critical infrastructure against cyber threats.

3. Cyber Security Act 2024: An Attempt to Upgrade

With so many stories of cyber threats and cyberattacks incidents, the Malaysian lawmakers brought this issue to the primary stage of policy-making by introducing Cyber Security Act 2024 [Act 854]. The Act was first passed by the House of Representatives on 27th March 2024 and was finally gazetted on 26th June 2024. The Act is meant to enhance the national cyber security by providing for the establishment of the National Cyber Security Committee, duties and powers of the Chief Executive of the National Cyber Security Agency, functions and duties of the national critical information infrastructure sector leads and national critical information infrastructure entities and the management of cyber security threats and cyber security incidents to national critical information infrastructures, to regulate the cyber security service providers through licensing, and to provide for related matters.

There are a number of critical provisions under this Act, i.e.:

- The establishment of the National Cyber Security Committee whose functions include to plan, formulate and decide on policies relating to national cyber security; to decide on approaches and strategies in addressing matters relating to national cyber security; and to monitor the implementation of policies and strategies relating to national cyber

security. Besides, the Committee will be able to advise and make recommendations to the Federal Government on policies and strategic measures to strengthen national cyber security; to give directions on matters relating to national cyber security; and to basically oversee the effective implementation of the Act (Cyber Security Act 2024, 2024).

- The classification of the National Critical Information Infrastructure (NCII) sectors to include eleven sectors, namely government; banking and finance; transportation; defence and national security; information; communication and digital; healthcare services; water, sewerage and waste management; energy; agriculture and plantation; trade, industry and economy; and science, technology and innovation (Cyber Security Act 2024, 2024).

- Designation of NCII sector lead and NCII entity. The Act empowers the Minister, upon the recommendation of the Chief Executive, to appoint any Government Entity or person to be the NCII sector lead (Cyber Security Act 2024, 2024: Section 15). Subsequently, the NCII sector lead may designate any Government Entity or person who owns or operates a national critical information infrastructure as a NCII entity (Cyber Security Act 2024, 2024: Section 17).

- The Act requires cyber security service provider who provides a cyber security service to NCII entity to obtain a special license (Cyber Security Act 2024, 2024: Section 27).

4. Statutory Duties of the NCII Entity

The legislation sets some statutory duties for the entities (government or non-government alike) designated as National Critical Information Infrastructure (NCII) entity. Those duties are quite comprehensive, consisting of both preventive and responsive actions that seek to ensure the objectives of cybersecurity for the primary players in Malaysia. Those duties include the following:

1. Duty to provide information relating to national critical information infrastructure (Cyber Security Act 2024, 2024, Section 20). This necessarily means that NCII entity are, when required, bound to disclose information about their critical computer or computer system which covers both information technology and operational technology system.

2. Duty to implement code of practice (Cyber Security Act 2024, 2024: Section 21). Under this provision, a NCII entity shall implement the measures, standards and processes as specified in the code of practice to ensure the cyber security of the national critical information infrastructure owned or operated by the national critical information infrastructure entity.

3. Duty to conduct cyber security risk assessment and audit. A NCII entity are obliged undet the new law to conduct a cyber security risk assessment in respect of the NCII owned or operated by such entity in accordance with the code of practice and directive. Apart from that, NCII entity shall ensure audit is carried out by an auditor approved by the Chief Executive to determine the compliance of the NCII entity with this requirement of the Act (Cyber Security Act 2024, 2024: Section 22).[3] The risk assessment and audit shall be held in a manner and time to be prescribed by the Authority.

4. Duty to give notification on cyber security incident. If it comes to the knowledge of a NCII entity that a cyber security incident has or might have occurred in respect of the NCII owned or operated by the NCII entity, the entity shall notify the Chief Executive and its NCII sector lead of such information within the period and in such manner as may be prescribed (Cyber Security Act 2024, 2024: Section 23).[4]

5. Participation in cyber security exercise held by the Chief Executive is necessary for the purpose of assessing the readiness of any NCII entity in responding to any cyber security threat or cyber security incident (Cyber Security Act 2024, 2024: Section 24).

5. Conclusion

Cyber Security Act 2024 is meant to provide a coordinated national mechanism to defend Malaysia's NCII by outlining various preventive, detective and responsive measures to protect our cyberspace. Among those preventive and detective measures are the obligations for the

[3] Cyber Security Act 2024, section 22. The corresponding Regulations 2024 prescribed that the cyber security risk assessment has to be conducted at least once in a year, while the compliance audit at least once in two years.

[4] Cyber Security Act 2024, section 23. The corresponding Regulations 2024 stated that the cyber security incident notification must be made immediately, and within six hours some initial information need to be reported to NACSA. Subsequently, more thorough report needs to be submitted within fourteen days after the first initial report.

NCII entity to conduct cyber security risk assessment and audit as well as undertaking cyber security hygiene and exercises. Furthermore, as part of responsive measures, the duty to notify cyber security incident is crucial. Failure to do those obligations constitutes an offence under the Act.

All these mechanisms introduce new norms of cyber security in Malaysia. Most, if not all, of data breaches in the past came to our attention only long after they happened, and often through third party channels. This would hamper any effort to prevent the harm or losses to the Malaysian NCII sectors as well as individuals. The Act is hoped to bring a loud and clear message about Malaysia's aim to achieve a national cyber resilience and cyber sovereignty as outlined by the Government's Malaysia Cyber Security Strategy 2020-2024. For this end, we hope the new Cyber Security Act 2024 paves the way for a better security in Malaysian digital economy.

Cybersecurity is more than just a policy product; it is a national journey worth travelling. It requires a long-term plan that visions the whole aspects of the national objective, economic growth and sustainability and social wellbeing. To achieve this, cybersecurity law and policy shall be firmly rooted in our commonly shared values and tradition as well as being driven by civility and innovation.

References

ITU. (2008). ITU-T X.1205: Overview of Cybersecurity. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items (Accessed on December 20, 2024).

ITU. (2024). G20: Digital connectivity to advance sustainable development, ITU News Magazine, 1/10/2024, https://www.itu.int/hub/2024/10/g20-digital-connectivity-to-advance-sustainable-development/ (Accessed on December 20, 2024).

Malay Mail. (2019). No Sabotage in KLIA Systems Disruption, Transport Minister Insists. (October 29, 2019), https://www.malaymail.com/news/malaysia/2019/10/29/no-sabotage-in-klia-systems-disruption-transport-minister-insists/1804770 (Accessed on December 20, 2024).

NACSA. (2024). Cyber Security Act 2024. https://www.nacsa.gov.my/act854.php, (Accessed on December 20,2024).

Prime Minister's Office Website. (2024). PADU ensures Government services will be enjoyed by deserving recipients – PM Anwar. 2 January 2024, https://www.pmo.gov.my/2024/01/padu-ensures-government-services-will-be-enjoyed-by-deserving-recipients-pm-anwar/ (Accessed on December 20, 2024).

The Star. (2022). Trains 'disappeared' from Our Control Screens on Nov 8, Says Prasarana. (November 10, 2022), https://www.thestar.com.my/news/nation/2022/11/10/trains-039disappeared039-from-our-control-screens-on-nov-8-says-prasarana (Accessed on December 20, 2024)

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. 11/1/2024, https://www.weforum.org/publications/global-cybersecurity-outlook-2024/ (Accessed on December 20, 2024).

İKİNCİ KARABAĞ SAVAŞI SONRASI OLUŞAN YENİ POLİTİK DENGELER: "TEK YOL TEK KUŞAK" PROJESİ EKSENİNDE AZERBAYCAN'IN YENİ BÖLGESEL DİJİTAL MERKEZE DÖNÜŞMESİ

Nigar GULIYEVA*

Orcid: 0000-0002-6266-5353

Özet

Azerbaycan'ın güney-batısında yer alan Karabağ; Ermenistan'ın 1991-1993 yılları arasında Azerbaycan ile girmiş olduğu savaş sonucu 30 yıl denetim altına almıştır. Bu sürede, bir milyondan fazla sivil Azerbeycan halkı, zorla yurtlarından edilerek sürülmüş, bölgede kalmalarına izin verilmemiştir. Çok sayıda Azerbeycanlı sivil halk katledilmiş ve milyar dolarlarla ifade edilebilecek maddi zararlar ortaya çıkmıştır. Bölgede bu denli siyasi bir denge değişimi Güney Kafkasya'ya da yansımış; bu da siyasi istikrarsızlık ve çekişmelerin ard arda yaşanmasına neden olmuştur. Soruna uluslararası hukuk çerçevesinde çözüm arayışları ve buna ilişkin girişimler sonuçsuz kalmış. Azerbaycan'ın, Birleşmiş Milletlerin uluslararası hukuk çerçevesinde yaptığı tüm girişimler sonuçsuz kaldığı gibi barışçıl çözüm önerileri de yok sayılmıştır. Süreç bölgedeki Azerbaycanlı yurttaşlar açısından çekilmez bir hal almış, uluslararası alınan hiçbir çözüm Ermeni tarafınca uygulanmadığı gibi, Ermenilerin yerel halk üzerindeki siyasi-sosyal baskı, şiddetini arttırmıştır. Eylül 2020`de savaş başlamış 44 gün süren bu savaş sonucunda Azerbeycan bölgenin kontrolünü ele geçirmiştir. Azerbaycan'ın bu savaş sonrası elde ettiği kazanımlar hem siyasi itibarını geri kazandırmış hem bölgede bir güç olduğunu ispatlamıştır. Bu sonuç, bölgede jeopolitik bağlamda siyasi ve ticari dengelerinin değişmesine neden olmuştur. Bu minvalde Çin tarafından 2013 yılında açıklanan "Tek Yol Tek Kuşak" projesine Azerbaycan dahil edilmiştir. Bu bağlamda bu çalışma, Azerbaycan'ın bu proje içine dahil olarak jeopolitik anlamda kazandığı önemi ve dijital jeopolitikte elde edeceği kazanımları inceleyecektir.

Anahtar kelimeler: Karabağ Savaşı, Toprak Bütünlüğü, Jeopolitik Gerçek, İpek Yolu, Tek Yol Tek Kuşak.

* Teacher at Baku Higher Oil School, Nigar_guliyeva1984@yahoo.com

NEW GEOPOLITICAL REALITIES AFTER THE SECOND KARABAKH VICTORY: TURNING AZERBAIJAN INTO A REGIONAL DIGITAL HUB WITHIN THE FRAMEWORK OF THE "BELT AND ROAD INITIATIVE"

Abstract

Located in the southwestern part of Azerbaijan, Karabakh was under Armenian occupation for 30 years as a result of the war between Armenia and Azerbaijan from 1991 to 1993. During this occupation, over one million Azerbaijani civilians were forcibly displaced and deprived of their homes. Hundreds of thousands of Azerbaijani civilians were killed, and the region suffered economic damage worth billions of dollars. This shift in political balance had profound repercussions across the South Caucasus, resulting in ongoing political instability and conflicts. Efforts to resolve the issue within the framework of international law and through diplomatic initiatives remained fruitless. Armenia's persistent violations of ceasefire agreements further escalated tensions. Despite Azerbaijan's attempts to seek peaceful solutions and its adherence to United Nations-backed legal processes, these efforts were disregarded, exacerbating the dire conditions for Azerbaijanis in the region. Additionally, the Armenian side intensified its socio-political oppression and violence against the local Azerbaijani population. Anticipating that neither international nor national mechanisms would resolve the conflict, Azerbaijan launched a military operation in September 2020. This 44-day campaign successfully liberated its occupied territories. The victory restored Azerbaijan's political prestige and demonstrated its strength to neighbouring countries, leading to significant shifts in the geopolitical and economic dynamics of the region. In this context, Azerbaijan was integrated into China's "Belt and Road Initiative," unveiled in 2013. This inclusion highlights Azerbaijan's strategic importance in regional geopolitics. Accordingly, this study will examine the geopolitical significance and the digital geopolitics Azerbaijan has gained by becoming part of this initiative.

Keywords: Karabakh War, Territorial Integrity, Geopolitical Realities, Silk Road, One Belt One Road, Digital Infrastructure

1. Giriş

Sovyetler Birliği'nin dağılmasıyla Ermenistan "ulusların kendi kaderini tayin hakkı" ilkesini kendi perspektifince yorumlayarak 1991-1993 yılları arasında Azerbaycan topraklarının %20'ye yakınını kendi kontrolü altına almıştır. Uzun yıllar süren ulusal ve uluslararası sorunun

hukuk çerçevesinde çözülmesi amaçlansa da bu amaca ulaşılamamıştır. Birleşmiş Milletler Güvenlik Konseyi (BMGK) tarafından başvurular üzerine çözüme yönelik alınan 822, 853, 874, 884 numaralı konsey kararları mevcut olmasına rağmen; Ermenistan bu barışçıl çözümlere yanaşmamış uluslararası hukuku da yok saymıştır. Karabağ sorununa ilişkin çözüm arayışları, ulusal ve uluslararası düzeyde çeşitli girişimlerle desteklenmiştir. 1992 yılında ABD, Fransa ve Rusya'nın da yer aldığı Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) Minsk Grubu, bu çabaların başlıca platformlarından biri olmuştur. Ayrıca, 1994 yılında Azerbaycan ve Ermenistan arasında imzalanan Bişkek Ateşkes Anlaşması, bölgedeki çatışmaların sona erdirilmesi amacıyla hayata geçirilmiştir. Ancak, Ermenistan'ın bu karar ve anlaşmalara uymaması, bölgede kalıcı barışın sağlanmasını engellemiştir.

Tarihsel Süreç

Coğrafi konum olarak incelediğimizde Azerbaycan'ın kuzeyinde Rusya, güneyinde İran, güneybatısında Türkiye Cumhuriyeti, doğuda Hazar denizi, batıda Ermenistan ile sınırları mevcut olmakla Tarihi İpek Yolu üzerinde bulunmaktadır. Avrupa ile Asya'yı ve özelliklede Türkiye ile diğer Türk Cumhuriyyetleri arasında bir güzargah olması ülkenin statejik konumunu güçlendirmektedir. (Nerimanlı, 2015: 2) (Bkz Resim.1)

Resim.1 Kaynak: Tebriz Nerimanlı, "Karabağ Savaşının Türkiye, Azerbaycan ver Ermenistan İçin Sosyal ve Ekonomik Etkileri"

Yakın dönemin tarihine başvurduğumuz zaman, 1813 yılında Gülüstan ve 1828 yılında Türkmençay anlaşmaları, Azerbaycan'ı Kuzey ve Güney olarak ikiye bölünmesini sağlamıştır. Bu bölünmenin ardından devam eden tarihi süreçte Sovyetler Birliği'nin 1922 yılında kurulmasıyla Azerbaycan, Ermenistan Sovyet yönetimi altına girdi. Karabağ bölgesi 1923 yılında Azerbaycan Cumhuriyeti'ne bağlı özerk bir bölge statüsü kazanmıştır. Bu karar hiçbir zaman Ermenistan yönetimi tarafından kabul edilmemiştir. 1980'lerde ise Sovetler Birliği'nin

zayıflaması ve ardından dağılmasıyla sonuçlanan süreçte ise sonuç olarak Karabağ Sorunu gün ışığına çıkmıştır. (BBC News, 2020)

1991 yılında Ermenistan'ın bağımsızlığı ilan edildikten sonra, Dağlık Karabağ Ermenileri ayrılma isteklerinde bulunarak, 10 Aralık 1991 yılında Dağlık Karabağ Ermenileri referandum ile Azerbaycan'dan ayrılmak için oy kullanmış, yapılan referandumdan sonra Dağlık Karabağ'ın bağımsızlığını ilan etseler de, bu girişim uluslararası toplumda karşılık bulamamıştır. Bölgede çıkan çatışmalar 1992 yılında Ermenistan ordusu ve Dağlık Karabağ Ermenileri ile Azerbaycan ordusu arasında sıcak çatışmalara dönüşerek Sovetlerin dağılmasından sonra Kafkasya'da yaşanan büyük savaşlar arasında yer almış.

1994 yılından ateşkes ile başlayan ve 30 yıl süren Karabağ sorununa uluslararası hukuk çerçevesinde çözümün bulunamaması Azerbaycan tarafının barışçıl ümitlerini yitirmesine neden olmuştur. Bundan dolayı Azerbaycan hükümeti 2010 yılından itibaren uluslararası hukuktan kaynaklanan haklarına dayanarak askeri gücünü kullanabileceği yönünde deklarasyonlar yapmaya başlamıştır. Bu deklarasyonlar ile Dağlık Karabağ ve çevresinde bulunan yedi bölgenin (ilçe) işgaline karşı gerekli siyasi, diplomatik ve askeri yöntemlere başvuracağını uluslararası alanda her platformda belirtmesine yani işgale karşı bir askeri güç kullanımının sinyallerini vermeye başlamıştır. Sovetler Birliği'nin dağılması ile Karabağ Ermenileri "ulusların kendi kaderlerini tayin hakkı" ilkesini meşrulaştırmak için bölgede bölücü eylemlere başvurmayı tercih etmişler. Ancak Güney Kafkasya'da Sovetler Birliğinin dağılmasından sonra uyulması gereken tek ve önemli ilke "*sınırların dokunulmazlığı*" ilkesi olduğu bilinmektedir. Uluslararası hukuk çerçevesinde konuyu değerlendirdiğimizde Ermenistan'ın selfdeterminasyon argümanları "kendi kaderini tayin hakkı ilkesi'nın" arkasına sığınarak Azerbeycan'nın toprak bütünlüğünü ihlal ettikleri ve uluslararası hukuk normlarına aykırı davrandıkları kabul edilmektedir. (Kurban ve Çümen, 2020: 3)

Ermenistan devletinin bu yaklaşımı uluslarası alanda kabul görülmese de ve uluslararası hukuk normlarına aykırı davranmış olsa da hiçbir güç Ermenistan'ın Azerbeycan'nın toprak bütünlüğünü ihlal etmesinin ve bölgede barışı tehdit altına almasını engelleyememiştir. *28 Aralık 1991 yılında Hankendi, 26 Şubat 1992 yılında Hocalı (bu bölgede, insanlık dışı eylemler sergilenerek Azerbeycan Türklerine karşı soykırım yapılmıştır), 8 Mayıs 1992 Şuşa, 18 Mayıs Laçın, 2 Ekim 1992 Hocavend, 2 Nisan 1993 Kelbecer, 7 Temmuz 1993 Ağdere, 23 Temmuz 1993 Ağdam, 23 Ağustos 1993 Cebrail, 23 Ağustos 1993 Fizuli, 31 Ağustos 1993 Gubadlı, 29 Ekim 1993 Zengilan* Rusların desteğini alan Ermeniler tarafından işgal edilmiştir. (Anadolu Ajansı, 2020)

Uluslararası düzen çerçevesinde değerlendiriğimiz zaman 1992 yılında AGİT girişimi ile Minsk Grubu oluşturulmuştur. ABD, Fransa, Rusyan'nın eş başkanlarından oluşan bu Minsk Grubu günümüze kadar Karabağ sorununu kendi çıkarları bağlamında ele aldıkları için sorunun çözümüne ilişkin ciddi adımlar atılmamıştır. Bu grup sadece 2020 yılına kadar mevcut statükonun devam etmesine neden olmuştur. Bölgede her bir devletin kendi çıkarları olduğu için sorunun çözülmesinde BM kararlı çerçevesinde sorun değerlendirilmemiş, zira kendi iç ve dış siyasi çıkarları çerçevesinde sorunu ele almayı tercih etmişlerdir. (Sıtkı, 2020:3) Halbuki 30 Nisan 1993 yılında BM Güvenlik Konseyi Ermeni birliklerin işgal ettikleri Azerbaycan topraklarından çekilmeleri için dört (822, 853, 874, 884) numaralı kararlar kabul etmiştir. (Anadolu Ajansı, 2020)

30 yıllık zaman diliminde Karabağ sorununa Minsk Grubu'nun sunmuş olduğu çözumler arasında 2007 yılında kabul edilmiş Madrid Prenseplerini de göstermek mümkündür. (Haber 7, 2010) 30 sene devam eden sorunun uluslararası hukuk çerçevesinde çözülmesi hedeflenmiş olsada, Karabağ sorunu somut sonuçlar doğurmamış ve buda bölgedeki gerilimin artmasına yol açmıştır. Ermenistan'ın, Azerbaycan-Ermenistan sınırındaki ateşkes ihllaleri gerilimi artırarak çözüm arayışlarını engellemiştir. Ermenistan'ın Azerbaycan'ın sivil yerleşim yerlerini hedef alması, çözüm sürecini daha da karmaşık hale getirerek barışa giden çabaları zayıflatmıştır.

Azerbaycan hükümetinin 2010 yılında başlayan bu söylemleri, Türkiye gibi komşu ve dost ülkelerin de desteği ile askeri eğitim, askeri güç ve askeri teknolojisini geliştirme yönünde ilerlemiştir. Hükümet hem askeri bütçesini arttırmış hem de gerekli askeri eğitim ve teçhizat eksiliklerini tamamlamıştır. Ancak Azerbaycan hükümeti için saldırıların başlamasını ve Dağlık Karabağ bölgesinin işgalini tetikleyen olay, Azerbaycan'ın stratejik bölgesi olan Tovuz bölgesine Temmuz 2020 de Ermenilerin saldırısı ve bu saldırılar sonrasında 27 Eylül 2020 tarihinde de bir ateşkes ihlalinin daha vuku bulması olmuştur. Akabinde 27 Eylül 2020 tarihinde başlayan ve 44 gün devam eden işgal süresi Azerbaycan'ın İkinci Karabağ Zaferi olarak sonuçlanmıştır. Bu zafer ile Azerbaycan topraklarını işgalden kurtararak toprak bütünlüğünü yeniden sağlamıştır.Karabağ sorununun çözüme kavuşması, bölgede barışın sağlanması ve Azerbaycan'ın kendi toprak bütünlüğünü yeniden sağlamış olması beraberinde yeni imkanlara da yol açmıştır. İkinci Karabağ Savaşı 10 Kasım 2020 tarihinde Azerbaycan Cumhurbaşkanı İlham Aliyev, Ermenistan başbakanı Nikol Paşinyan ve Rusya Devlet Başkanı Vladimir Putin tarafından "Dağlık Karabağ Ateşkes Antlaşması'nın" imzalanması ile sonuçlanmıştır. Bu anlaşmada dikkat çeken maddelerden biri Azerbaycan ile Nahçivan'nı birbirine bağlayacak olan *Zangezur Koridoru'nun* güney rotası olarak tüm ulaşımlar için açılmasıdır. Bu ateşkes antlaşması ile Azerbaycan siyasi itibarını kazanıp bölgedeki gücünü

ortaya koymayı başarmıştır. Bundan dolayı uluslararası alanda bölgedeki güçlü devletler tarafından göz önüne alınması kaçınılmaz olmuştur.

Hazar Denizi'ne kıyısı olan Azerbaycan, doğal kaynaklar konusunda oldukça zengindir. Bu yüzden ülkeye birçok küresel ve bölgesel aktör ilgi duymaktadır. Çin'in Azerbaycan'a olan ilgisinin temeli Çin`den Avrupa`ya uzanan bir demiryolu hattı geliştirmeye çalışmasından kaynaklanmaktadır. Bunun dışında Azerbaycan üzerinden gidecek güzergâh Çin'in mallarının daha güvenli şekilde taşınmasını sağlayacaktır. Ayrıca Azerbaycan'ın sahip olduğu doğal kaynakları ve bölgedeki gücü de Çin'in Azerbaycan'a odaklanmasına vesile olmaktadır. Azerbaycan ile ilgili belirtilmesi gereken bir diğer önemli husus ise, Azerbaycan'ın Tek Yol Tek Kuşak projesinde yeni katılımcıların dahil edilme sürecinde önemli ve kararlı bir jeopolitik, politik, kültürel ve ulaşım alanı olması durumudur.

SSCB'nin dağılması ile uluslararası arenada tekrar söz hakkını alan özerk kullanan Azerbaycan, Bakü-Tiflis-Ceyhan petrol boru hattı, Güney Gaz Koridoru ve Trans-Hazar Uluslararası Taşımacılık Rotası dahil olmak üzere bir dizi önemli bölgesel ve kıtalararası enerji ve ulaşım projelerini ya aktif olarak başlatmış ya da katılmıştır. Ülkenin kalkınmasında önemli rol oynayan enerji kaynakları Azerbaycan'ı Güney Kafkasya'nın en güçlü ülkelerinden biri haline getirmiştir. Bununla beraber Azerbaycan tarihi ipek yolu üzerindeki konumu ile Avrupa ile Asya kıtasını birbirine bağlaması yüzyıllardır vazgeçilmez ticari noktalardan biri olmasına neden olmuştur.

Dijital İpek Yolu kapsamında konuyu ele aldığımızda, Karabağ sorunun çözüme ulaşması bölgede barışın sağlanmasını ve yeni işbirliklerinin oluşmasını imkan sunmakta. Dijital İpek Yolu projesi Asya ile Batı arasında yeni bir ekonomik ve kültürel bağ kurma vizyonunu taşımakta. Bu proje, eski İpek Yolu'nun dijital çağda yeniden hayat bularak şekillenmesi olarak değerlendirilmekte. Fiziksel malların taşındığı geleneksel yolla beraber, veri transferi ve dijital hizmetlerin hızla aktarılmasını sağlayarak Dogu ile Batı`nı bir birine bağlayan dijital altyapıların geliştirilmesi ön plana çıkmaktadır.

Çin'in Bir Kuşak Bir Yol projesi kapsamında, dijital koridorların kurulmasıyla dijital altyapı yatırımları ve teknolojik işbirlikleri ile bu projenin hayata kecmesi hedeflenmekte. Dijital İpek Yolu, internet erişimi, bulut bilişim, YZ, e-ticaret, dijital ödemeler gibi alanlarda ülükeler arası işbirliklerini güçlendirerek, bölgesel ve küresel ticaretin daha verimli hale gelmesini sağlamaktadır. Bu proje bölgesel barışın ve ekonomik kalkınmanı teşvik etme potansiyeline sahiptir. Belirtmek gerekiyor ki, teknolojik çözümler, bölgede sınır aşan işbirliklerinin önünü açarak, veri paylaşımını teşvik ederek, diplomatik ve ekonomik ilişkilerin gelişmesine ve ülkeler arasında daha hızlı ve şeffaf iletişim imkânları sunma potansiyeline sahip. Bu bağlamda,

Dijital İpek Yolu projesi, Azerbaycan'ın güvenlik ve savunma stratejisini güçlendirerek bölgede istikrarın ve işbirliğinin gelişmesinide sağlamaktadır.

Kadim İpek Yolu Projesi ve Tarihsel Yolculuğu

İpek yolu (die seidenstrasse) kavramı ilk defa 1877'de Alman coğrafyacı Ferdinand von Richthofen tarafından kullanılmıştır. (Chin, 2013: 196) Yakın bir zamana kadar bu ticaret yolları için hiçbir zaman İpek Yolu tabiri kullanılmamıştır. O dönemlerde Semerkand Yolu, Kaşgar Yolu, Tebriz Yolu gibi gidilen güzergah veya Kuzey Yolu, Güney Yolu, Batı Yolu gibi ilgili yönler yola adını verirdi. (Tarihi, Bugünü ve Geleceğiyle İpek Yolu, 2015) Çin'in Xian şehrinden başlayarak Orta Asya, Anadolu ve Akdeniz aracılığıyla Avrupa'ya kadar uzanan kadim ticaret yolu tek bir rotadan oluşmamakta tam aksine bütün Asya'yı birbirine bağlayan büyük bir ağ biçiminde örgütlenmişti. Bu açıdan Asya'yı dünya ekonomisine entegre eden bir işlevi olan İpek Yolu, özellikle 2. yüzyıl ve 16. yüzyıl arasında tartışmasız bir ekonomik güç merkezi konumunda olmuştur. Oueh'e göre o dönemde dünyanın iktisadi sıklet merkezi Asya'ydı. Ekonomik güç daha sonra Atlantik Okyanusu'nun ortasına kayınca İpek Yolu'nun önemi azalmıştır. (Güven, 2015) Jean-Paul Roux'a göre ise eskiden İpek Yolu, Orta Asya'nın servetiydi. Bu yolun kapanmasıyla bölgede felaket çanları çalmış ve bu yolla birlikte kültürü de yok olmuştur. Zamanla daha ekonomik ve güvenli yolların bulunması ile önemini büyük ölçüde yitiren İpek Yolu, günümüzde ise başta Çin olmak üzere Asya'da birçok ülkenin ekonomik olarak yükselişe geçmesi ile yeniden önemli hale gelmiştir. (Özdaşlı, 2015: 585)

Azerbaycan, tarih boyunca bilinen en eski ve en gelişmiş ilk ticaret yolu olan İpek Yolu üzerinde bulunmaktadır. İpek Yolu ise ismini çok eski çağlarda Çin İpeği'nin tüm dünya da olan popülaritesinden gelmektedir. Bu ticari yol aracılığı ile kervanlarla taşınarak batıya ulaştırılan ipek kumaşının ismi nedeni ile bu yol bu isimle anılmaktadır. Coğrafi konumu nedeniyle, eski çağlardan beri doğu ile batı arasında bir köprü işlevi gören Azerbaycan, İpek Yolunu en önemli kavşak noktalarından biri olmuştur. Orta Çağda, İpek Yolu Çin'den başlayıp Orta Asya'ya, oradan Azerbaycan'a ve Anadolu'ya geçerek Trakya üzerinden Avrupa'ya uzanmıştır.

Bu tarihi bilgilerin ardından İkinci Karabağ Savaşı sonrası Azerbaycan'ı bölgedeki siyasi ve ticari güç dengelerini değiştirmesi nedeni ile tekrar değerlendirmemiz gerekecektir. Bu hususta ilk ele alınması gereken siyasi gelişme savaş sonrası bir Zengezur Koridorunun önemidir.

Zengezur Koridoru veya Nahçıvan Koridoru, Ikinci Karabağ Savaşı`nın Azerbaycan tarafından kazanılmasının ardından Azerbaycan ve Ermenistan arasında imzalanan ateşkes antlaşmasının 9. Maddesi gereğince Azerbaycan ile ekslav parçası olan Nahçivan Özerk Cumhuriyeti

arasında bağlantıyı kuracak olan koridordur. Zengezur Koridoru Azerbaycan`ın ana kısmını onun bir parçası olan Nahçivan Özerk Cumhuriyeti ile bağlayan bir ulaşım koridorudur. Daha geniş anlamda, Zengezur Koridoru, Nahçivan'ı Azerbaycan ve Türkiye ile bağlayarak, Nahçıvan'dan Türkiye'ye, oradan Akdeniz üzerinden diğer batı ülkelerine, bir sözle, bölge ülkelerine Çin, Orta Asya-Azerbaycan-Türkiye-Avrupa transit-ulaşım hattını kullanma imkânı sağlamaktadır. Aslında anlaşılacağı üzere, sadece Azerbaycan ile Nahcivan'ı değil, Türkiye ile Azerbaycan'ı ve Azerbaycan üzerinden Türkiye'nin diğer Türk Cumhuriyetleri ile ulaşımını sağlayarak, uzak doğu'ya kadar ulaşım anlamına gelmektedir.

İkinci Karabağ Savaşının ardından küresel projelerden biri olan, 2013 yılında Çin tarafından açıklanan ve faaliyete geçen "Tek Yol Tek Kuşak" projesidir. Bu proje 6 bölgeyi kapsayarak, bölge ülkeleri ile "*Alt Yapı ve Tesis Bağlantıları", "Yatırım ve Ticaret İlişkilerin Gelişmesi", "Finansal Entegrasyon", "Kalkınma Politikaların Koordinasyonu", "Sosyal ve Kültürel Alanda İşbirliyin Gelişmesi"* alanlarında işbirliğinin yapılmasını hedeflemektedir. Bu proje kapsamında dikkat çeken *Alt Yapı ve Tesis Bağlantıları* projesidir ki, bölge ülkeleri ile yapılacak olan işbirliğinde Çin *Dijital İpek Yolunu* tesis ederek Avrasya'daki etkisini artırmayı planlamaktadır. Bu proje yeni *Dijital Silah Yarışı* olarak da değerlendirilir ve bu yarış ABD'nin, Çin'in bu teknolojileri kullanmaması için askeri ve güvenlik risklerini savunarak ilerlemesini engellemeye amaçlamaktadır.

Çin Dışişleri Bakanı Jinping'in ifadesiyle "yeni yüzyılda yeni bir anlam ve mahiyetlerle doldurulması" amaçlanan Yeni İpek Yolu Projesi'nin doğuyu batıya bağlaması ile Çin ekonomisine büyük bir güç kazandıracaktır. (Sputnik Turkiye, 2015) Pekin kendisini merkeze aldığı bu yeni ekonomik atağı ile dünya pazarına daha hızlı ve ucuz yollardan ulaşmayı, küresel kriz nedeniyle talep azalması yaşayan ekonomisine güç kazandırmayı, ekonomik büyümeye paralel olarak artan hammadde ihtiyacını kolay ve ucuz yollardan karşılamayı amaçlamaktadır. Yalnızca taşımacılık hattı ile sınırlı olmayan bu proje ile İpek Yolu üzerindeki ülkeler arasında işbirliği ve ortak yatırımların artırılmasını amaçlamakta ve yolun bir ekonomik kuşak haline getirilmesini öngörmektedir. Bu haliyle proje, Çin'in dev pazarı ve yüksek performanslı üretim gücüyle birlikte Avrupa'nın sermayesi ve teknolojisi, Orta Asya'nın ise enerji kaynaklarını içeren çok yönlü bir katılımı ihtiva etmektedir. (Atlı, 2014: 76)

Tek Yol Tek Kuşak Girişimi`nin ilkeleri, genel çerçevesi, bölgesel işbirliği öncelikleri ve mekanizması açıklanmıştır. Buna göre; Çin`in bu yeni vizyonu çok kutuplu bir dünya eğilimini kapsayan, iktisadi küreselleşme, kültürel çeşitlilik, küresel serbest ticaret rejimi ve açık bölgesel işbirliği ruhu içinde açık dünya ekonomisini hedeflemektedir. Yayınlanan eylem planına göre bu girişim, kuşak üzerindeki ülkelerin ortaklıklarını güçlendirmek, bağımsız, dengeli ve

sürdürülebilir bir kalkınmayı teşvik etmek, bölgedeki ülkelerin kalkınma stratejilerini koordine etmek, yatırım ve tüketimi teşvik ile yeni iş olanaklarını ortaya çıkarmak gibi ekonomik saiklerin yanı sıra kültürlerarası iletişimi ve insani ilişkileri geliştirmek, ilgili ülke halkları arasında iletişimi, karşılıklı öğrenmeyi, güven ve karşılıklı saygı, barış ve refah içinde birlikte yaşama gibi insani değerleri de kapsamaktadır. Çin, bu yeni girişiminin Birleşmiş Milletler Şartı`nın amaç ve ilkeleri doğrultusunda beş ilkeden oluşan "barış içinde birlikte yaşama" prensibine dayandığını ifade etmektedir. Bunlar: ülkelerin egemenliği ve toprak bütünlüklerine karşılıklı saygı, karşılıklı saldırmazlık, içişlerine karışmama, eşitlik ve ortak yarar ile barış içinde birlikte yaşamadır. (Ministry of Foreign Affairs The People's Republic of China, 2015). Projenin altyapı ve mali giderlerinin karşılanmasına yardımcı olması için Çin'in öncülüğünde aralarında Türkiye, Azerbaycan, Kırgızistan'ın da bulunduğu 57 ülke ile Asya Altyapı Yatırım Bankası (AAYB) kurulmuştur. AAYB'ye başvuru yapan ülkeler arasında İngiltere, Almanya, Fransa gibi Avrupa'nın en önemli güçlerinin yanı sıra Suudi Arabistan, Ürdün gibi Ortadoğu'nun dikkate değer ülkelerin olması Çin'in artan ekonomik gücüne paralel olarak uluslararası alanda önemsenen bir ülke haline geldiğini göstermektedir. Yeni İpek Yolu Projesi (YİYP), Çin'in ucuz işgücü ile geniş pazar ağını Avrupa'nın sermayesi ve Orta Asya'nın kaynakları ile buluşturmayı hedefleyen çok yönlü bir küresel girişimdir. YİYP ile Çin, başta Orta Asya ülkeleri olmak üzere sınır ötesi ulaşım ve alt yapı projeleri geliştirerek hem bölge hem de dünya ekonomisi ile bütünleşme sürecini hızlandırmayı hedeflemektedir. Projenin, ekonomileri 21 trilyon dolara ulaşan kuşak üzerindeki 65 ülkenin ekonomik ve kültürel hayatına canlılık kazandırması beklenmektedir. Pekin'in "refah kuşağı" olarak tasavvur ettiği projenin ilgili ülkeler arasında iş birliğini, ortak yatırımları ve kültürel iletişimi arttırması beklenmektedir. (Özdaşlı, 2015: 588)

Azerbaycanda dijitalleşen bu dünyada yurt içi ve sınır ötesi telekomünikasyon projelerini takip ederek, önemli ulaşım merkezlerine dahil olarak bölgenin önemli *Dijital Merkezi* statüsünü kazanmayı hedeflemektedir. Bakü-Tiflis-Ceyhan petrol boru hattı, Güney Gaz Koridoru ve Trans-Hazar Uluslararası Taşımacılık Rotasından sonra *Dijital İpek Yolu* projesine dahil olmak Azerbaycan'a *Dijital Güzergâh* olma imkanını sağlayacaktır.

İkinci Karabağ Savaşına Giden Süreç

Karabağ sorununa uluslararsı hukuk çerçevesinde başta BM olmak üzere Minsk Grubu üye devletleri ve uluslarası toplum çözüm bulamamaları Azerbaycan'nın Türkiye'nin desteğiyle askeri eğitimini, güçünü ve teknolojisini geliştirmeye kararlı kılmıştır. 2003 yılından itibaren

Azerbaycan savunma giderlerine büyük bütçe ayırmaya başlamış, 16 Aralık 2005 tarihinde Azerbaycan Cumhurbaskanı İham Aliyev'in kararı ile Savunma Sanayi Bakanlığı'nın oluşturulmasına dair karar imzalanmıştır. Belirtmemiz gerekiyor ki, bölge bütünlüğünün korunması adına Azerbaycan ulusal güvenliği ve ulusal güç kapsamından haraketle ulusal güvenlik konsepti ve askeri doktrinlere yer vermiştir. 23 Mayıs 2007 yılında "Azerbaycan'ın Ulusal Guvenlik Konsepti", 8 Haziran 2010 yılında ise "Azerbaycan'ın Askeri Doktrini" yayınlanmıştır. (Şiriyev, 2010: 135)

2007-2014 yılları arasında Savunma Sanayi Bakanlığının üretim teknolojilerinin geliştirilmesi için 50'den fazla yeni üretim tesisleri kurduğu gözlemlenmiştir. 2014 yılı verilerine göre üretimin 26.3% oranında artdığı bilinmektedir. İmal edilmiş ve teslimi gerçekleşmiş savunma sanayi ürünlerinin 2014 yılı ile 2013 yılı verileri karşılaştırıldığı zaman %30 civarında artış sergilediği bilinmektedir. Global Firepower isimli kurumun askeri güç değerlendirmesinde 106 ülke arasında Azerbaycan 50. sırada yer alan ülke olarak değerlendirilerek, Güney Kafkasya da askeri savunması en güçlü olan ülke olduğu kabul edilmiştir. (Özalp, 2015: 122)

2010 yılı Azerbaycan'nın askeri harcamalarına bakıldığı zaman ise 1.42 milyar dolar artış görülmektedir. Belirtilen rakam 2004 yılında yapılan askeri harcamalarla kıyaslandığı zaman resmi Bakü'nun bu harcamaları üç katına çıkardığı bilinmektedir. Ayrıca Azerbaycan'nın 2010 yılında askeri harcamaları Erivan'ın aynı yıla ait milli bütçe tutarını da geçtiğini göstermektedir. "2012 SIPRI raporuna esasen, Azerbaycan'ın 2007-2011 döneminde silah ithaalatı, 2002-2006 dönemine göre %164 artmış ve Azerbaycan dünyada en çok silah ithaal eden 38'inci ülke olarak belirlenmiştir." (Bilgin, 2020: 4)

2016 yılından itibaren Bakü ile Ankara arasında gelişen savunma entegrasyonu, askeri işbirliği Bakü lehine değişerek Azerbaycan'a önemli kazanımlar sağlamıştır. Karabağ savaşında kullanılan Türk yapımı İHA'lar ve 120 km menzile sahip TRG-300 Kaplan Füzesi gibi önemli silahlar Azerbaycan ordusunun kabiliyetini arttırarak sahada önemli avantajlar sağlamıştır, nitekim 2016 yılında Ermenistan ile yaşanan çatışma Azerbaycan'ın güvenlik stratejisindeki gelişmelerin somut örneği olarak değerlendirilmektedir. (Bilgin, 2020: 4)

10 Kasım 2020 yılında imzalanmış olan "Dağlık Karabağ Ateşkes Antlaşmasının" değerlendirdiöimizde, bu anlaşmanın ardından öne çıkan önemli antlaşmalardan birinin de "Şuşa Beyannamesi" olduğunun altını çizmek gerekmektedir. Bölgede 15 Haziran 2021

tarihinde imzalanmış olan Şuşa Beyannamesi, Ankara ve Bakü arasında imzalanan önemli belge niteliğindedir. 15 Haziran NATO zirvesinin hemen ardından Türkiye Cumhuriyeti Cumhurbaşkanı Recep Tayyip Erdoğan'ın, Azerbaycan'ı ziyaret etmesi sırasında Azerbeycan Cumhurbaşkanı İlham Aliyev ile birlikte Şuşa şehrini ziyaret ederek her iki ülke aralarında Şuşa Beyannamesi'ni imzalamış böylelikle Azerbaycan'ın yanında olduklarını, müttefik olduklarını bu belge ile tüm dünyaya ilan etmişlerdir. Şuşa Beyannamesi tam adıyla "Türkiye Cumhuriyeti ile Azerbaycan Cumhuriyeti Arasında Müttefiklik İlişkileri Hakkında Şuşa Beyannamesi"dir. Azerbaycan ve Türkiye arasında imzalanmış olan ve "müttefiklik" kelimesi geçen ilk önemli belgedir. (Anadolu Ajansı, 2021)

Şuşa Beyannamesindeki önemli maddelerden biri de, iki devletten birine üçüncü bir devlet tarafından saldırı söz konusu olduğunda; her iki devletin birbirine yardım sağlamayı kabul ettiğinin beyannamede karşılıklı imza altına alınmış olmasıdır. Beyannemede yer alan bu madde, NATO Antlaşması'nın 5. maddesi kapsamında paralellik sağladığından bu minvalde de değerlendirilebilmektedir. **Şuşa Beyannamesi, Türkiye'nin Kafkasya'daki bölge ülkeleri ve komşu Orta Asya ülkeleri ile yakın ilişkiler kurma imkanını sağlamış, hem ekonomik hem de ulaşım açısından bağlarının güçlenmesinin önünü açmıştır.**

Karabağ Zaferinde dikkat çeken bir başka önemli husus Türkiye ile Azerbaycan'ın birbirine karadan ulaşımını sağlayacak olan paha biçilmez öneme sahip Zengezur koridorunun açılması olmuştur. Zengezur Koridoru "Doğu-Batı Koridoru", "Kuzey-Güney" Uluslararası Ulaşım Koridoru (ITC) ve Hazar Ulaştırma Ağı'nı (CTN) güçlendirerek Hazar'dan Avrupa'ya uzanan Petrol ve Gaz Boru Hattı Sistemi'nin (OGPS) işleyişine katkı sağlayarak Tek Yol Tek Kuşak projesinde yer alan Dijital İpek Yolunda bu koridordan geçmesinin önünü açmaktadır. Zengezur Koridorunun faaliyete geçmesi, halihazırda Avrupa Birliği (AB), ABD, Rusya ve Çin'in enerji tedarik hatları için önemli rol oynayarak bölgenin transit kapasitesini arttıracak niteliktedir. (ANKASAM, 2021)

3. "Tek Yol Tek Kuşak" Projesi Çerşevesinde Azerbaycan'ın Bölgesel Dijital Merkeze Çevrilmesi

Modern İpek Yolu diğer bir adıyla Tek Yol Tek Kuşak projesi 2013 tarihinde Şi Cinping tarafından acıklanmış ve bu proje doğu ile batıyı birleştirerek yüze yakın ülkenin yer aldığı küresel ticaret yolu zincirinini oluşturulacağı proje olarak değerlendirilmektedir. Proje 6 bölgeyi kapsamakta ve bu bölgeler şu şekilde değerlendirilmiştir;

- **“Doğu Asya:** Çin, Moğolistan
- **Güneydoğu Asya:** Brunei, Kamboçya, Endonezya, Laos, Malezya, Myanmar, Filipinler, Singapur, Tayland, Timor-Leste, Vietnam
- **Orta Asya:** Kazakistan, Kırgızistan, Tacikistan, Türkmenistan, Özbekistan
- **Ortadoğu ve Kuzey Afrika:** Bahreyn, Mısır, İran, Irak, İsrail, Ürdün, Kuveyt, Lübnan, Umman, Katar, Suudi Arabistan, Filistin, Suriye, Birleşik Arap Emirlikleri, Yemen
- **Güney Asya:** Afganistan, Bangladeş, Bhutan, Hindistan, Maldivler, Nepal, Pakistan, Sri Lanka
- **Avrupa:** Arnavutluk, Ermenistan, Azerbaycan, Belarus, Bosna-Hersek, Hırvatistan, Çekya, Estonya, Gürcistan, Macaristan, Letonya, Litvanya, Makedonya, Moldova, Karadağ, Polonya, Rusya, Sırbistan, Slovakya, Slovenya, Ukrayna ve Türkiye” (M5 DERGİ, 2021)

Tek Yol Tek Kuşak projesi kazan-kazan ilkesine dayanarak bölge ülkeleri ile ekonomik ilişkileri geliştirirken, siyasi ilişkilerinde Çin tarafından kuvvetlendirilmesi amaçlanmaktadır. Bu bağlamda Çin projede yer alan ülkeler üzerinde önemli bir siyasi etki oluşturmayı amaçlamaktadır. (Filiz, 2020: 119)

Çin devlet başkanı Xi Jinping’in Tek Yol, Tek Kuşak sloganı ile ilk kez Kazakistan’da dile getirdiği Yeni İpek Yolu Projesi, o tarihten bu yana Pekin’in en önemli dış politika hedeflerinden biri haline gelmiştir. Avrupa ile Asya arasında yeni bir ekonomik koridor olması beklenen proje, Çin açısından siyasi, ekonomik ve kültürel kazanımları olan çok yönlü bir stratejidir. Pekin’in özellikle 2000’li yıllardan itibaren izlediği çok yönlü dış politika anlayışının bir parçası olma niteliğindeki bu proje ile Çin, daha önce çok fazla etkili olmadığı birçok bölgede daha etkin bir güç haline gelmeyi hedeflemektedir. Bununla birlikte bu girişim ABD’nin tek kutuplu dünya anlayışına karşı Çin’in son yıllarda izlediği politikaları da destekler mahiyettedir. (Özdaşlı, 2015: 579)

İpek Yolu yüzyıllar boyunca Doğu ve Batı arasında insanların, malların ve fikirlerin taşındığı ticaret ve etkileşim kanalı olmuştur. (Atlı, 2014:76) Yüzyıllardır nesilden nesile aktarılan; barış ve işbirliği, açıklık ve kapsayıcılık, karşılıklı öğrenme ve karşılıklı yarar ilkelerini barındıran İpek Yolu Ruhu, kuşak ülkelerin gelişmesi, refah düzeyinin artması ile insan uygarlığının ilerlemesi açısından büyük katkı sağlamıştır. Bu bakımdan Doğu ile Batı arasında iletişimi ve işbirliğini simgeleyen bu ruh; dünyadaki tüm ülkeler tarafından paylaşılan ortak tarihi ve kültürel mirastır. (Ministry of Foreign Affairs The People’s Republic of China, 2015)

Tek Yol Tek Kuşak projesinde “Alt Yapı ve Tesis Bağlantıları”, “Yatırım ve Ticaret İlişkilerin Gelişmesi”, “Finansal Entegrasyon”, “Kalkınma Politikaların Koordinasyonu”, “Sosyal ve

Kültürel Alanda İşbirliğin Gelişmesi" gibi beş temel alan yer alarak ülkeler ile işbirliğinin güçlenmesi amaçlanmaktadır. (Clifford Chance, 2017).

Projede yer alan Alt Yapı ve Tesis Bağlantıları Çin'in dijital alanda boşlukların farkına vararak 2015 yılında Dijital İpek Yoluna ihtiyaç olduğunu ortaya koymuştur. Başlangıçta, tedarik zincirinde şeffaflığın geliştirilmesi için nesnelerin interneti (İoT) ve veri üretimine yönelik bir dijital devrim olarak görülsede, daha sonra bu gelişmeler kendisiyle bağımsız platformların birbirleriyle iletişim kurmasını ve bağımsız veri depolarının oluşturulmasına neden olmuştur. Dijital İpek Yolun'nun stratejisi geniş bir dizi Çin kamu politikasını ve BİT altyapı yatırımlarını içermektedir. İlk günden bu yana Dijital İpek Yolu projesi fiber optik kabloyu basitçe yaymanın ötesine geçerek 5G ağları biçiminde ağ ekipmanı, teknoloji ve kolaylaştırıcı yazılımlar içeriyor. BeiDou navigasyon sistemleri tarafından da desteklenen 5G ağının sürekli olarak alınması ve optik kablolara erişim ile Çin, Avrasya'daki etkisini artırmayı planlamaktadır. Bu yeni Dijital Silah Yarışı olarak değerlendirilen yarış, ABD'nin, Çin'in bu teknolojileri kullanmaması için askeri ve güvenlik risklerini savunarak ilerlemesini engellemeye amaçlamaktadır. (Wheeler, 2020)

5G teknolojisi yüksek hıza sahip olarak veri aktarımında yüksek kapasiteli, gecikme süresi kısa, az maliyetli ve güvenilir mobil iletişim hizmeti sunmayı hedeflemektedir. 5G teknolojisi ile iletişim sistemlerinde yaşanan birçok sınırlamaların ortadan kalkacağı ve veri transferlerinde hızın 20 gigabite ulaşılması amaçlanmaktadır. Böylece yüksek hıza sahip olan bu teknoloji veri transferlerinde gerekli olan bulut sistemleri, artırılmış gerçeklik ve sanal gerçeklik gibi uygulamaları indirmeden saliseler içinde verilerin aktarılmasında kullanılması amaçlanmaktadır. 5G teknolojisi sadece akıllı şehirler ve insanlarla cihazlar arasında değil, aynı zamanda cihazlar arasında da kesintisiz ve verimli iletişimin sağlanmasını hedeflemektedir. (Sarığül, 2018)

İletişimin sağlanmasında BİT'e değer kazandıran önemli bir faktör mevcuttur. Bu faktör günümüzde petrol kadar değerli olan veridir. Petrol ana kaynak olarak değerlendirilsede, petrolün sınırlı bir kaynak olduğunu hepimiz bilmekteyiz, lakin veri sınırsız bir değer ve bu değer gelişen teknolojiler sayesinde saliseler içerisinde çoğalmakta ve tükenmez bir sanal ortamda bulunmaktadır. Veri için teknoloji dünyasını atan kalbi diyebilmekteyiz. Verisiz BİT işlevsiz olmakla anlamsızdır.

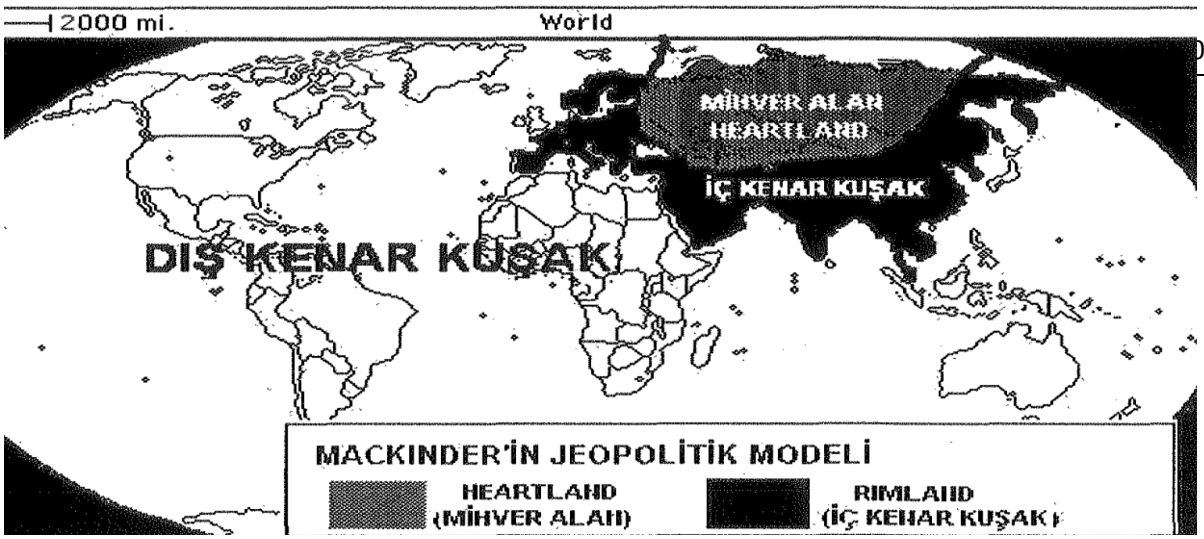
Veri aktarımı Tek Yol Tek Kuşak projesi kapsamında *Dijital İpek Yolu* üzerinde iletişimin hızlı bir şekilde yapılmasını hedefleyerek, petrol kadar önemli olan Veri'nin Çin için ne kadar değerli olduğunu ortaya koymaktadır. Dijitalleşen çağda verileri elinde bulunduran dünyanın güçünü elinden bulundurur perspektifi üzerinden değerlendirme yaptığımızda; Tek Yol Tek Kuşak

projesi ile Çin hükümetinin yakın gelecekte dünyanın süper gücüne sahip birkaç ülkeden biri olacağının kaçınılmaz olarak gerçekleşeceği kanaatinde olduğumu belirtmek isterim.

Tam bu noktada dikkatlerinizi bugün kısmen gerçekleşen bazı teorilere çevirmenizi isteyeceğim. Öncelikle, 1904 yılında H.Mackinder tarafından geliştirilmiş olan "*Kara Hakimeyet Teorisi*" ön plana çıkmaktadır. Mackinder'in görüşüne göre yeni uluslararası global sistem içerisinde yer almak isteyen devletler kara'da egemenliklerini sağlamalıdırlar. Mackinder'e göre coğrafya acısından "merkez" bölgeye sahip olan dünya adasına sahip olur teorisini savunmaktaydı. Merkez bölgesi için önce *Georgraphical Pivot of History* (Tarihin Coğrafi Mihveri), daha sonra *Heartland* (Kalpgah) (Bkz. Resim.2) adı kullananan Mackinder, dünyanın geri kalan bölgesini sahip oldukları özelliklere göre iki kuşağa bölmuş. Bu iki kuşak şu şekildedir;

- **İç Kuşak** - Merkez bölgesinin cevresinde bulunan Almanya, Avusturya, Balkanlar, Turkiye, İran, Pakistan, Hindistan ve Çin'i kapsar.
- **Dış Kuşak** - İngiltere, Kuzeybatı Afrika, Avustralya, A.B.D. ve Kanada'yı kapsar. (İşcan, 2004: 16)

Harita-1: Halford J. Mackinder'in Jeopolitik Modeli



Resim.2 Kaynak: Uluslararası İlişkilerde Klasik Jeopolitik Teoriler ve Çağdaş Yansımaları, İsmail Hakkı İşcan

Daha sonra, Nicholas John Spykman "*Kenar Kuşak" (Rimland)* olarak savunduğu teoride Kalpgah olarak adlandırılan Avrasya ile Rusya'yı çevreleyen Türkiye, Irak, İran, Pakistan, Afganistan, Hindistan, Çin ve Kore'nin yer aldığını Kenar Kuşağı kontrol eden Avrasya'yı kontrol eder; Avrasya'yı kontrol eden ise dünyayı kontrol eder teorisini savunmuştur. (Anadolu Ajansı,2018) (Bkz: Resim.3)

Bu iki düşenceye zamanla, Amerikalı Amiral Alfred Tayer Mahan "*Deniz Hakimiyet Teorisini"* geliştirerek denizlere hakim olan dünyayı kontrol eder kuramını savunurken, İkinci Dünya Savaşından sonra denizlerin ve karanın üstünü kuşatan havanın da bu ikisi kadar önemli olduğunu savunan ABD'li havacılar tarafından *"Hava Hakimiyet Teorisi*" geliştirildiği bilinmektedir.

Resim.3 Kaynak: https://newellta.weebly.com/political-theories.html

Bu teoriler kapsamında Tek Yol Tek Kuşak projesini değerlendirdiğimiz zaman projenin 6 bölge: *Doğu Asya, Güneydoğu Asya, Orta Asya, Ortadoğu ve Kuzey Afrika, Güney Asya, Avrupa'yı* kapsayarak, bölge ülkeleri ile *"Alt Yapı ve Tesis Bağlantıları", "Yatırım ve Ticaret İlişkilerin Gelişmesi", "Finansal Entegrasyon", "Kalkınma Politikaların Koordinasyonu", "Sosyal ve Kültürel Alanda İşbirliyin Gelişmesi"* alanlarında iş birliğinin sağlanacağını daha öncede belirtmiştim. Bu 6 bölgeyi incelediğim zaman Mackinder ve Spykeman tarafından zamanında geliştirilmiş olan Heartland ve Rimland teorileri, Mahan tarafından savunulan Deniz Hakimiyet Teorisi ve son olarak İkinci Dünya Savaşından sonra geliştirilmiş olan Hava Hakimiyet Teorileri aslında "Tek Yol Tek Kuşak" projesinde yer almakta, çünkü Çin 6 bölgede yer alan tüm devletlerle hem karada, hem havada, hemde denizlerde işbirliğinde bulunmayı amaçlamaktadır.

Tek Yol Tek Kuşak projesinin Kafkasya bölgesi açısından değerlendirdiğimizde; öncelikle İkinci Karabağ Savaşının bitmesi bölgede güvenliğin sağlanması anlamına gelmektedir. Ayrıca

bölgede Azerbaycan ile Türkiye'yi bir birine bağlayacak olan *Zengezur koridoruun* sağlanmış olmasının önemi de yadsınamaz bir gerçeklik taşımaktadır. Bu koridor alternatif güzergah statüsünü (güney güzergahı) taşımaktadır. Tek Yol Tek Kuşak projesinde kullanılabilecek önemli güzergah niteliğini taşıyan bu koridor, bölgenin Dijital Merkeze çevrilmesinde önemli rol oynamaktadır.

Bağımsızlığını kazandıktan sonra Azerbaycan, Bakü-Tiflis-Ceyhan petrol boru hattı, Güney Gaz Koridoru ve Trans-Hazar Uluslararası Taşımacılık Rotası dahil olmak üzere bir dizi önemli bölgesel ve kıtalararası enerji ve ulaşım projelerini başlatarak bu projelerde yer almıştır. Dijitalleşen bir dünyada bu projelerin yanında Azerbaycan yurt içi ve sınır ötesi telekomünikasyon projelerini de takip ederek, önemli ulaşım merkezlerine dahil olarak bölgenin *Dijital Merkezi* statüsünü de kazanmayı hedeflemektedir.

10 Nisan 2020 tarihinden itibaren Azerbaycan parlamentosu Hazar Denizi'nin dibinden Azerbaycan ile Türkmenistan arasında bir trans-Hazar fiber optik kablonun döşenmesine ilişkin yasayı kabul ederek cumhurbaşkanının onayına sunmuştur. (https://president.az/articles/36415)

Yüksek veri iletim kapasitesine sahip olan yeni denizaltı fiber optik kablo, Azerbaycan ve Türkmenistan'ı bir birine bağlayacaktır. Bu hattın oluşturulması, Frankfurt ve Mumbai internet merkezlerini birbirine bağlayarak Avrupa ve Asya arasında Dijital İpek Yolu`nun oluşması için önemli ölçüde katkıda bulunarak web trafiğinin Avrupa'dan Türkmenistan, Özbekistan, Afganistan, Pakistan ve Hindistan'a Azerbaycan toprakları üzerinden aktarılmasını sağlayacaktır. Azerbaycan, bu trans-Avrasya dijital telekomünikasyon koridorunun oluşturulmasına katılarak, kendisini bölgesel bir Dijital Merkez haline getirmeyi amaçlamaktadır. Azerbaycan'nın Dijital Merkez haline gelmesi bölgenin internet erişiminin ana satıcısı olmasını sağlayarak, ithaalatçıdan bir dijital hizmet ihracatçısına dönüşmeyi hedeflemektedir. (Jamestown Foundation, 2020)

Bu program çerçevesinde ülke dışında yürütülen altyapı projeleri arasında Hazar Denizi'nin dibinde Azerbaycan ile Kazakistan arasında da bir başka fiber optik kablonun yapımı da yer alıyor. (Trend News Agency, 2021) Azerbaycan'nın Dijital Merkeze çevrilmesi, sadece Güney Kafkasya için değil, aynı zamanda Orta Doğu, Orta Asya ve Güney Asya için de bölgesel bir siber hizmet merkezi haline gelmesi açısından önemlidir. Çünkü Londra, Frankfurt, Sofya, İstanbul, Moskova, Amsterdam ve Dubai gibi ülkelerle beraber yeni bir İntenet Değişim

Noktası (IXP) olarak Bakü'nün çeşitli dijital hizmetlere erişimi olan 1,8 milyar kişiye ulaştıracağı düşünülmektedir. (Caspian News, 2019)

Burada belirtmek isterdim ki, Çin ve Kazakistan arasında 2019 yılından itibaren Dijital İpek Yoluna dair çalışmaların başlaması, Azerbaycan ve Kazakistan arasında Hazar denizinin üzerinden fiber optik kablonun düzenlenmesi Azerbaycan'a dijitalleşen çağda yeni jeopolitik kimlik kazandırmaktadır. Fakat Azerbaycan sadece Dijital Güzergah olarak kalmayı planlamıyor, burada aynı zamanda veri merkezlerinin kurulması da hedeflenmektedir. Bu bağlamda da Dijital İpek Yolu'nun bir parçası olarak, Çinli şirketler ev sahibi ülkelerde veri merkezleri kurmayı hedeflemektedir. Alibaba Cloud, 2017 yılında Malezya, Endonezya ve Singapur da dahil olmak üzere dünyanın on yedi bölgesinde "Uçan Apsaras Veri Merkezleri" adı verilen bulut bilişim büyük veri merkezleri kurarak Asya'nın en büyük bulut tabanlı bilgi işlem platformunu oluşturdu. China Telecom Global, Tek Yol Tek Kuşak ülkelerinde büyük kapasiteli sunucuları barındıracak veri merkezleri ve bulut bilişim hizmetlerini barındırmak için veri depolama sistemlerini de inşa ediyor. Dijital İpek Yolu üzerinden aktarılan verilerin yönetilmesi, aktarılması ve depolanması, donanımın ve yazılımın yalnızca kurulması değil, aynı zamanda bakımının da Çin şirketleri tarafından yapılacağı proje kapsamında bilinmektedir. ("Matthew S. Erie† and Thomas Streinz, 2021:52)

DEĞERLENDİRME

Modern İpek Yolu'nun kurulmasının dijitalleşen çağda yeni teknolojiler sayesinde gerçekleşeceği perspektifi ile ele alırsak; 20. yüzyılın başlarında geliştirileren teorilere, "Kara Hakimiyet Teorisi", "Deniz Hakimiyet Teorisi" ve "Hava Hakmiyet Teorisine" birde "***Veri Hakimiyet Teorisi***", kuramını uluslarası ilişkiler disiplininden gelen biri olarak öne sürmek isterim. İzah etmek isterim ki, "***Veri Hakimiyet Teorisi'nin***" günümüzde "Kara Hakimiyet Teorisi", "Deniz Hakimiyet Teorisi" ve "Hava Hakmiyet Teorisi" kadar önemli yer tuttuğunu belirterek, veriler modern çağın petrolu niteliğini taşıdığını - ***veriyi kontrol eden dünyayi kontrol edeceğinin*** altını tekrarla çizmek isterim

Tek Yol Tek Kuşak projesi vasıtasıyla, Çin uluslarası ilişkilerde zaten önemli yere sahip olan Kara, Deniz ve Hava Hakimiyetinde fiziki gücü elinde bulundurmakla beraber, Dijital İpek Yolu üzerinden de aktarılacak olan verilere sahip olarak dünya hakimiyetini kendi kontrolü altına almayı hedeflemektedir. 2013 yılında Çin'in ilan etmiş olduğu projesini incelediğimde,

Çin somut güçle beraber, soyut gücede sahip olmayı amaçlayarak dünya hakimiyetini elinde bulundurmak niyetindedir.

Bununla birlikte bu girişim ABD'nin tek kutuplu dünya anlayışına karşı Çin'in son yıllarda izlediği politikaları da destekler mahiyettedir. Özelikle 11 Eylül saldırılarından sonra ABD'nin Çin'in "hayat alanı" olarak gördüğü bölgelere yönelmesi ile Çin; Şanghay İşbirliği Örgütü (ŞİÖ), BRICS (Brazil, Russia, India, China and South Africa) gibi mekanizmalarla bölge ülkeleri ile işbirliğini artırmaya çalışmıştır. Bu bakımdan Yeni İpek Yolu Projesi de ABD hegemonyasına ve onun tasarladığı tek kutuplu dünya anlayışına karşı bir başkaldırı olarak değerlendirilmektedir. (Özdaşlı, 2015: 579)

Yeni İpek Yolu'nun açıklanan ve açıklanmayan hedefleri göz önünde bulundurulduğunda İkinci Dünya Savaşı sırası ve sonrasında oluşturulan küresel düzene bir alternatif oluşturacağı, en azından küresel güç ABD'nin dengeleyebilecek bir proje niteliği taşıdığı gerek uluslararası ilişkilerde gerekse de akademik dünyada dile getirilen konuların başında gelmektedir.

Sonuç olarak; Azerbaycan bölgesel olarak da İkinci Karabağ Zaferi sonucunda Türkiye ve Türki Cumhuriyetleri ile bağlarını güçlendirmiş, Kafkasya Bölgesinde bölgenin istikrarına yönelik güçlü ve vazgeçilmez bir ülke olduğunu ortaya koyarak siyasi ve ekonomik yükselişini devam ettirmiş; Çin'in Yeni İpek Yolu projesinde de hem jeopolitik konumunun önemi hem güçlü ekonomisi ile vazgeçilmez olduğunu tüm dünyaya göstermiştir.

KAYNAKÇA

Aljazeera Türk, Kafkasya'nın Açık Hesabı: Dağlık Karabağ, 09.08.2014, http://www.aljazeera.com.tr/dosya/kafkasyanin-acik-hesabi-daglik-karabag, (Erişim Tarihi: 07.26.2021)

Anadolu Ajansı, Dağlık Karabağ'daki İşgale Son Verilmesini Öngören BMGK Kararları Uygulanmıyor, 29.09.2020, https://www.aa.com.tr/tr/azerbaycan-cephe-hatti/daglik-karabagdaki-isgale-son-verilmesini-ongoren-bmgk-kararlari-uygulanmiyor/1989110#, (Erişim Tarihi: 07.26.2021)

Anadolu Ajansı, Jeopolitik Teoriler Temelinde Doğu Akdeniz ve Türkiye, 10.04.2018, https://www.aa.com.tr/tr/analiz-haber/jeopolitik-teoriler-temelinde-dogu-akdeniz-ve-turkiye/1113793, (Erişim Tarihi: 08.04.2021)

Anadolu Ajansı, Asrın Anlaşması 25 yaşında, 20.09.2019, https://www.aa.com.tr/tr/dunya/asrin-anlasmasi-25-yasinda/1589095, (Erişim Tarihi: 08.08.2021)

Anadolu Ajansı, Şuşa Beyannamesi Bölgesel Barış ve İş Birliğinin Teminatı, 22.06.2021, https://www.aa.com.tr/tr/analiz/susa-beyannamesi-bolgesel-baris-ve-is-birliginin-teminati/2280430, (Erişim Tarihi: 07.29.2021)

Anadolu Ajansı, Azerbaycan'ın İşgal Altındaki Toprakları Karabağ: Ermenistan, Uluslararası Hukuku Hiçe Sayarak, Azerbaycan Topraklarının Yüzde 20'sini Oluşturan Karabağ'ın İşgalini Sürdürüyor, 29.09.2020, https://www.aa.com.tr/tr/azerbaycan-cephe-hatti/azerbaycanin-isgal-altindaki-topraklari-karabag/1989594, (Erişim Tarihi: 26.07.2021)

ANKASAM, Zengezur Koridoru'nun Stratejik Önemi, 01.06.2021, https://www.ankasam.org/zengezur-koridorunun-stratejik-onemi/, (Erişim Tarihi: 29.07.2021)

Atlı, A. (2014). Çin ve Yeni İpek Yolu Projesi. *Analist*, Sayı 44, ss.74-77

Azerbaycan Cumhuriyeti Hükümeti ile Türkmenistan Hükümeti Arasında Azerbaycan-Türkmenistan Hazar Denizi`nin Dibi İle Fiber Optik İletişim Hatlarının Ortak İnşası, Mülkiyeti ve Kullanımına İlişkin Kanun, https://president.az/articles/36415, (Erişim Tarihi: 08.06.2021)

BBC News, Dağlık Karabağ Neden Önemli, Azerbaycan ve Ermenistan Arasındaki Sorun Ne Zaman ve Nasıl Başladı?, 28.09.2020, https://www.bbc.com/turkce/haberler-dunya-54330024, (Erişim Tarihi: 26.07.2021)

Bilgin, Mustafa Sıtkı. (2020), "Karabağ Zaferine Giden Süreç ve Jeopolitik Sonuçları", *Türk Dünyası Araştırmaları,* Cilt.129, Sayı: 255, ss.315-334

Caspian News, Azerbaijan Digital Hub Program Receives Prestigious Award, 13.12.2019, https://caspiannews.com/news-detail/azerbaijan-digital-hub-program-receives-prestigious-award-2019-12-12-35/, (Erişim Tarihi: 08.06.2021)

Clifford Chance, (2017). China's Belt and Road Challenges and Opportunities, https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2016/09/chinas-one-belt-one-road-challenges-and-opportunities.pdf, (Erişim Tarihi: 08.04.2021)

Chın, T. (2013). The Invention of the Silk Road, 1877. *Chicago Journal*, 40(1), ss.194-219

Haber 7, Madrid Prensipleri Karabağ'a Barış Getirecek Mi?, 01.04.2010, https://www.haber7.com/yazarlar/mehmet-fatih-oztarsu/504649-madrid-prensipleri-karabag8217a-baris-getirecek-mi, (Erişim Tarihi: 07.26.2021)

İşcan, İsmail Hakkı , (2004) Uluslararası İlişkilerde Klasik Jeopolitik Teoriler ve Çağdaş Yansımaları, *Uluslararası İlişkiler Dergisi*, Cilt: 1 Sayı: 2, ss. 47-79

Jamestown Foundation, The Increasing Role of Azerbaijan as a Regional Digital Hub, 26.05.2020, https://jamestown.org/program/the-increasing-role-of-azerbaijan-as-a-regional-digital-hub/, (Erişim Tarihi: 08.06.2021)

Kurab, Vefa ve Çumen Nur, (2020), Tarihi ve Güncel Boyutları İle Karabağ, Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü, *Disiplinlerarası Politika Vizyonu ve Stratejiler 2020*, https://aybu.edu.tr/GetFile?id=8480a131-8a18-4262-9996-19d5dcff8669.pdf

Kürekçay Anlaşması, https://www.virtualkarabakh.az/tr/post-item/32/52/kurekcay-anlasmasi.html, (Erişim Tarihi: 07.19.2021)

Sarıgül, Tuba, "5G: Mobil İletişim Sistemlerinde Kökten Değişim", 2018, https://bilimgenc.tubitak.gov.tr/makale/5g-mobil-iletisim-sistemlerinde-kokten-degisim, (Eriim Tarihi: 08.04.2021)

Matthew S. Erie† and Thomas Streinz, (2021), The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance, *New York University Journal of International Law and Politics*, Cilt.54, No.1, ss.1-92

Ministry of Foreign Affairs The People's Republic of China, (2015), "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road", 28.05.2015,https://www.mfa.gov.cn/eng/zy/jj/2015zt/xjpcxbayzlt2015nnh/202406/t20240606_11381659.html, http://en.ndrc.gov.cn/newsrelease/201503/t20150330_669367.html, (Erişim Tarihi: 12.06.2024)

M5 Dergi Batı'dan Doğu'ya Geçen 'Güç': Bir Kuşak Bir Yol – Modern İpek Yolu, 07.02.2021, https://m5dergi.com/one-cikan/batidan-doguya-gecen-guc-bir-kusak-bir-yol-modern-ipek-yolu/, (Erişim Tarihi: 08.03.2021)

Nerimanlı, Tebriz. (2015). Karabağ Savaşının Türkiye, Azerbaycan ve Ermenistan İçin Sosyal ve Ekonomik Etkileri, *Journal of İnstitute of Economic Development and Social Researches*,Cilt: 1 Sayı: 1, ss.31–36

Özalp, Görkem Ozan, (2015), Azerbaycan Cumhuriyeti'nin Savunma Yapısı ve Güvenlik Politikası, *Uluslararası Stratejik Araştırmalar Kurumu,* Cilt: 10, Sayı: 20, ss.107-140

Özdaşlı, Esme. (2015), Çin`in Yeni İpek Yolu Projesi ve Küresel Etkileri, *International Periodical for the Languages, Literature and History of Turkish or Turkic Cilt* 10/14, 2015, ss.579-596

Roux, J. P. (2006). Orta Asya: *Tarih ve Uygarlık*. Çev. Lale Arslan, Kabalcı Yayınları: İstanbul

Sak, Güven. (2015), Türkiye'nin Bir İpek Yolu Stratejisine İhtiyacı Var, https://www.tepav.org.tr/tr/blog/s/5177/Turkiye___nin+bir+Ipek+Yolu+stratejisine+ihtiyaci+var, (Erişim Tarihi: 2.06.2024)

Takvim, Aliyev'den Ermenistan'a Jet Yanıt! "Karabağ Azerbaycan'dır, ünlem", 04.10.2019,https://www.takvim.com.tr/dunya/2019/10/03/aliyevden-ermenistana-jet-yanit-karabag-azerbaycandir-unlem, (Erişim Tarihi: 08.07.2021)

Taner Filiz, (2020), Çin'in Küresel Tek Kuşak Tek Yol Girişiminde Türkiye'nin Konumu Üzerine Bir İnceleme, *Sosyal Bilimler Dergisi*, Cilt: 2 Sayı: 2, ss.117–133

Tarihi, Bugünü ve Geleceğiyle İpek Yolu. 05.05.2015, https://turkish.cri.cn/882/2015/05/05/1s168157.htm, (Erişim Tarihi: 12.06.2024)

Trend News Agency, "Kazakistan-Azerbaycan: Yeni İşbirliği Fırsatları" Etkinliğinde Trans-Hazar Fiber Optik Kablo Hattı Projesi Vurgulandı, 05.03.2021, https://az.trend.az/business/3390933.html, (ErişimTarihi: 08.06.2021)

TRT Haber, Azerbaycan'ın Karabağ Zaferi: İşte Anlaşmanın Maddeleri, 11.11.2020, https://www.trthaber.com/haber/dunya/azerbaycanin-karabag-zaferi-iste-anlasmanin-maddeleri-529782.html, (Erişim Tarihi: 07.29.2021)

Türkiye Cumhuriyeti ile Azerbaycan Cumhuriyeti Arasında Müttefiklik İlişkileri Hakkında Şuşa Beyannamesi, (2021), https://www.tccb.gov.tr/assets/dosya/2021-06-15-Azaebaycan-SusaBeyannamesi.pdf (Erişim Tarihi: 29.07.2021)

Sputnik Türkiye, Yeni Oyun Kurucu: Asya Altyapı Yatırım Bankası, 26.03.2015, https://anlatilaninotesi.com.tr/20150326/1014652688.html, (Erişim Tarihi: 29.07.2021)

Şiriyev, Zaur. (2010), Azerbaycan'ın Askeri Doktrini ve Dış Politika Yansımaları, *Uluslararası Stratejik Araştırmalar Kurumu, USAK,* ss.132-147

Wheeler Andre, China's Digital Silk Road (DSR): The New Frontier in the Digital Arms Race?, 19.02.2020 https://www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/, (Erişim Tarihi: 08.04.2021)

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

THE POLITICS OF CYBER-SECURITY

Onur YILMAZ[*]

Orcid: 0000-0001-6846-0968

By Dunn Cavelty, M. (2024). The Politics of Cyber-Security (1st ed.). Routledge. https://doi.org/10.4324/9781003497080

Myriam Dunn Cavelty, a recognized expert and academic in cybersecurity, international relations, and security, authored The Politics of Cyber-Security. She is a Senior Researcher and Vice President of Education and Research at the Center for Security Studies (CSS) at ETH Zurich. Cavelty, who focuses primarily on cyber security policies, concentrates on these policies' social, political, and economic dimensions. She has written numerous books and academic articles in the field of cyber security, becoming an essential reference source with her work titled Cyber-Security and Threat Politics: US Efforts to Secure The Information Age. Cavelty's extensive experience and research in the field make her a credible and authoritative voice on the subject.

The author identifies her target audience in this book as academics, policymakers, and students interested in international relations, security studies, and cyber security. Cavelty aims to expose the political dimensions of cyber security policies, their technological and political interactions, and the real-world implications of these factors. She argues that cyber security policies must no longer be examined solely from a technical perspective, as the issue has evolved into a domain that needs to be assessed within the context of international relations, power dynamics, and state actions. In this regard, she emphasizes the necessity of historical analysis to understand the new reality; the cyber domain has integrated itself into real life over the past 30 years, sometimes with states intervening to seek political gains within this domain (Cavelty, 2024: 1-15). Thus, the book's introduction highlights the importance of considering the new historical, political, and technical conditions in addressing cyberspace security. As a result, the new reality of cyber security is discussed in a manner that positions states at the center, reflecting the field's current state.

[*] Research Assistant, Ph.D. Candidate, Political Science and International Relations, Istanbul Aydın University - İstanbul, Turkey. E-mail: yilmaz12onr@gmail.com

In the second section, which emerges from the debate on cyber policies, the book adopts a comprehensive approach to reveal the interactions between cyber security, cyberspace, and politics. According to this view, cyberspace and cyber security influence politics, while cyber security policies also affect, shape, and guide cyberspace and cyber security. On the other hand, it is essential to balance traditional political approaches encountered in forming cyber security policies and the dynamic nature of such policies. Thus, developing cyber security policies requires rediscovering various bureaucratic units and evaluating and establishing their responsibilities and roles within a new legal framework. The treatment of cyber security policies spans a broad spectrum from securitization tendencies to technological routines and their applications in daily life, and it is observed to develop in a context where different perspectives are raised simultaneously. Considering the undeniable impacts of digital technologies on power dynamics, wealth distribution, and even conflicts today, it becomes easier to comprehend the structure that intersects technology and politics. The growing number of studies in International Relations focusing on cyber security and technology emerges due to these influences (Cavelty, 2024: 16-31).

In the fourth section, which examines how states consider cyber security as a political issue, topics such as cybercrime, cyber espionage, and cyber warfare are discussed, highlighting states' growing interest in this area. It is noted that since the 1980s, the cyber domain has presented a constantly changing and anarchic situation characterized by malicious software, damage to critical infrastructure, espionage, and information warfare, prompting states to implement various policies in this domain. Concepts like Morris Worm, Moonlight Maze, and Electronic Pearl Harbor are now seen as having social significance and political implications. As a result, states have moved far beyond merely viewing electronic developments as reflections of progress. Instead, they must develop policies that consider the threats and attacks associated with these developments. Consequently, the complex structure of cyber threats makes it unlikely for states to cope with them individually. At this point, the collaboration between the public and private sectors requires various partnerships, cooperation, information sharing, and coordination. It necessitates a tripartite defense approach, which manifests in combating cybercrime, protecting critical infrastructures, and safeguarding the private sector. On the other hand, there is a debate about the role of states. Some view the role and degree of intervention of states or state regulations as essential, while others find it more appropriate for the private sector to operate autonomously in this area and for market mechanisms to function. The potential for cybersecurity measures and policies to be repressive is also a significant point

of contention (Cavelty, 2024: 32-54). This is because there are concerns and related criticisms regarding the possibility that such measures may limit privacy and freedom of expression. Nevertheless, cybersecurity is not just a technical issue; it has political, economic, and social dimensions, and due to various reasons, such as its borderless nature and the anonymity of the perpetrator, it requires international cooperation. The transformation of states' presence in the cyber domain that began in the 2000s is discussed in the fourth section. Accordingly, the state, which was previously involved in the cyber domain for reasons such as combating cybercrime, preventing service disruptions, and eliminating data breaches, has started to be a direct supporter or perpetrator of various cyber incidents. The reality of new cyber attacks that can yield widespread consequences brings to mind disaster scenarios in the collective consciousness. It compels states to take action to avoid being victims of such possibilities. As states begin to view the cyber domain as both a threat and an opportunity, they have initiated measures and efforts to enhance their capabilities. Countries like the USA, Russia, and China have entered a reality where they invest in cyber capabilities to conduct operations against political rivals or enemies. The increasing complexity of cyber attacks, associated with more political and strategic objectives, has resulted in many states seeking to develop their capabilities. Examples of this new reality include the Stuxnet attack against Iran, efforts to control internet traffic through programs like TEMPORA, TURMOIL, and TURBINE, and state-sponsored hacker attacks on the networks of the 2016 Democratic National Committee and many other US institutions. Therefore, in which states engage as primary actors, cyberspace has transformed into a synergistic structure that must be addressed with technical concerns and strategic and political goals and objectives (Cavelty, 2024: 55-78).

In the book's fifth chapter, views are presented regarding the notion that the perception of cyber threats is, in essence, a result of a political process. Although a centralized structure has not articulated these perceptions, it is emphasized that they are formed within a political process and undergo changes over time, ultimately serving cognitive and political objectives. The importance of this discussion lies in revealing the existence of a political discourse process in determining what constitutes a threat during the categorization of cyber threats and how it should be addressed. For instance, while cybercrime is not inherently evaluated politically, it can be considered an element of security policy when linked to state or non-state actors and causes significant harm. Similarly, categories like cyber espionage, cyber influence operations, cyber terrorism, or cyber warfare emerge from the degree of state involvement and the political processes they pursue or participate in (Cavelty, 2024: 79-103). With states becoming actors in

cyberspace in all their aspects, there is a belief that various norms that everyone must adhere to must be developed in this domain.

The book's sixth chapter provides a comprehensive overview of the development of international cybersecurity norms. States' increasing use of cyber tools to achieve their political objectives has created the necessity for regulating state behaviors. Diplomatic forums like the UN have played central roles in establishing regulatory norms. The UN's Group of Governmental Experts has brought together experts from various countries to work on foundations such as norms for state behavior, the applicability of international law, confidence-building measures, and cybersecurity capacity development. However, the disagreements regarding the applicability of international law in the cyber domain and the balance between state sovereignty and individual freedoms cannot be overlooked as part of this process. While Western countries advocate for openness and freedom of expression in cyberspace, states like China and the Russian Federation have proposed ideas emphasizing state control and sovereignty. These ideological differences have complicated the norm-formation processes. On the other hand, given that states have engaged in various actions despite norms, even reaching the brink of war, the effectiveness of these norms is also a matter of debate. Possible reasons for this include the time it takes for norms to be adopted, conflicts of interest among state institutions that would implement these norms, and the inadequacy of norms to restrict the actions of powerful states. In short, while cybersecurity norms are developing, they are shaped by the intricate and complex interactions between diplomacy and state policies. However, the prerequisite for the success of these norms is international cooperation and harmony.

The book's seventh chapter, which operates through cyber incidents, states that these incidents are significant elements shaping international relations and security strategies. It is emphasized that cyber incidents, which start by exploiting security vulnerabilities and are evaluated in the context of technical impacts and socio-political frameworks, have gained security-political significance. Cyber attacks/incidents resulting from violating cybersecurity vulnerabilities through malware, worms, Trojan horses, spyware, and ransomware can result in strategic and significant damage. Therefore, focusing solely on the technical aspects of these incidents while neglecting their strategic, social, and political contexts will reduce the effectiveness of security strategies. For this reason, cyber incidents must be addressed holistically, and it should not be overlooked that they arise from a socio-political process.

The book's eighth chapter examines the current state of cyber operations, their uses, and expected benefits. It proves these cyber operations are primarily carried out for espionage and often manifest as minor disruptions. This chapter mainly explores why states need such operations, analyzing how technological capabilities and politically encountered constraints influence their decisions to use cyber operations. The example of Ukraine illustrates that such cyber operations did not significantly alter the war's course, emphasizing that these operations are predominantly focused on intelligence gathering. Thus, it is argued that the potential for cyber operations to cause genuine destruction is limited. Consequently, evaluations suggest that the strategic value of cyber operations may be overstated while noting that they could be used to achieve various political objectives. In summary, the idea that cyber operations play a more supportive role than a coercive or conflict-escalating element in military operations is emphasized.

In the final chapter, it is highlighted that cybersecurity policies need to be approached with an interdisciplinary framework due to the multifaceted nature of cyberspace, alongside predictions that cybersecurity will become increasingly important with the global digital transformation and that security concerns arising from this transformation will escalate. It is suggested that the progression of digital transformation may involve various challenges and inequalities, potentially turning security into a privilege; state-sponsored cyber attacks are expected to develop in a more sophisticated manner, possessing significant resources, which may lead to more advanced and effective Cyber-attacks; as societies continue their digital transformation, states are anticipated to adopt more proactive roles in this area, vying to shape it; and in the context of strategic competition, digital sovereignty is likely to instigate transformative changes resonating across diplomatic, economic, and strategic domains. Cavelty asserts that cybersecurity should be approached interdisciplinarily and anticipates increased security concerns with digital transformation. The proactive role of states in cyberspace and the importance of international cooperation are emphasized.

Overall, this book provides a comprehensive analysis not just of existing theories, practices, or problems in cyber policies but also of ongoing dialogues, developing policies, and collective actions. It offers a general and thorough perspective that contributes significantly to the literature and is an essential resource for experts, policymakers, academics, and students.

SİBER SALDIRILAR ASİMETRİK SAVAŞIN BİR PARÇASIDIR

Naman Bakaç[*]

Orcid: 0000-0002-7806-4827

İsrail'in Lübnan'da çağrı cihazları, telsiz ve radyo panellerine yönelik gerçekleştirdiği eylem; sosyal bilimciler, bilişim uzmanları, askeri stratejisiler ile mühendisler tarafından siber terör veya siber savaş suçları kapsamına girip girmediğini gündeme getirdi. Bu gündeme; birkaç gün önce CIA eski şefi Leon Panetta'nın saldırıyı terörizm olarak nitelendirmesi ile eylem, siyasi ve teknokratlar tarafından da oldukça sofistike ve ilginç bulundu. Bu siber terörün oluş biçimine dair birçok teknik iddialar ve senaryolar da gündeme geldi. Saldırının teknik kısmı kadar failine dair medyada "olağan şüpheli" olarak İsrail'in gösterilmesi de kaçınılmaz olmakla beraber, "olağan şüpheli"den saldırıyı üstlendiğine dair herhangi bir açıklama görmedi kamuoyu.

İsrail'in siber terör kapsamına giren bu eylemi; siber güvenlik, siber istihbarat, siber savunma, siber caydırıcılık, siber hukuk, siber tehditler, siber suçlar, siber terör, siber savaş ve siber politikalar gibi birçok başlığın ne denli hayati ve öncelikli olduğunu bir kez daha gösterdi. Tüm bu hayati başlıkları, Prof. Dr. Nezir AKYEŞİLMEN ile konuştuk. Türkiye'de ilk akademik dergi olma özelliğine sahip ***Siber Politikalar Dergisi'***nin editörü olan YEŞİLMEN, ***Disiplinlerarası Bir Yaklaşımla: Siber Güvenlik ve Siber Politika*** ismiyle bir kitapta yayınladı ve şu anda Selçuk Üniversitesi Uluslararası İlişkiler Bölümü'nde akademisyen olarak siber güvenlik, siber politikalar, siber hukuk ve siber suçların insan hakları ilişkisi bağlamında hem dersler vermekte hem de akademik makaleleri bulunmaktadır.

Siz uzun yıllar uluslararası ilişkiler disiplini ile beraber; siber güvenlik, siber politikalar, siber hukuk, siber uzay ve siber tehditler gibi alanlarda akademik çalışmalar yapan ve Türkiye'de bu alanda ilk akademik dergi çıkaran bir uzmansınız. 17 ve 18 Eylül'de Lübnan'da patlatılan çağrı cihazları, telsizler ve radyo panelleri saldırısına baktığınızda bu gelişmeyi siz nasıl okudunuz? Nereye oturttunuz? İşin teknik kısmına ve oluş biçimine dair yaklaşımınız nedir?

[*] Batman Mezopotamya Turizm Mesleki ve Teknik Anadolu lisesi.

Lübnan'da gerçekleştirilen saldırı, hem bölgesel hem de küresel güvenlik açısından oldukça dikkat çekici. İsrail'in geçmişte de siber savaş ve iletişim sistemlerine yönelik saldırılar düzenlediğini biliyoruz. Bunlardan en dikkat çekeni 2010 yılında İran Nükleer Tesislerine yönelik gerçekleştirilen ve tahminen en az 1000 reaktörün kullanılamaz hale geldiği Stuxnet saldırısıdır. Stuxnet birçok teknik ve statejik açıdan dünyada bir ilkti. Fiziksel zarar verdiği için ilk siber silah olarak kabul edilmektedir, Yine teknik karmaşıklığı nedeniyle ki o güne kadar üretilen en karmaşık zararlı yazılımdan 20 kat daha karmaşıktı (kodun uzunluğunun 50 bin satır olduğu söyleniyor. Yani bir doktora tezi kadar uzun). Siber güvenlik firmaları çok sayıda uzmanla kurdukları ekiplerle teknik yapısını çözmeye çalıştılar. Sanayi tesislerine yapılan bu saldırı, air-gap dediğimiz internete bağlı olmayan networklara yapılan ilk siber saldırıydı. Stuxnetten sonra dünya çapında bir siber güvenlik algısı gelişti ve ülkeler o zamana kadar dijital alanı bir oyun, eğlence, ekonomi ve iletişim alanı olarak görmekten çok bir politika alanı olarak görmeye başladılar. Yani askeri, güvenlik ve stratejik açıdan kayda değer bulmadıklarından ilgilenmediler. Fakat stuxnet bu algıyı küresel çapta değiştirdi. Tabi daha önce de bu algıyı farklı düzeylerde kıran gelişmeler yaşandı.

İnternetin ilk 20 yılı (1969-1989) görev-ce barışçıl ve zararlı yazılımın olmadığı bir dönemdi. Fakat 1989'da Morris kurtçuğu o zaman internete bağlı olan 60 bin bilgisayarın %10'u yani 6000'ı etkilendi. Bu bilinen ilk zararlı yazılım olarak kabul ediliyor. Bu saldırı ve sonrasında 1990'lar genelde bireysel düzeyde siber güvenlik algısı ve endişesini oluşturdu. Fakat 2000 yılında mafya Çocuk saldırısı olarak da bilinen ve Yahoo, eBay, CNN gibi büyük küresel firmalara yapılan saldırı sonucu network güvenliği ya da kurumsal güvenlik sorunu veya algısı ortaya çıktı. Hala ulusal ve uluslararası güvenlik açısından alarm zilleri çalmamıştı. İlk zil 2007 yılında Rusya menşeli olduğu tahmin edilen Estonya'ya yönelik DDoS (hizmet yavaşlama ve engelleme) saldırıları oldu. Tabi en belirletyici olan ise yukarıda bahsedilen Stuxnet oldu. 2016 yılında yine Rusya'nın ABD Başkanlık seçimlerine yönelik saldırı da bu alandaki başat ve belirleyici saldırılardandır. Hizbullah'a yönelik bu son saldırı da en az Stuxnet ve diğerleri kadar ulusal ve uluslararası güvenlik üzerinde etkileri olacaktır.

Telsiz ve Radyo Panellerinin Hedef Alınması, Askeri ve Lojistik Koordinasyonu Sekteye Uğratmak İçindir

Bu saldırıyı teknik açıdan değerlendirirsek, siber uzayın dışında geleneksel elektromanyetik alanlar üzerinden yapılan bir saldırı olarak nitelendirebiliriz. Çağrı cihazları ve radyo panelleri gibi iletişim sistemlerine saldırı, modern savaşta bilgi akışını kesmek, psikolojik baskı yaratmak ve iletişimi koparark sahada taktik üstünlük sağlamak amacıyla kullanılıyor. Teknik olarak,

bu saldırının hedefi iletişim altyapısını kırmak ve savunma mekanizmalarını zayıflatmaktır. Bu da hibrit savaşın bir parçası olarak görülebilir.

Bu saldırı, sadece fiziksel yıkım değil, aynı zamanda bilgi ve iletişim sistemlerine yönelik bir operasyonu temsil ediyor. Siber savaş unsurları devreye girerek, karşı tarafın iletişim ağlarını ve stratejik haberleşme araçlarını etkisiz hale getirmeyi hedefliyor. Özellikle telsiz ve radyo panelleri gibi iletişim cihazlarının hedef alınması, askeri ve lojistik koordinasyonu sekteye uğratmak amacıyla yapılmış olmalıdır. Bu saldırılar, bilgi üstünlüğü sağlama çabalarının bir parçası olup, askeri operasyonları zayıflatma, karar alma süreçlerini yavaşlatma ve psikolojik üstünlük elde etme amacı taşır. İsrail'in bu saldırıları, bölgedeki güç dengesini değiştirme ve belirli alanlarda taktik avantaj sağlama amacı güdüyor. Siber saldırılar asimetrik savaşın bir parçasıdır. Saldırıların ahlaki, insani ve hukuki boyutu bir tarafa bırakılacak olursa, bu alanda İsrail bu yöntemleri sık sık kullanan ve yenilikçi yöntemler geliştiren bir ülke. Bu yönüyle İsrail'in en başarılı aktörlerden birisi olduğu açıktır.

Bu saldırılarla ilgili piyasada bir dizi senaryo ve teori var. Bir kısmı akla yatkın, fakat bir kısmı siber teknolojinin yapısını bilmeyen tamamen afaki iddialara dayalı argümanlar. Bu saldırı teknik yönüyle incelendiğinde piyasadaki birçok teorinin doğru olma ihtimalinin düşük olduğu görülecektir. Neden mi? Birincisi, bu bataryalar ya aşırı şarj, ya da sıkıştırma, darbe ya da ısınma sonucu patlayabilirler. Bu örnekten yola çıkarak, şimdiye kadar kazara da olsa neden hiç biri patlamadı? Ikincisi, velev ki patladı, bu bataryalar genellikle 500mAh ya da 1000 mAh olurlar ki boyutları oldukça küçüktür. Bunların patlatma örnekleri internette mevcut. Onlara bakarsanız bu kadar büyük zarar verecek kapasitede olmaları imkansız gibi. Oysa Hizbullah'a yönelik saldırıda gördüğümüz patlamalar çok büyük patlamalar. Sanki bir Pager bataryası değil de elektrikli araba bataryası gibi. Üçüncüsü, o zaman geriye bir teori kalıyor o da bu cihazlara önceden patlayıcı bir düzeneğin yerleştirilmiş olması ihtimali. Bu büyük bir operasyon gerektirir. Devlet ve devlet dışı aktörlerin iş birliğini gerektirir. Bu nedenle, işin içinde hem İsrail devleti hem de bazı firmaların olma ihtimali var. Bu firmalar lojistik firması olabileceği gibi, üretici firma da olabilir. Dördüncüsü, diyelim ki düzenek kuruldu, bir de o düzeneği patlatacak bir yazılım geliştirmeniz ve bu cihazlara yüklemeniz gerekir. Bu da zaman ve büyük bir çaba gerektirir. Bu süreci tam olarak anlamak için daha çok bilgiye ihtiyaç var. Bu zamanla ortaya çıkacaktır. Fakat bu saldırı siber güvenlik tarihinde bir dönüm noktası olacaktır. Tıpkı 2000 yılındaki mafya çocuk saldırısı, 2007deki Estonya'ya yönelik DDoS saldırıları ve 2010'da İran nükleer tesislerine yönelik Stuxnet saldırısı gibi.

Bu Saldırı, Teknik ve Sosyal Mühendisliği Birleştirdiği İçin, Hibrit Bir Siber Saldırıdır

Bu saldırı salt teknik bir saldırı olmayıp, aynı zamanda dolandırıcılığa dayalı bir sosyal mühendislik saldırısıdır da. Bu nedenle, bu saldırı hem teknik hem de sosyal mühendislik yöntemlerini birleştirdiği için hibrit yani karma bir siber saldırıdır. Uluslararası siber saldırılarda teknik saldırıları engellemeye yönelik ciddi ürünler geliştirilmiş durumdadır. Teknik saldırıların başarılı olma ihtimali artık daha zor. Fakat kullanıcı hatası, manipülasyon zaafı ve dolandırıcılığa dayalı sosyal mühendislik saldırılarının başarı oranı çok yüksek. Sosyal mühendislikte yöntemler bitmez. Bu nedenle önlem almak oldukça zordur. Bu nedenledir ki son yıllarda başarılı siber saldırıların %90'ından fazlasını sosyal mühendislik saldırıları olduğunu ileri süren raporlar var.

Toparlayacak olursak, bu saldırı ve kullanılan teknikler daha çok tartışılacak ve muhtemelen hiçbir zaman işin aslını tam olarak öğrenemeyeceğiz. Fakat şunu iyi bilmeliyiz ki bugün siber teknoloji alanında geldiğimiz nokta ve siber saldırıların geldiği düzey işin daha başlangıcında olduğunu ileri sürmek yanlış olmaz. Teknoloji geliştikçe yeni kolaylıklar ve konforun yanında yeni saldırı yöntemleri ve tehditler ortaya çıkmaktadır. Siber teknoloji bugün baş döndürücü bir hızla gelişiyor ve hayatımıza getirdiği yenilikler (değişimler) de baş döndürücü bir hızla artıyor.

Uluslararası Siber Hukuk Çok Zayıf, Son 1 Aya Kadar Bm'de Yapılmış Tek Bir Siber Hukuk Anlaşması Yoktu

Saldırının teknik kısmı dışında bir de hukuki, siyasi ve askeri kısmına bakılacak olursa, siber hukuk ve siber politikalar alanında yetkin bir isim olarak İsrail'in bu saldırısı uluslararası ilişkiler literatüründe neye tekabül ediyor? Siber suçlar bağlamında İsrail, neyle itham edilebilir? BM ve uluslararası hangi kurum harekete geçebilir? Mesela bu bir siber terör veya siber savaş suçu mudur? Eğer öyleyse hangi kurum, ne yapmalıdır?

Maalesef uluslararası siber hukuk oldukça zayıftır. Ulusal ve bölgesel çapta bir takım hukuki düzenlemeler olsa bile, son bir aya kadar BM nezdinde yapılmış tek bir siber hukuk anlaşması maalesef yoktu. BM üyelerinin özellikle büyük güçlerin siber alanla ilgili farklı düşünmesi ve farklı çıkarlara sahip olması nedeniyle, uzun yıllar bu alanda hiçbir anlaşma yapma başarısı gösterilemedi. Ta ki 8 ağustos 2024 tarinde kabul edilen siber suçlarla mücadele anlaşmasına kadar. O da çok dar ve ciddi müdahalelerle birçok konuda özellikle insan hakları ve ifade özgürlüğünü koruma konusunda haddinden fazla devlet merkezli olduğu eleştirilerini almaktadır. BM'nin siber saldırılara yönelik net bir mevzuatı olmamakla birlikte, 2015 yılında kabul edilen siber suçlarla mücadeleye dair küresel inisiyatifler ve Uzmanlar Grubu Raporu uluslararası hukuk çerçevesinde siber saldırıları düzenlemektedir. Fakat şunu unutmayalım ki bu düzenleme bir anlaşma değil, yani devletler üzerinde bağlayıcı değildir. Tavsiye niteliğindedir, fakat yine de bir referans metindir.

Siber hukuk açısından bakıldığında, İsrail'in bu saldırısı, uluslararası hukukta henüz tam anlamıyla düzenlenmemiştir. Ancak yine de mevcut hukuki çerçevelere dayanarak bu saldırı uluslararası insancıl hukuk**,** Birleşmiş Milletler (BM) Şartı ve siber suçlara karşı mücadele eden uluslararası normlar kapsamında ele alınabilir. İsrail'in saldırıları toplumu korku ve dehşete sevk ettiği için terör, ya da siber terör olarak değerlendirilebilir. Yine BM saldırmazlık ilkesi gereği egemen bir ülkenin topraklarına saldırı düzenlediği için uluslarararası hukuku ihlal eden, saldırmazlık ilkesini çiğneyen, bir devletin toprak bütünlüğüne ve/ya siyasi bağımsızlığına yönelik saldırı suçu olarak değerlendirilebilir. İsrail, bu saldırıyla sivil iletişim altyapılarına zarar vermişse, bu durum uluslararası insancıl hukukun ihlali olarak değerlendirilebilir. Cenevre Sözleşmeleri ve ek protokoller, savaş durumunda sivillerin korunmasını şart koşar. Sivil iletişim ağlarına yönelik saldırılar, orantısız güç kullanımı ve sivil hedeflere zarar verme suçlamalarına yol açabilir.

Bu Saldırı, Toplumu Korku Ve Dehşete Sevkettiği İçin Siber Teröre Girebilir

Özetle İsrail neyle suçlanabilir:

1. Egemen bir devlete karşı yasadışı kuvvet kullanımı**:** BM Şartı'na aykırı olarak kuvvet kullanımı ve siber saldırı gerçekleştirmek.
2. Sivil altyapıya zarar verme**:** Cenevre Sözleşmeleri ve insancıl hukuk açısından, sivil altyapılara zarar verildiği iddia edilebilir.
3. Orantısız güç kullanımı**:** Eğer saldırının askeri bir gerekliliği aşarak sivil halkı hedef aldığı gösterilirse, orantısız güç kullanımı suçlaması yapılabilir.
4. Siber savaş suçu: Saldırının doğası gereği, askeri ve sivil hedefler arasındaki farkı gözetmeden yapılan siber saldırılar, savaş suçu kapsamına girebilir.
5. Siber terör: Toplumu korku ve dehşete sevk ettiği için siber teröre girebilir.

Tabi bütün bunlar için İsrail'in bu saldırıları işlediğine dair net kanıt gereklidir. Zira siber saldırılarda failleri bulmak çoğu zaman zordur. Hatta sofistike saldırılarda bu imkansıza yakın bir zorluğu ifade ediyor. Literatürde iyi bilinen Estonya'ya yönelik DdoS saldırıları, Stuxnet, ABD seçimlerine yönelik saldırılarda bile itham edilen taraflar hiçbir zaman sorumluluk kabul etmediler. Zira, bu saldırıları ortaya çıkaracak teknik bir bilgi ve uygulama henüz mevcut değildir. Fakat genelde siber saldırılar fiziksel ya da kinetik çatışmaların devamı niteliğindedir. Estonya'ya yönelik saldırı yapıldığında Rusya ve Estonya arasında devam eden bir gerginlik vardı, İran'a yönelik Stuxnet saldırısı İran-Batı ya da ABD ve İsrail ile olan çatışması sonucu yapıldığı tahmininden yola çıkılarak ve saldırının teknik karmaşıklığı dikkate alınarak ABD ve İsrail fail olarak ilan ediliyor. Yine ABD se.imlerine müdahale ABD ile var olan çatışmasının

bir devamı olabileceği gerçeğiyle ileri sürülüyor. Tabi bu konuda yürütülen bazı hukuki süreçler de önemli ipuçları vermişti. Son olarak İsrail ve Hizbullah arasında var olan kinetik çatışmadan ve saldırının teknik karmaşıklığından (bu kadar karmaşık bir teknik saldırıyı ancak İsral yapabilir algısından) yola çıkılarak İsrail fail olarak gösteriliyor.

Siber Teröre Karşı; BM, UCM Ve Uluslarararası Telekominikasyon Birliği Devreye Girebilir

Özellikle siber terör ve siber savaş suçları incelendiğinde, Birleşmiş Milletler, Uluslararası Ceza Mahkemesi (UCM) ve Uluslarararası Telekominikasyon Birliği (ITU) gibi kurumlar devreye girebilir. Güvenlik Konseyi, bu tür olayları ele almak ve uluslararası barışı ve güvenliği sağlamakla görevlidir. Konsey, bir soruşturma başlatarak olayın tüm yönlerini inceleyebilir ve gerekli yaptırımları belirleyebilir. UCM, eğer bu saldırıda bireysel sorumluluğu olan kişiler varsa ve ilgili devletler UCM'ye üye ise, bu kişiler hakkında dava açılabilir. Uluslararası Telekomünikasyon Birliği (ITU) siber güvenlik konusunda uzmanlaşmış bir kuruluştur. Bu tür olaylar karşısında üye devletlere teknik destek sağlayabilir ve uluslararası standartlar çerçevesinde bu saldırıların insani ve hukuki boyutlarını değerlendirebilir. Tabi burada iki temel sorun var. Birincisi, siber alanda askeri ve sivil alan ayırımı maalesef yoktur. Dijital alanda sınırlar olmadığından, sivil ve askeri alanları ayırmak da imkansızdır. Bu nedenle, hukuki anlamda kesin bir değerlendirme yapmak zordur. İkincisi, ulusal düzeyde olduğu gibi, uluslararası düzeyde de hukukun gücü değil, güçlünün hukuku karşımıza çıkmaktadır.

İngilizce ve Türkçe çıkardığınız akademik bir dergi olan *Siber Politikalar Dergisi'nde* Elif Gürdal Limon'un Askeri Haberleşme Sistemleri üzerine 2023 tarihli dikkat çekici bir yazısını okudum. Yazıda; *"Siber güvenlik ortamı devletlerin ve diğer aktörlerin bir savaş alanı olarak gördükleri ve ulusal güçleriyle bütünleştirdikleri bir konu haline gelmiştir. Bu açıdan siber güvenlik ulusal güvenliğin bir parçasıdır. Siber savaş diğer savaş türleri arasında yerini almıştır" diyor.* Siber güvenlik, nasıl ulusal güvenliğin bir parçası haline geldi? Siber savaş, diğer savaş türleri arasındaki yerini nasıl almış oldu?

Elif Gürdal Limon'un makalesinde de vurgulandığı gibi, siber güvenlik, devletlerin ve diğer aktörlerin stratejik çıkarları doğrultusunda giderek ulusal güvenliğin ayrılmaz bir parçası haline gelmiştir. Bu dönüşüm, teknolojinin hızla ilerlemesi ve dijital altyapıların günlük hayatın ve devlet işleyişinin merkezinde yer almasıyla doğrudan bağlantılıdır. Siber savaşın diğer savaş türleri arasındaki yerini alması ve siber güvenliğin ulusal güvenliğin ayrılmaz bir bileşeni haline gelmesi birkaç önemli gelişmeye dayanmaktadır.

Devletler, askeri, ekonomik, sosyal ve siyasi işlevlerini yürütmek için kritik altyapılarında dijital teknolojilere daha fazla bağımlı hale geldi. Bankacılıktan enerji sistemlerine, iletişim ağlarından ulaşım altyapılarına kadar birçok alan, siber tehditlere açık hale geldi. Bu dijitalleşme, saldırıya açık daha fazla alan yaratırken, ulusal güvenlik için de siber savunmanın önemini artırdı. Örneğin, elektrik şebekeleri gibi kritik altyapılara yönelik siber saldırılar, geniş çaplı elektrik kesintilerine ve toplumsal kaosa yol açabilir. Bankacılık ve finans sistemlerine yönelik saldırılar, ekonomik istikrarı tehdit edebilir. Ya da askeri komuta ve kontrol sistemlerine yönelik saldırılar, ülkenin savunma kabiliyetini zayıflatabilir.

Ayrıca 2000'li yılların ortasından itibaren ülkeler ulusal siber güvenlik strateji belgeleri geliştirmeye başladılar. Bu belgeler genelde o ülkelere yönelik siber riskler ve tehditleri belirlemekte ve onlara karşı alınabilecek teknik, hukuki, kurumsal kapasite geliştirme ve işbirliğine yönelik önlemleri, politikaları, stratejileri ve uygulamaları kapsamaktadır. Yine son yıllarda aralarında Türkiye (son ulusal siber ggvenlik strateji belgesinde bu vurgu var), Çin, ABD'nin de yer aldığı birçok ülke ulusal güvenlik strateji belgelerinde açıkça siber güvenliğin ulusal güvenliğin önemli bir bileşeni haline geldiğini ifade etmektedir.

Bu nedenle, siber güvenlik artık yalnızca teknik bir mesele değil, aynı zamanda politik ve hatta sosyolojik bir sorundur. Teknik önlemlerin yanında savunmayı güçlendirecek hukuki vesiyasi karar ve stratejiler gerektiriyor. Bunun ötesinde toplumu siber güvenlik kültürü konusunda bilgilendirmek ve bilinçlendirmek gerekiyor. Özellikle siber güvenlik kültürü diyorum Çünkü siber güvenlikten farklı olarak siber güvenlik kültürü pozitif güvenlik anlayışına dayalı bir kavramdır. Pozitif güvenlik de salt olumsuzluklar ve siber saldırıları önlemeye yönelik bir strateji olmayıp, güvenlik ve özgürlük dengesini koruyan bir anlayıştır. Negatif güvenlik ise, herşeye rağmen, hak ve hukuk pahasına güvenliği sağlamaktır. Oysa bu anlayış bir güvenlik politikası değil aslında kendisi bir güvenlik sorunudur. (Pozitif) Siber güvenlik özetle vatandaşın temel hak ve özgürlüklerini koruyan, açık ve erişilebilir internet sağlayan ve aynı zamanda güvenliği ihmal etmeyen bir güvenlik anlayışıdır.

Siber güvenlik bugün devletlerin ulusal güvenliğini koruma stratejilerinin bir parçası haline geldi. Devletler, dijital altyapılarını korumak için siber ordular ve siber savunma mekanizmaları oluşturmak zorunda kaldılar. Siber ordu deyince üniformalı, silahlı asker düşünmemek gerekir. Bu alanda faaliyet gösteren bilgisayar uzmanlarından oluşan kişiler ve/ya şirketler olabilir. Bugün birçok siber güvenlik firması aslında o ülkelerin ordularına bağlı sivil görünümlü siber ordunun bir parçasıdır. Bu nedenle, bu tür yapılanmalardan dolayı literatürde yeni vekalet savaşları kavramı geliştirildi. Yani devletler diğer bir devlete ya da yapıya saldırırken ortaya çıkma ihtimaline binaen uluslararası suç teşkil etmesin diye bu şirketler

üzerinden saldırı yaparlar. Siber güvenlik, geleneksel ulusal güç unsurlarına (askeri güç, ekonomik güç, diplomatik güç) ek olarak yeni bir ulusal güç unsuru olarak kabul görmeye başladı. Bir ülkenin siber kapasitesi, diğer ülkelerle olan ilişkilerinde ve uluslararası arenada rekabetçi konumunda belirleyici rol oynar.

Kısacası, siber güvenliğin ulusal güvenliğin önemli hatta bence en önemli bileşeni haline gelmesinin başlıca bir kaç nedeni var. Birincisi, giderek hayati önemi artan bilginin kontrolü. Bilgi dediğimiz şey internette paylaşılan yazı, resim, video, görünen ve görünmeyen her türlü datayı içerir. İkincisi, eenerji, ulaşım, iletişim, finans ve ticaret gibi kritik altyapılar giderek daha fazla siber ortama bağımlı hale gelmiştir. Bu altyapılara yönelik siber saldırılar, bir ülkenin ekonomik ve sosyal hayatını felç edebilir. 2007'de Estonya'da olduğu gibi. Üçüncüsü, siber teknoloji askeri operasyonları desteklemek, maliyetlerini düşürmek ve hatta karşı tarafı şaşkına çevirmek için kullanılan ciddi bir araç hatta silah haline geldi. Bu da askeri rekabeti bu alana taşıdı ve asimetrik bir alan oluşturdu. Yine bu çerçevede, devletler arasındaki rekabet, siber alana da taşınmıştır. Siber casusluk, siber sabotaj ve siber propaganda gibi faaliyetler, devletler arasında yeni bir çatışma alanını oluşturmuştur.

Siber savaş, ya da siber çatışmalar asimetrik savaş türlerinden biri olarak kabul edilmeye başlandı. Geleneksel savaşlarda güçlü askeri güce sahip devletler avantajlıyken, siber savaşta bu denge bozulabilir. Zayıf devletler veya devlet dışı aktörler bile sofistike siber saldırılar düzenleyerek büyük devletlerin kritik altyapılarına zarar verebilir. Tabi siber savaş kavramı çok da hazzettiğim bir kavram değil. Siber alanı aşırı şekilde güvenlikleştiren ve bu yönde önlemler almayı teşvik ettiği için. Siber alanda bırakalım devletler ya da büyük sivil yapıları bazen bir kişi hatta bir çocuk bile bir devlete muazzam zarar verebilir. Bunun en tipik örneği 2015 yılında Kane Gamble adında 15 yaşındaki bir İngiliz çocuk Irak ve Afganistan savaşlarına tepki olarak o zamanki CIA başkanı John Brennen'in kişisel sosyal medya hesaplarını hackleyerek 2000 üzerinde CIA ajanın kişisel bilgileri ile 10 binlerce gizli savaş belgesini ifşa etti. Dijital alan devletlerin yanında kişiler dahil olmak üzere devletdışı aktörleri de fazla güçlendiriyor. Hatta bugün siber alanın en güçlü aktörleri devletler değil, big-tech firmaları denilen büyük teknoloji firmalarıdır. Bunlar Cisco, IBM, Microsoft, Google, Twitter vs'dir. Bütün bunlar siber çatışmaları ya da siber savaşları asitmetrik yapmak için açık delillerdir. Düşünün 15 yaşındaki bir çocuk CIA tarihinin en büyük zararını verebiliyor. Bu durum, siber savaşın klasik savaş türleri arasındaki yerini sağlamlaştırmasına neden oldu.

Uluslarararası Düzenin Karar Alıcıları, Kendilerine Yakın Ülkelerin Terör ve Savaş Suçlarını Görmezden Geliyorlar

İşin teknik kısmı dışında, uluslararası ilişkiler bölümünde bir akademisyen olarak, İsrail'in Gazze ve Lübnan'daki bu savaş suçu ve terör uygulamalarına karşı, bölgesel ve küresel barışı, küresel hukuku ve insan haklarını korumak bağlamında İsrail'i durdurabilecek aktör veya kurum neden cevval değil? Neden durdurulamıyor İsrail? Savaş suçu ve terörden yargılanabilecek yüzlerce kuvvetli delil varken uluslararası kurumların varlık sebebi ve misyonu sorgulanıyor bildiğiniz gibi dünya kamuoyunda. Mevcut uluslararası düzen İsrail'in güvenliği için mi şekillendi diye insan sormadan edemiyor. 2.Dünya savaşı sonrası şekillenen Pax-Americana veya demokratik liberal uluslararası düzen bu haliyle devam edebilir mi? Gazze'deki soykırımdan sonra uluslararası düzenin nasıl şekilleneceğini öngörüyorsunuz?

Uluslarararası barış ve istikrarı korumak başta Birleşmiş Milletler ve büyük güçlerin hukuki ve ahlaki sorumluluğudur. Bunun yanında diğer uluslarararası örgütler ve devletler hatta tüm toplum organlarının hukuki ve ahlaki sorumlulukları söz konusudur.

Uluslarararası müdahale ve yaptırımlar hususunda da maalesef çok kere çifte standartlara şahit olmaktayız. Uluslarararası düzenin karar alıcıları kendilerine yakın ülkelerin terör ve savaş suçlarını görmezden gelebiliyorlar. Bunu sadece İsrail örneğinde değil, son 80 yılda bunun çok örneğini gördük. Başka ülkelerin topraklarında terör estiren, hatta işgal eden, kendi vatandaşlarına yönelik sistematik insan hakları ihlali yapan birçok ülke uluslarararası arenada yaptırımlara maruz kalması gerekirken, ceza almadan hatta başkasını aynı suçlarla suçlayarak da gezebiliyor. Bu çifte standart menfaatler sözkonusu olduğunda çoğu kişinin/toplumun ve ülkenin başvurduğu hatta savunduğu bir yol. Herkes kendi terörünü meşru görüyor maalesef. İş kendisine gelince o farklı deyip işin içinden sıyrılıyor. Diğer birçok devlet de 'zamanı gelince lazım olabilir' diyerek bu hukuksuzluklara ya sessiz kalıyor ya da cılız bir tepki veriyor.

Bunun yanında bu alanda BM çerçevesinde bağlayıcı karar alma yetkisine sahip tek organ BM Güvenlik Konseyidir (BMGK). BMGK yapısı itibariyle demokratik olmadığı gibi, beş daimi üyenin sahip olduğu veto hakkı da birçok hukuksuzluğa kaynaklık etmektedir. Bu nedenle, Genç Sivillerin geliştirdiği ve sontrasında Erdoğan'ın sıkça kullanarak uluslararasılaştırdığı 'Dünya Beşten Büyüktür' sloganı yerinde bir tespittir. Fakat bu slogan bana kalırsa eksiktir, iş adalet ve hukuka geldiğinde dünya 200'den (yaklaşık 200 olan üyesine atfen) de büyüktür. Gerçekte bir adaletin sağlanabilmesi için devletleri de aşan küresel demokratik bir yapıyı ve işleyişi hedeflemeliyiz. Aksi takdirde devlet-merkezli her düzen içinde yapısal olarak büyük adaletsizlikleri ve istikrarsızlıkları içerir. Kısacası, burada sorun yapısaldır ve ciddi bir BM reformuyla ancak mümkün olabilir. O da bugünkü konjönktürde oldukça zor görünmektedir. Bir takım revizyonist talepler var, fakat statüko çok daha güçlü görünüyor.

Siber Uzay, Uluslararasi İlişkilerdeki Anarşik Düzeyi Artırdı ve Anarşiyi Gerçek Bir Hobsiyan'a Çevirdi

Diğer önemli bir husus, uluslararasi örgütlerin kendilerini oluşturan devletlerden bağımsız olamaması. BM diyoruz ama BM, onu oluşturan üyeler ve karar alma yetkisine sahip olan güçlü ülkelerden bağımsız bir yapı değildir. Evet başta BM olmak üzere diğer uluslararasi örgütlerin bir dizi eksikleri var, zaafları var. Bu konuda 1970'lerden beri geliştirilen geniş bir akademik literatür var. Fakat yine bu örgütler dünya barışı için hayati bir görev ifa etmektedirler. Bugün BM'yi uluslararası sitemden çekersen hala mevcut olan 350 uluslararasi çatışma ve 40 olan savaşın en az 10 katına çıkması içten bile değildir. O zaman kimin gücü kime yeterse politikası devreye girecektir. Bugün uluslararası kurumlardan çekindiği için saldırgan olamayan bazı ülkeler, ilk fırsatta sağa sola saldıracaklardır. Zaten son yıllarda sistem kısmen zayıflayınca Afrika, Ortadoğu ve Kafkaslarda bunun birçok örneğini gördük. Bu kaos ve hobsiyan anarşik düzen daha da derinleşecektir. Aslında bunu siber uluslararasi ilişkilerle de açıklamak mümkündür. Çünkü son fiziksel tehditlerden bağımsız olarak, siber uzay uluslararasi ilişkilerdeki anarşik düzeyi arttırdı. Gerçek hobsiyan bir anarşiye çevirdi. Ünlü MIT hocalarından Mısır asıllı ve siber politika öncülerinden Prof. Nazli Choukri buna hiper anarşi diyor ki doğrudur. Zira fiziksel uluslararasi ilişkilerde görece bir düzen sağlayan uluslararasi örgütler, uluslararasi hukuk, uluslararasi toplum, diplomasi gibi kurumlar siber uluslararasi ilişkilerde ya çok zayıflar ya da hiç yoklar. Bu nedenle, buradaki düzen oldukça çatışmalı olan hiper anarşik bir ortamdır, der. Son İsrail saldırıları da bunu hem fiziksel hem de siber alanda açıkça göstermektedir.

Batının İsrail'i Desteklemesi, Liberal ve Ahlaki Değerleri Gözardı Eden Bir Yaklaşımdır

Tabi ki bu kurumları eleştirelim, daha iyisi için çabalayalım fakat yıpratmamaya özen göstermeliyiz. TV'lerde bu konularda İlber Hoca'nın ifadesiyle oldukça cahil olan bazı kimselerin bu kurumları tahfif etmesi, aşağılaması, gereksiz göstermesi, hatta çete ve terör gibi haddi aşan sıfatlar kullanması ciddi bir sorumsuzluk göstergesidir. Bu kadar cehalet okumakla olur dedirten cinsten bir yaklaşım. Daha önemlisi, İsrail konusunda ya da başka bazı hususlarda uluslararasi örgütlerin olabildiğince güçlü ve cevval olmasını arzulayan bazı kişiler, işin ucu kendilerine değince ya da desteklemedikleri hususlara gelince bu örgütlerin bu kadar yetkiye sahip olmaması gerektiğini savunan tutarsız hatta ahlaksız kişiliğe bürünüyorlar.

Maalesef Güvenlik Konseyinde daimi üyeler olarak yer alan başta ABD, Fransa ve İngiltere, İsrail'i güçlü bir şekilde destekliyorlar. ABD koşulsuz bir destek sunuyor. Bu yaklaşım hem

ABD'ye hem de Pax-Amerikana olan uluslararası sisteme çok ciddi zarar veriyor. Bugüne kadar savunageldikleri liberal ve ahlaki değerleri gözardı eden bir yaklaşım. ABD'de güçlü bir yahudi lobisi var. Fakat parti fark etmeksizin bu koşulsuz destek artık lobi şirketlerini de aşan hatta ABD'de belli çevrelerde eleştirilen bir noktaya geldi.

Mevcut uluslararası düzen, 20. yüzyılın ikinci yarısında birçok alanda başarılar elde etse de, özellikle İsrail-Filistin çatışması başta olmak üzere birçok benzer çatışmaları yönetmede gösterdiği zaafiyet nedeniyle bu düzenin sürdürülebilirliği artık büyük bir soru işaretidir. Son Gazze saldırıları, bu düzenin ne ölçüde işlediğini sorgulatan en çarpıcı örneklerden biridir. İfade ettiğiniz gibi bu süreç devam ederse mevcut uluslararası sistem zaten bir sorgu sürecinde, daha da sorgulanacak ve alternatiflere daha fazla açık hale gelecektir. ABD ve batının bu koşulsuz desteği aynı zamanda uluslararası düzeyde insan hakları ve demokrasi argümanlarını da zayıflatmaktadır. Başka yerde bu değerleri önceledığini söyleyen aktörler eğer, birçok göstergeye göre savaş suçu, insanlığa karşı suç ve soykırım suçu teşkil eden İsrail saldırganlığı savunmaya devam ederslerse bu değerleri gerekçe göstererek artık kimseyi ikna edemeyecekler. İkna olmayınca da kolay kolay bu ihallerin yoğun olduğu ve müdahale gerektiren başka yerlerde de uluslararası kamuoyunun desteğini bulamayacaklar. Bu da mevcut sistemi zaafa uğratacaktır. Hatta buna alternatif teokratik rejimlerin kurulacağı oldukça baskıcı ve zalim düzenler bile ciddi destek almaya başlayacaktır. Uluslararası sitem maalesef böyle bir trende girmiş durumda. Bu terndin bizi götüreceği durak maalesef daha barışçıl ve özgürlükçü olmayacaktır.

Dijital Caydırıcılık Siber Güce Pararlel Bir Olgudur

Çıkardığınız derginin 2021'deki 11.sayısında Ozan Sabri Tuncer'in *"Siber Caydırıcılık"* üzerine ilginç bir makalesi vardı. Bu makaleden hareketle siber terör, siber saldırı ve siber suçlara karşı siber caydırıcılığı sağlamanın yolu yordamı üzerine neler söylersiniz? Siber caydırıcılık kapasitesini artırmak için ne tür stratejiler izlenmelidir? Bununla ilişkili siber ordu kurma, siber istihbarat gibi literatürde yer alan gelişmeler, siber saldırılar ve siber savaşlar karşısında önleyici ve caydırıcı nasıl olunabilirler?

Dijital alanda siber caydırıcılık var mı? tartışması uluslararası ilişkilerde son 10 yılda çokta tartışıldı. Kimisi yok dedi, kimisi var da zayıf dedi, kimisi nükleer caydıcılığı bile aşan bir düzeyde dedi. Siber caydırıcılık, devletlerin veya diğer aktörlerin siber saldırılara karşı caydırıcı güçlerini artırmalarını gerektirir. Bunun için, güçlü bir siber altyapı, yazılım ve donanımın yerli üretimi, güçlü bir siber hukuk ve kurumsal çerçeve, kapsamlı bir teknik ve bilinç eğitimi ve

uluslararası işbirliği gerekir. Bu bağlamda, Ozan Sabri Tuncer'in makalesin de geçtiği gibi, caydırıcılığı sağlayan temel unsurlar arasında güçlü altyapı, sürekli siber tatbikatlar, işbirliği, eğitim ve karşı saldırı kapasitesi yer alıyor.

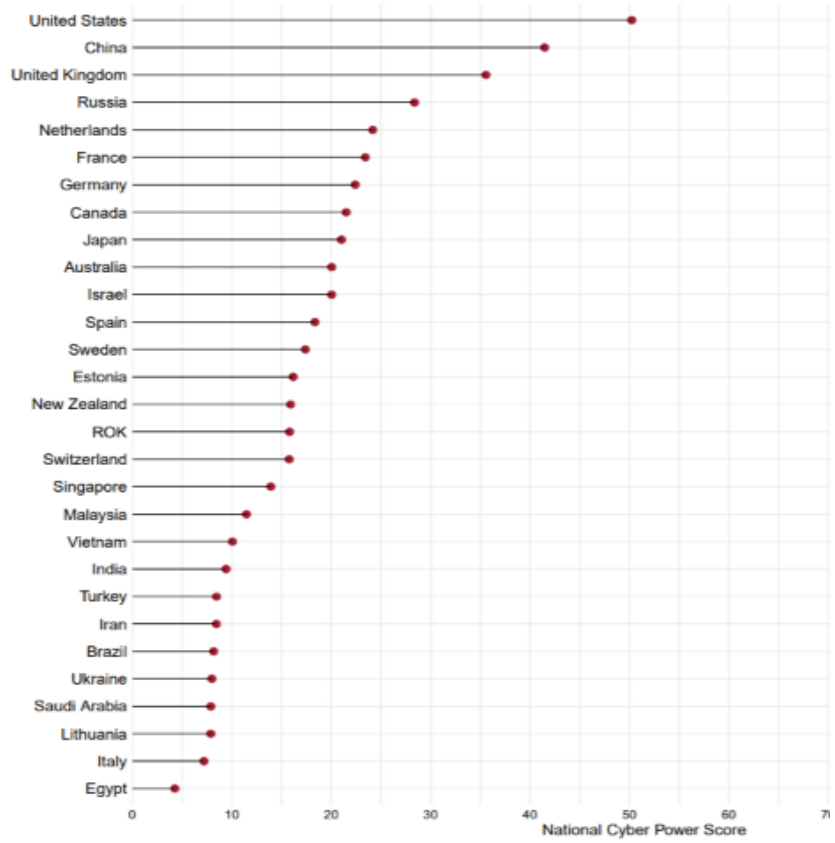
Dijital caydırıcılık siber güce pararlel bir olgudur. Siber güç kendi başına birşey ifade etmez, diğer ulusal güç unsurlarıyla birleşerek ancak ulusal gücün bir bileşeni olur. Bu çerçevde, uluslararası istatistikler ve endexler bize bir takım ipuçları verebilir.

Cambridge Belfer Merkezi tarafından oluşturulan daha önce bir akademik çalışmamda kullandığım *Ulusal Siber Güç Endeksi* (NCPI), 30 ülkenin siber yeteneklerini, siber yöntemlerle yedi yeteneği elde etme çabalarını değerlendirerek analiz eder. Bu yetenekler;

• Saldırgan siber grupların gözetlenmesi ve izlenmesi,
• Ulusal siber savunmaların güçlendirilmesi ve geliştirilmesi,
• Bilgi ortamının -siber uzayın- kontrol edilmesi ve manipülasyonu,
• Ulusal güvenlik için yabancı istihbarat toplama,
• Ticari kazanç veya sanayi büyümesinin geliştirilmesi,
• Bir düşmanın altyapısını ve yeteneklerini yok etme veya etkisiz hale getirme, ve,
• Uluslararası siber normları ve teknik standartları tanımlama gücü. (Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, Dan. & Schwarzenbach, A. (2020). *National Cyber Power Index 2020*. Belfer Centre; Akyeşilmen, N. (2022). Türkiye in the global cybersecurity arena: Strategies in theory and practice. *Insight Turkey, 24*(3), 109-134 ve).

NCPI, ülkelerin gözetim, savunma, kontrol, istihbarat, ticaret, saldırı ve normlar dahil olmak üzere çeşitli alanlardaki niyet ve yeteneklerini analiz eden tablo aşağıdadır.

Graph 1: NCPI 2020: Most Comprehensive Cyber Powers



Kaynak: https://www.belfercenter.org/sites/default/files/2024-09/NCPI_2020.pdf

Siber Caydırıcılığı Artırmanın En Önemli Unsuru, Yerli Yazılım ve Donanım Kapasitesini Artırmaktır

Siber caydırıcılık, potansiyel saldırganları eylemlerinden vazgeçirmek amacıyla belirli maliyetler ve riskler oluşturarak, saldırının sonuçlarının olumsuz olacağını gösteren bir stratejidir.

- Siber caydırıcılık kapasitesini artırmak için izlenebilecek bazı stratejiler şöyle sıralanabilir.
- Öncelikle uygulanabilir, gerçekçi ve şeffaf bir ulusal siber güvenlik strateji belgesini ortaya koyabilmek,
- Yazılım ve donanım üretme kapasitesini arttırmak,
- Teknolojik altyapıları güncel ve güçlü tutmak,
- Kritik altyapıların korunması için ulusal çerçeveler ve uygulamalr geliştirmek,
- Siber güvenlik farkındalığının artırılması,

- Siber güvenlik eğitimi, özellikle Avrupa Konseyi'nin geliştirdiği dijital vatandaşlık eğitimini ya da OECD'nin küresel vatandaşlık eğitimini yaygınlaşrarak müfredatın her düzeyine yerleştirmek,
- Güncel tehditlere karşı sürekli güncellenen savunma mekanizmaları geliştirmek,
- Potansiyel tehditlerin erken tespiti,
- Karşı saldırı planlarının geliştirilmesi,
- Siber saldırıların tespit edilmesi ve engellenmesi için gerekli teknik bilgi ve becerilerin geliştirilmesi,
- Iyi koordine edilmiş ve güçlü ulusal siber olaylara müdahale ekiplerinin geliştirilmesi,
- Diğer ülkelerle işbirliği ve bilgi paylaşımı,
- Ortak operasyonlar ve tatbikatlar,
- Uluslararası standartların geliştirilmesi,
- Siber suçlarla mücadeleye yönelik yasal düzenlemelerin yapılması,
- Siber suçluların cezalandırılmasının sağlanması
- gibi bir dizi strateji geliştirilebilir. Fakat en önemlisi nedir derseniz yerli yazılım ve donanım üretme kapasitesinin geliştirilmesi, dijital vatandaşlık eğitimi ve ulusal ve uluslararararası işbirliklerinin geliştirilmesidir. Siber güvenlikte en zayıf halka bireydir ya da kullanıcıdır. Bu nedenle teknik ve bilinmçlendirme eğitimi siber güvenliğin en temel taşıdır. Acil ve anlık bir ihtiyaçtır. Gecikmeksizin önlemler alınmalıdır.

Birçok Konuda Olduğu Gibi Türkiye'de Siber Alanda da Ciddi Şefafflık Sorunu Var

Cumhurbaşkanı Erdoğan, 7 Ekim'den beri İsrail'in işgalci ve yayılmacı politikalarının Gazze'den sonra sırasıyla Lübnan, Suriye ve Türkiye gibi bölge ülkelerini de kapsayacağını ve sıranın bölge ülkelerine geleceğinden dem vuruyor. İsrail'in işgalci ve yayılmacı politikası ile gelecek olası siber saldırılara ve siber savaşa karşın, Türkiye'deki siber güvenlik kurumlarınınım kapasitesini nasıl buluyorsunuz? Siber ordu, siber istihbarat, siber savunma ve literatürde siber uzay denilen Türkiye'nin ise siber vatan dediği bu başlıklardaki gücü nedir? Türkiye ne tür yazılımsal ve donanımsal hamlelere imza atmıştır? Siber caydırıcılık, siber güvenlik ve siber ordu alanındaki karnesi nedir?

Tabi bu konuda daha çok açık kaynaklar üzerinden yorum yapma imkânımız var. Maalesef birçok konuda olduğu gibi Türkiye'de siber alanda da ciddi bir şefafflık sorunu vardır. Herkesin paylaştığı ve güvenlik açısından herhangi bir sorun teşkil etmeyen veriler bile kamuoyundan gizlenmektedir. Bu hem bilimsel çalışma yapmak açısından ciddi bir çıkmazdır hem de onların

akademik olarak yorumlanması ve olası politik tavsiyelerin geliştirilmesi açısından engel teşkil etmektedir. Sadece bürokrat kafası bize yeter anlayışı ulusal düzeyde ciddi bir potansiyel kaybına neden olmakrtadır.

Türkiye'nin dünyadaki gelişmelere paralel olarak 2010'lardan itibaren siber güvenlik alanında önemli adımlar attığına şahit oluyoruz. İlk ulusal siber güvenlik strateji belgesini 2013 yılında yayımladı ve bugüne kadar üçüncü versiyonunu kamuoyuyla paylaştı. Son belgede daha önceki belgelerde detaylı bir şekilde yayımlanan siber güvenlikten sorumlu kurum ve kuruluşlar ile eylem planı son raporda gizlendi. Dünyada bu tarz gizlenme örnekleri pek yoktur ki zaten daha önceki raporlarda bunlar yayınlanmış. Bazı şeyler gizlense bile bunları gizledim denmez. Gizlersin sadece. Siber güvenlik strateji belgesi önemli bir hamle, fakat bu belgenin gerçekçi, uygulanabilir ve kapasite ile uyumlu olması gerekir. Tabi son raporda eylem planı gizlenince birçok şeyleri tartışmak ya da analiz etmek zor. Eski raporlar üzerinden yorum yapılabilir.

Yine son yıllarda Türküye Silahlı Kuvvetleri bünyesinde kurulan daha önce elektronik harp birimi Siber Savunma Komutanlığı'na dönüştü. Emniyet ve jandarmada siber istihbarat ve suçlarla mücadele birimleri, MİT, BTK ve TÜBİTAK bünyesinde kurulan birimler, SOMEler ve organizasyonları, Havelsan, Aselsan ve diğer özel ve yarı resmi şirketlerin faaliyetleri çok nemli adımlar olarak göze çarpıyor. Son yıllarda üretilen yazılımlar, siber güvenlik çözümlemeleri, güvenlik duvarı gibi daha dar çerçeveli donanımlar da yeterli olmasa bile kayda değer gelişmelerdir. Bu adımlar sayesinde, dışa bağımlılığı azaltmak ve siber güvenlik ekosistemini güçlendirmek amaçlanmıştır. Ancak, bu alandaki çalışmaların henüz yeterli düzeyde olmadığı ve daha fazla yatırıma ihtiyaç olduğu söylenebilir.

Türkiye Siber Güvenlik Alanında Son Yıllarda Kurumsal ve Hukuk Alanında Önemli Bir Yol Katetti

Kavramsallaştırmalar bazen konuyu daha iyi anlamak ve çözümler geliştirmek için yararlı olabilir. Fakat bu kavramsallaştırmalar, bilimsel ve teknolojinin doğasıyla uyumlu olduğu sürece böyledir. Siber vatan ya da Çinlilerin siber egemenlik dediği kavramlar kulağa hoş geliyor fakat siber teknolojinin doğası dikkate alındığında bazı sıkıntılar barındıran kavramlardır. Siber vatan kavramı, Türkiye'de dijital ekosistemi bir bütün olarak korumayı ve bunu ulusal güvenliğin bir bileşeni olarak algılamakta. Çin'in siber egemenlik kavramı da benzer bir kavramdır. Fakat siber uluslararası ilişkilerde, fiziksel uluslararası ilişkilerde olduğu gibi sınırlar yok. Hukuk, özellikle uluslararası hukuk çok zayıf. Hukuku uygulama kapasitesi oldukça zayıftır. Bu nedenle, düşünüldüğünde kavramların içi boş kalıyor. Yerli fizik ya da yerli matematik demek gibi birşey. Fakat kavram olarak kullanmakta bir beis yok bence.

Türkiye siber güvenlik alanında son yıllarda kurumsal ve hukuk alanında önemli yol katetti fakat ulusal siber güç endeksinde görüldüğü gibi, daha çok ciddi adımların atılması gerekir. Bir de bu teknoloji bir hareketli hedef gibidir. Sürekli değiştiğinden alınacak her önlem yakın gelecekte eksik ya da zayıf kalabiliyor. Kurumsal ve teknik alanda bir sürekli değişim ve gelişim momenti kazanmak önemli. Bu da ciddi uzmanlıkla ve partizanlık yapmadan uzman görüşleri, uzman destekleri almakla mümkündür. Bu alan olabildiğince teknik ve bilgi istiyor. Ehliyet ve liyakat her alanda çok önemli fakat burada çok ama çok daha önemli.

Global Siber Güvenlik Endeksi'ne Göre Türkiye, Güçlü Bir Performans Sergilemektedir

Dışişleri Bakanı Hakan Fidan, geçtiğimiz günlerde *"Siber Güvenlik Teşkilatı"* kurulmasına dönük bir hazırlıktan bahsetti. Türk Silahlı Kuvvetleri bünyesinde de Siber Savunma Komutanlığı oluşturuldu. Türkiye'nin ister İsrail'den gelebilecek, ister mafyatik veya dış istihbarat kurumlarından gelebilecek askeri veya siyasi siber tehditlere karşı hangi kurumları şu anda aktif durumdadır? Bize bu kurumlardan ve neler yaptıklarından biraz bahsedebilir misiniz? Geçenlerde Uluslararası Telekomünikasyon Birliği (ITU) tarafından hazırlanan, "*Global Siber Güvenlik Endeksi"* ne dair verileri gördüm. Eğer sizde gördüyseniz bu endekse göre Türkiye'nin durumu nedir?

Dışişleri Bakanı Hakan Fidan'ın açıkladığı "Siber Güvenlik Teşkilatı" projesi, Türkiye'nin siber güvenlik alanında atacağı ciddi bir adım olur. Yukarıda bahsettiğimiz başlıca kurumlar ve var olan diğer pek çok irili ufaklı kurum da önemli işler yapıyorlar, fakat yetersizler. Daha bu hafta bütün vatandaşların kimlik bilgilerinin çalındığına dair yoğun tartışmalar yaşadık. Bu nedenle, kapsamlı çalışmalar yapacak, bağımsız bir siber güvenlik kurumu gerekir. Geç bile kalındı bu hususta. Fakat zararın neresinden dönülürse kardır. Kurum kurmak yetmez, niteliği çok önemli. İsrail'in ulusal siber güvenlik koordinasyon merkezi olan siber güvenlik kurumu doğrudan İcranın başı olan Başbakana bağlıdır. O nedenle, esnek, hızlı, yetkin ve etkin bir yapısı vardır. Yine siber güvenlik sadece dijital alan uzmanlarıyla, yani teksniyenlerle sınırlandırılmamalıdır. Böyle bir kurumda teknik elemanların yanında siyasetten psikolojiye, hukuktan çevreye kadar geniş yelpazede bir uzman kadrosuna sahip olmalıdır. Tıpkı ABD ulusal güvenlik ajansı NSA gibi. Bizde kurulacak kurum doğrudan icranın başına bağlı, etkin ve yetkin bir kurum, farklı

disiplinlerden uzmanlar ve pattizan olmayan bir kadro kurulursa, iş yapar. Yoksa var olan bir dizi kurumlardan birisi olmaya devam eder.

Siber güvenlik bir bütündür, kurumsal altyapıyı hukuki çerçeveden, eğitimi işbirliğinden ayıramayız. *BM ITU Küresel Güvenlik endeksi* bu alandaki çalışmaların ilklerindendir. Son 10 yılda 5. Endeksi yayanladı ki bu çok büyük bir başarı aslında bir uluslararası örgüt için. Yöntem açısından bilimselliği ve ölçülebilirlik kapasitesi sorgulansa bile (çünkü endeks maalesef üye ülkelerle yapılan anket verisine dayanıyor) önemli bir göstergedir.

Türkiye, son yıllarda siber güvenlik alanında önemli ilerlemeler kaydetmiş ve özellikle askeri, devlet ve istihbarat kurumları aracılığıyla bu alanda kapasitesini genişletmiştir. Siber Savunma Komutanlığı, BTK (USOM), MİT ve TÜBİTAK BİLGEM gibi kurumlar, Türkiye'nin siber tehditlere karşı direncini artırmada kritik rol oynamaktadır. Bununla birlikte, Dışişleri Bakanı Hakan Fidan'ın bahsettiği Siber Güvenlik Teşkilatı gibi **yeni yapılar, Türkiye'nin ulusal siber savunma kapasitesini daha da güçlendirecek adımlar olarak değerlendirilmektedir.** Global Siber Güvenlik Endeksi'ne **göre Türkiye, güçlü bir performans sergilemekte olup, gelişmiş kapasitesini daha da ileriye taşıyarak siber güvenlik alanında küresel düzeyde daha etkili bir oyuncu olma potansiyeline sahiptir.**

Ben Bu Dönemi, Belirsizlikler Çağı Ya Da Post-Truth Çağı Olarak Adlandırıyorum

Tarım toplumu, sanayi toplumu, bilgi toplumu gibi kategorilerden sonra içinde yaşadığımız çağa dair birtakım okumalar yapmaktalar fütüristler, postbiyologlar, genom uzmanları, nano ve tekno-mühendisler, sosyal bilimciler…. Yapay zekânın geleceği, Endüstri 1.0'den Endüstri 10.'nun konuşulduğu, makine-insan denilen insan 3.0'dan İnsan 4.0'a yani ölümsüz insana geçeceği söylenen devasa tekno gelişmeler… Peki, siz şu anda insanlığın içinden geçtiği 21.yüzyıl çağını siz neyle adlandırıyorsunuz? Nasıl bir dünya mimarisi kuruluyor? Nasıl bir toplum ve birey bizi bekliyor?

İçinde yaşadığımız zamanı anlatmak için bir dizi tanımlama kullanılmaktadır ve muhtemelen hepsi de kendi ekosisteminde doğrudur. Dijital çağ, bilgi çağı 2.0, yapay zeka çağı, siber-biyolojik çağ gibi. Ben bu dönemi daha çok belirsizlikler çağı, ya da post-truth dedikleri herşeyin algı ve mnaipülasyona dayandırıldığı gerçeğin kaybolduğu çağ şeklinde adlandırıyorum. Yapay zekâ ve veri de çok önemli bu çağda. Yakın zamana kadar, bu çağda veriye hükmeden dünyaya hükmeder denirdi. Çünkü veri bu çağın petrolu olarak tanımlanmaktaydı. Fakat şimdi onun yerine yapay zekayı geliştiren dünyaya hükmeder deniyor. Eskiden çağla ifade edilen büyük değişimler şimdi birkaç yılla ifade edilir oldu. Bu değişime

ayak uydurmak çok zor. Ciddi bir çaba ve emek gerektiriyor. Hamasi söylemlerle, gerçekten kopuk iddialarla bir yere kadar gidilebilir ancak.

Teknoloji hız demek, fakat hız kontrol edilmezse felaket getirir. Bugün birçok siber olay ve siber tehditler bizim hızlı davranmamız ve yeterince düşünmeye zaman ayırmamamızdan kaynaklanıyor. Hızlı mesaj atacağız diye yanlış kişilere mesaj atarız. Bize gelen oltalama mesajlarına inanarak hızlıca hesaplarımızı koruyacağız diye kendi elimizle şifrelerimizi ya da bilgilerimizi saldırganlara yolluyoruz. Bu çağda bizi kurtaracak şey düşünerek hareket etmektir.

Ahlak Yüzlü Bir Teknoloji Şiariyle Daha İnsani ve Ahlaki Bir Dijital Düzen Kurulabilir

Teknoloji kötü birşey değil aksine çok yararlı birşey. Konumuz siber güvenlik olunca olumsuzluklarına odaklandık, oysa siber teknoloji ve dijitalleşme insanlığı geleceğidir ve bu bilinçle onu gözümüz gibi korumalıyız. Bu da ancak küresel bir işbirliği ile mümkündür. Fiziksel çevreyi korumak için nasıl bir çalışma ve bilinç varsa (yeterli değil fakat küresel çapta son yıllarda bir pozitif algı inşa edildi) dijital çevreyi korumak için de aynı hassasiyet ve çaba sarf edilmelidir. Bu yapılmazsa gelecek nesiller çok büyük zorluklar çekecektir. Bütün bunların önüne geçmek ya da bu etkileri hafiletmenin yolu siber ahlakı geliştirmekten geçer. Ahlak yüzlü bir teknoloji şiariyle ancak daha insani ve daha ahlaki bir dijital düzen kurulabilir. Dijital bir küresel toplum var bugün. 5.5 milyar insan interneti kullanıyor. Bunun farkında olarak daha evrensel ve küresel işbirliği ve eşitliği koruyan bir düzen kurulmalıdır.Teknolojiye düşmanlık yapılmaz, teknolojiyle savaşılmaz. Adapte edilir ve insani bir yüz kazandırılarak insanlığın hizmetine sunulur. Buna katkı sunmak bütün dijital vatandaşların ahlaki sorumluluğudur.

Giderek dijitalleşen bir dünyada veri çok önemli ve yapay zeka hayatımızı derinden şekillendirmeye devam ediyor. Siber güvenlik kişsel düzeyden küresel düzeye bir sorun olmaya devam ederken, insan-makina iletişimi derinleşecektir. *Black Mirror* dizi bu konuda bize ciddi ipuçları vermektedir. Gelecekte toplumların teknoloji tutsağı haline gelmesi, insanların robotlaşması, insan beynine fiziksel müdahaleler gibi ahlaki sorunlar insanlığa yönelik ciddi sorunlardır. Gelecekte bireysel anayasalardan, dijital devletlere kadar tahmin edilmesi zor projelerle karşılaşılabilir.

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 Cyberpolitic

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 Cyberpolitic

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.