ISSN: 2587-1218

CYBERPOLITIK JOURNAL
Siber Politikalar Dergisi

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

www.cyberpolitikjournal.org

Winter 2023

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. Mustafa Cüneyt Özşahin

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: BASICS OF THE METAVERSE

Dear Readers,

We are proud to present to you the 16th issue of the *Cyberpolitik Journal*. It is a great honor for all of us to continue our journey that we started eight years ago without interruption. As the digital world grows every day and every second, new developments and new technologies emerge, we are trying to read and understand this domain within our limitations.

In an era dominated by the omnipresence of technology and interconnected digital ecosystems, the role of digital citizenship education cannot be overstated. The articles featured in the 8th volume and 16th issue of the *Cyberpolitik Journal* bring forth a compelling narrative, shedding light on diverse facets of cyber landscapes, from cybersecurity policies to geopolitical rivalries in cyberspace. Among these, the exploration of "Human Rights-Based Digital Citizenship Education" by Nezir Akyeşilmen stands out as a beacon, advocating for ethical considerations that pave the way for cyber peace.

The interconnectedness of our world has given rise to a digital society where the boundaries between physical and virtual realms blur. As such, fostering responsible digital citizenship is not merely an educational endeavor but a prerequisite for cultivating a global culture of cyber peace. Akyeşilmen's emphasis on human rights as the cornerstone of digital citizenship education is timely and resonates with the growing need to address the ethical dimensions of our online existence. The author develop and propose a human rights-based model for digital citizenship education that claiming ethics as the backbone of cyber peace. The article focuses on the basic elements of digital citizenship education and develops principles of education model from internationally recognized human rights instruments.

In the contemporary geopolitical landscape, cyber threats and attacks transcend national borders, making it imperative for nations to collaboratively address the challenges posed by the digital domain. The comparison of cybersecurity policies between Türkiye and England, as articulated by Gül Nazik Ünver, provides valuable insights into the diverse approaches

adopted by nations in fortifying their cyber defenses. National Cybersecurty strategies of Türkiye and Endland diverse but they have also many commanalities. International cooperation is a vital strategy for a successful cyber defence in cyberspace.

Akyeşilmen's proposition of a human rights-based approach to digital citizenship education urges us to consider the ethical implications of our actions in the digital realm. As we witness the fierce competition between major players like the United States and Russia in cyberspace, as presented by Gizem Dede, it becomes evident that a shared understanding of ethical behavior in the digital realm is essential for fostering trust and cooperation on the international stage.Dede, focuses mainly on cyber attacks by russia but it is well known that all actors in cyberspace are pro offense in digital realm.

Elif Güldal Limon's exploration of Turkey's military communication systems highlights the critical role of cybersecurity and the imperative of localizing capabilities in the face of evolving threats. It is within this context that digital citizenship education emerges not only as a tool for individual empowerment but as a collective defense mechanism against cyber threats that transcend borders.

In the realm of opinions, Yavuz Akdağ's perspective on Cyber-AI technology and international relations underscores the rapid advancements in technology and their profound impact on geopolitics. However, as we navigate this intricate landscape, E. Dilara Kılınç's focus on the problems of digital citizenship in the cyber world resonates strongly. The challenges posed by the digital realm extend beyond mere technological aspects; they encompass the very fabric of our society, demanding a comprehensive and ethical approach.

Kamil Tarhan's review of "Technology Ethics: A Philosophical Introduction and Readings" aligns with the call for a philosophical underpinning in our approach to digital world. It prompts us to delve into the ethical frameworks that guide our interactions in cyberspace, emphasizing the need for a holistic understanding that goes beyond technical proficiency.

In conclusion, the 8th volume and 16th issue of the Cyberpolitik Journal offers a comprehensive panorama of the challenges and opportunities presented by the digital era. In this landscape, digital citizenship education emerges as a linchpin for cultivating responsible

behavior, fostering ethical considerations, and ultimately contributing to the attainment of cyber peace. As we navigate the complexities of cyberspace, it is essential to recognize that the path to a secure and harmonious digital future begins with the education of responsible and ethically conscious digital citizens.

EDİTORYAL ÖNSÖZ: METAVERSİN TEMELLERİ

Sevgili okuyucular,

Cyberpolitik journal Dergisi'nin 16. sayısını sizlere sunmaktan gurur duyuyoruz . Sekiz yıl önce başladığımız yolculuğumuzun kesintisiz devam etmesi hepimiz için büyük bir onur. Dijital dünya her geçen gün büyürken, yeni gelişmeler ve yeni teknolojiler ortaya çıkarken, biz de bu alanı kendi sınırlarımız dahilinde okumaya, anlamaya çalışıyoruz.

Teknolojinin ve birbirine bağlı dijital ekosistemlerin her yerde mevcut olduğu bir çağda, dijital vatandaşlık eğitiminin rolü yadsınamaz. *Cyberpolitik Journal*'ın 8. cildi ve 16. sayısında yer alan makaleler, siber güvenlik politikalarından siber uzaydaki jeopolitik rekabetlere kadar siber ortamın farklı yönlerine ışık tutan ilgi çekici bir anlatıyı ortaya koyuyor. Bunlar arasında Nezir Akyeşilmen'in "İnsan Hakları Temelli Dijital Vatandaşlık Eğitimi: Siber barış için etik" araştırması, siber barışın yolunu açacak etik hususları savunan bir yol gösterici rehber olarak öne çıkıyor.

Dünyamızın birbirine bağlılığı, fiziksel ve sanal alanlar arasındaki sınırların bulanıklaştığı dijital bir toplumun ortaya çıkmasına neden oldu. Bu nedenle, sorumlu dijital vatandaşlığın teşvik edilmesi yalnızca eğitimsel bir çaba değil, aynı zamanda küresel bir siber barış kültürünün geliştirilmesi için bir ön koşuldur. Akyeşilmen'in dijital vatandaşlık eğitiminin temel taşı olarak insan haklarına yaptığı vurgu günceldir ve çevrimiçi varoluşumuzun etik boyutlarına yönelik artan ihtiyaçla örtüşmektedir. Yazar, etiğin siber barışın omurgası

olduğunu iddia eden dijital vatandaşlık eğitimi için insan haklarına dayalı bir model geliştirip önermektedir. Makale, dijital vatandaşlık eğitiminin temel unsurlarına odaklanmakta ve uluslararası kabul görmüş insan hakları belgelerinden eğitim modelinin ilkelerini geliştirmektedir.

Çağdaş jeopolitik ortamda siber tehditler ve saldırılar ulusal sınırları aşıyor ve bu da ulusların dijital alanın yarattığı zorlukları işbirliği içinde ele almasını zorunlu kılıyor. Gül Nazik Ünver'in dile getirdiği Türkiye ve İngiltere siber güvenlik politikaları karşılaştırması, ulusların siber savunmalarını güçlendirmek için benimsedikleri farklı yaklaşımlar hakkında değerli bilgiler sağlıyor. Türkiye ve Endland'ın ulusal siber güvenlik stratejileri farklılık gösterse de pek çok ortak noktaya da sahiptir. Uluslararası işbirliği, siber uzayda başarılı bir siber savunma için hayati bir stratejidir.

Akyeşilmen'in dijital vatandaşlık eğitimine insan hakları temelli bir yaklaşım önerisi, bizi dijital alandaki eylemlerimizin etik sonuçlarını düşünmeye sevk ediyor. Gizem Dede'nin de belirttiği gibi, siber uzayda ABD ve Rusya gibi büyük oyuncular arasındaki şiddetli rekabete tanık olduğumuzda, uluslararası alanda güven ve işbirliğini geliştirmek için dijital alanda ortak bir etik davranış anlayışının gerekli olduğu açıkça ortaya çıkıyor. Dede, ağırlıklı olarak Rusya'nın siber saldırılarına odaklanıyor ancak siber uzaydaki tüm aktörlerin dijital alanda da suç yanlısı olduğu biliniyor.

Elif Güldal Limon'un Türkiye'nin askeri iletişim sistemlerini incelemesi, siber güvenliğin kritik rolünü ve gelişen tehditler karşısında yeteneklerin yerelleştirilmesinin zorunluluğunu vurguluyor. Bu bağlamda dijital vatandaşlık eğitimi sadece bireysel güçlendirme aracı olarak değil, sınırları aşan siber tehditlere karşı kolektif bir savunma mekanizması olarak da ortaya çıkıyor.

Görüşler açısından Yavuz Akdağ'ın Siber-Yapay Zeka teknolojisi ve uluslararası ilişkilere bakış açısı, teknolojideki hızlı gelişmelerin ve bunların jeopolitik üzerindeki derin etkisinin altını çiziyor. Ancak bu karmaşık manzarada ilerlerken E. Dilara Kılınç'ın siber dünyadaki dijital vatandaşlık sorunlarına odaklanması güçlü bir şekilde yankılanıyor. Dijital dünyanın getirdiği zorluklar salt teknolojik boyutların ötesine uzanıyor; kapsamlı ve etik bir yaklaşım gerektiren toplumumuzun dokusunu kapsıyorlar.

Kamil Tarhan'ın "Teknoloji Etiği: Felsefi Bir Giriş ve Okumalar" incelemesi, dijital dünyaya yaklaşımımızda felsefi bir temel oluşturma çağrısıyla örtüşüyor. Teknik yeterliliğin ötesine geçen bütünsel bir anlayışa duyulan ihtiyacı vurgulayarak bizi siber uzaydaki etkileşimlerimize yön veren etik çerçeveleri araştırmaya teşvik ediyor.

Sonuç olarak Cyberpolitik Dergisi'nin 8. cildi ve 16. sayısı, dijital çağın sunduğu zorlukların ve fırsatların kapsamlı bir panoramasını sunuyor. Bu ortamda dijital vatandaşlık eğitimi, sorumlu davranışı geliştirmek, etik hususları teşvik etmek ve sonuçta siber barışın sağlanmasına katkıda bulunmak için bir temel taşı olarak ortaya çıkıyor. Siber uzayın karmaşıklıklarında yol alırken, güvenli ve uyumlu bir dijital geleceğe giden yolun sorumlu ve etik açıdan bilinçli dijital vatandaşların eğitimiyle başladığını kabul etmek önemlidir.

Nezir AKYEŞİLMEN, Ph.D

Editor-in-Chief

x

COMPARISON OF CYBER SECURITY POLICIES OF TÜRKİYE AND ENGLAND

Gül Nazik ÜNVER[1]

ORCID: 0009-0005-5003-1555

Abstract

This study evaluates and presents a comparative analysis of all political, strategic, educational, legal, economic, social and organizational aspects of Türkiye and England, which implement cyber security policies. In this study, the analysis of cyber security strategies followed by Türkiye and England has been tried to be revealed. In this study, it is seen that cultural differences play an important role in the cyber field of developed states like England and developing states like Türkiye. Cyber security policies implemented in Türkiye and England adopt a more flexible approach. As a result of this research, it has been seen that these two countries attach importance to their economic and individual dimensions.

The study firstly claims that it is possible to analyze cyber security policies in five dimensions comparatively according to the Global Cyber Security Index (GCI) data and that cyber policies interact at an international level. Cyber security policies include important strategic issues related to security. Secondly, it shows how Türkiye and England design and implement their national cyber security policies, how they approach counter-strategies, and how they respond to increasing threats in the cyber space. In this context, thirdly, by comparing these two countries within various cyber security indices, it is discussed how the best cyber policies can be for countries in the cyber field. Finally, suggestions are made to guide future research on this subject.

Keywords: Cyber Space, Cyber Security, Cyber Security Policies, Cyber Security Indices.

TÜRKİYE VE İNGİLTERE ÜZERİNDEN SİBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRILMASI

Özet

[1] Dr., Batman University, E-mail: gul.unver@batman.edu.tr This study was produced from the author's PhD thesis. For Detailed Information: Ünver, Gül Nazik (2023). Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği, *PhD Thesis*, Konya: Selcuk University.

Bu çalışma, siber güvenlik politikaları uygulayan Türkiye ve İngiltere'nin politik, stratejik, eğitim, yasal, ekonomik, sosyal, organizasyonel tüm yönlerini değerlendirmekte ve karşılaştırmalı bir analizini sunmaktadır. Bu çalışmada, Türkiye ve İngiltere'nin izlemiş olduğu siber güvenlik stratejilerinin analizi ortaya konulmaya çalışılmıştır. İngiltere gibi gelişmiş ve Türkiye gibi gelişmekte olan devletlerin siber alanda kültürel farklılıkların önemli rolü olduğu bu çalışma da görülmektedir. Türkiye ve İngiltere'de uygulanan siber güvenlik politikaları daha esnek bir yaklaşımı benimsemektedir. Bunu özellikle bu iki ülkenin ekonomik ve bireysel boyutlarını önemsediği bu araştırma sonucunda görülmüştür.

Çalışma ilk olarak, Küresel Siber Güvenlik Endeksi (GCI) verilerine göre siber güvenlik politikalarını beş boyutta karşılaştırmalı olarak analiz etmenin mümkün olduğunu ve siber politikaların uluslararası düzeyde bir etkileşim içinde olduğunu iddia etmektedir. Siber güvenlik politikaları, güvenlikle ilgili önemli stratejik konuları içermektedir. İkinci olarak, Türkiye ve İngiltere'nin ulusal siber güvenlik politikalarını nasıl tasarladıklarını ve bu politikaları nasıl uyguladıklarını, karşı stratejilere nasıl yaklaştıklarını, siber alanda artan tehditlere nasıl yanıt verdiklerini göstermektedir. Bu kapsamda da üçüncü olarak, bu iki ülkenin çeşitli siber güvenlik endeksleri dâhilinde karşılaştırılmasıyla, siber alanda ülkeler için en iyi siber politikaların nasıl olabileceği tartışılmaktadır. Son olarak bu konuda bundan sonra yapılacak araştırmalara yol gösterici önerilerde bulunulmaktadır.
Anahtar Kelimeler: Siber Alan, Siber Güvenlik, Siber Güvenlik Politikaları, Siber Güvenlik Endeksleri.

Introduction

In this study, cyber security policies are discussed comparatively with the examples of Türkiye and England (in this paper, the United Kingdom is referred to as England). States have their own historical and unique conditions in the development of their cyber security policies. Moreover, it is clear that structural similarities cannot be ignored in this development process. With cyber security, it is possible to explain the evolution of traditional processes into innovative processes in the 20th and 21st centuries. It is inevitable that there are similarities and differences in the improvement of cyber security policies in Türkiye and England. According to the Global Cybersecurity Index, based on the measurement data of cyber security impacts in Europe, England is ranked 1st in the list, while Türkiye is ranked 11th (Global Cybersecurity Index, ITU, 2018: 60). It is seen that England is better than

Türkiye in terms of implementing strategies. England is more active than Türkiye in coordinating and implementing cyber security policies.

Türkiye focuses on preventing the damage to the technical and organizational structure of cyber incidents. England, on the other hand, focuses on cyberspace to prevent cyber incidents from attacking national critical information infrastructures and key network resources. From a cyber security perspective, Türkiye's priority is public and state security, while England's priority is individual security and human rights. In cyber security, Türkiye encourages public institutions and works on the awareness of increasing their standards.

Türkiye's strategy aims to help individuals understand the risks linked to their use of technology and be able to use it safely to meet future challenges related to inclusive changes in the digitization of Turkish society. The basis of the national strategy in England is education and international cooperation to promote the economy, citizens and national values. Türkiye's strategy is to ensure that critical infrastructures are resistant to cyber attacks. Türkiye's strategy intends to support and raise awareness of cyber security. Türkiye's cyber security principles are efficiency, resilience and foresight. England's principles are broad and some focus on protection, accountability and cooperation. Türkiye and England have openly expressed their current or future action plans to promote global cooperation.

It is recommended in the study that the countries that will prepare or update their cyber security strategy should have a holistic perspective, determine their priorities and focus more on the aspects of cyber security that are compatible with their national priorities. Another important point is the fact that opportunities are taken into account as well as threats and risks in cyberspace. It is hoped that this study will be a beneficial guide for researching cyber security policies and collaboration models in future studies.

In Türkiye, the Internet had an impact in the world of defence, research and academia in the early 1990s. The innovators and founders of the communication infrastructure that individuals and societies generally trust and the services provided through it are represented by the Information Technologies and Communications Authority (ITC) in Türkiye. The innovators and founders of the communication infrastructure that individuals and societies generally trust and the services provided through it are represented by the Internet Service Providers Association (ISPA) in England. This study examines the data, national strategic documents, cyber security indexes, institutions and organizations for cyber security and other studies

conducted in this field of the leading UN agency, ITU, so as to better understand cyber security in Türkiye and England.

This study is systematically grouped in dimensions developed by various international organizations (ITU Global Cyber Security Index) related to cyber security policies. Cyber security policies of Türkiye and England are compared and examined in five main dimensions. Based on the comparison results, various inferences were made about the cyber security policies of Türkiye and England. In addition, it is not known for certain whether the proposed inferences will yield results due to the security in the cyber space, the implementation of policies against cyber attacks, and the constant change in cyber crimes. Therefore, in the inferences to be made for Türkiye and England, the social, cultural and legal structure of both countries has been tried to be taken into account. This study examines and compares the cyber security policies of the Turkish and British governments in five dimensions in the light of the information given in the GCI. In the light of the data obtained, it can be argued that the findings have very important implications for policy makers, public institutions and private sector leaders.

The main research questions of this study are as follows:

What is meant by cyber security and cyber security policy for Türkiye and England?
What types of institutions are dealing with Cyber Security? What are their duties? How do they work?
What should be the basic elements of an effective cyber security dimensions?
How are the five categories of activities (policy and strategy; culture and society; education, training and skills; legal and regulatory frameworks; standards, organizations and technologies) examined according to the development model?

In the light of these questions, the cyber security policies of Türkiye and England have been comparatively examined through official policy documents and related literature. Through the national and international security dimension of cyber security, the studies of Türkiye and England on cyber security have been examined and detailed. The cyber security policy problems of the two countries are explained, the creation of a new framework is discussed, and the need for classification is emphasized. In addition, this study shows that cyber security policy is diverse and it is important to examine the Global Cybersecurity Index in five dimensions when comparing states.

The first dimension of comparison is policy and strategy. According to this title, it is evaluated what kind of duties fall on which institutions in the decisions to be taken by the government

in cyber security and cyber crimes, and the strategy documents made by the government are examined.

The second dimension of comparison is culture and society. In this title, it examines attitudes, knowledge, assumptions, norms and values of societies regarding cyber security in terms of culture and society.

The third dimension of comparison is education, training and skills. In this title, training activities and training exercises for the Turkish and British governments to ensure cyber security throughout the country are examined. It is important that the Turkish and British governments consider increasing the reliability of government services and online commercial services, and develop a feedback mechanism in order to handle private or personal data, and to ensure trust in e-government and e-commerce services. These measures should go hand in hand with an effort to promote understanding of cyberattack and cyber security and reliability in its services and technologies. In the study, it is emphasized that cyber security education should be expanded in many educational disciplines at all levels (if appropriate conditions are provided), beyond technical and computer science disciplines.

The fourth dimension of comparison is the legal and regulatory framework. The strategic plans and legal regulations put into practice by the Turkish and British governments in cyber security, both politically and legally, are emphasized.

The fifth dimension of comparison is standards, organizations and technologies. In this title, the scientific studies of the Turkish and British governments in cyber security and technological activities developed as a result of these studies are examined. Organization and cooperation studies are analyzed, and standardization studies for both countries' critical infrastructure facilities, emergency institutional and sectoral response teams, national response units and government institutions are also evaluated.

Cyber Security in Türkiye and England

Cyber security does not belong to a state, region or a particular social organization, but concerns every society or person who uses the network or is widely impressed by the network technic. The cyber security domain is concerned with the perceived cyber security threat by a particular subject. The global cyber security field express to the present situations and events interested in cyber that impress the security, steady and progress of countries around the world. The scope of cyber security can be wide or minimal, and threatening to cyber security

vary in severity. Actually, the field of cyber security is a subjective situation and is about discourse analysis. Whole actors in the cyber space have the capability to start attacks. There is no geographical notion in the network ambience (Ünver, 2017: 117). Therefore, attack capacity isn't restricted by geographic space. Threatenings to the network ambiance cannot be resolved rapidly and effectively. It is also unfeasible to effectively implement deterrent policies in the network environment. Cyber security also has some common features such as the unbalance of power structure, lack of institutes and norms, and inadequate reciprocal trust.

The iteration of the 2020 Global Cyber security Index is a scale where each column is weighted by 20 points. In a composite weighted index, every indicator, sub-indicator, and micro-indicator is appointed a weight based on their importance. Weight can have a important effect on eventual points, and different technics can form diverse rankings. Country scores are scale between 0 and 100. The cyber security capacity maturity model of the countries with 100 and close to 100 points is good and close to good.

In the 2020 Global Cybersecurity Index, Türkiye ranks "97.49 points" and "11. ranks" (Global Cybersecurity Index, ITU, 2018: 25). It is seen that England is better than Türkiye in terms of implementing strategies. England is more active than Türkiye in coordinating and implementing cyber security policies. Türkiye focuses on preventing the damage to the technical and organizational structure of cyber incidents. England, on the other hand, focuses on cyberspace to prevent cyber incidents from attacking national critical information infrastructures and key network resources. From a cyber security perspective, Türkiye's priority is public and state security, while England's priority is individual security and human rights. In cyber security, Türkiye encourages public institutions and works on the awareness of increasing their standards. The United States, which ranks first, has a score of 100 according to the 2020 Global Cyber Security Index. The last countries in the survey, Micronesia, Vatican City and Yemen, are in the 182nd place with 0 points.

Table 1: Türkiye and England in the Five Dimensions of the Cyber Security Capacity Maturity Model

Countries	Eventual Points	Legal Measures	Technical Measures	Organizational Measures	Capacity Building Measures	Collaborative Measures
Türkiye	97.5	20	19.54	17.96	20	20
England	99.54	20	19.54	20	20	20

Source: Global Cybersecurity Index, *ITU*, 2020: 127-128; Ünver, 2023: 115, 154-155.

When analyzed regionally, scores and rankings in global cyber security change. Accordingly, Türkiye's cyber security capacity maturity "overall score is 97.5" in Table 1, while its cyber security capacity maturity ranking is 6th among European countries (Global Cybersecurity Index, ITU, 2020: 30). England is ranked 1st with 99.54 points (Global Cybersecurity Index, ITU, 2020: 30). Accordingly, England received full marks (20) from four of the five dimensions, while Türkiye received full marks (20) from three dimensions. According to Table 1, it has been seen that England is more advanced than Türkiye in the cyber security capacity maturity model.

According to Table 1, Türkiye needs some improvements in organizational and technical measures. It is seen that Türkiye is very close to the ideal point, according to the study of the Global Cyber Security Index, as it has a score of twenty or close to twenty in terms of legal measures, cooperative measures and capacity building measures. England needs some improvements in technical measures. It is known to be in the ideal spot as it has twenty points in legal measures, cooperative measures, capacity building measures and organizational measures and nearly twenty in technical measures.

Strategic management is an important aspect of national security. The first step for a comprehensive analysis ought to be the country's cyber security strategy. Providing security in cyber space is an important strategic priority for cyber threats, cyber attacks, cyber wars. The study on the subject has been done at various levels about cyber security in Türkiye. Examples include the "Tunisia Report"[2] (WSIS, 2005) adopted at the World Information Society Summit and the "Ninth Development Plan of Türkiye"[3].

The transformation of Turkish society into an information society is the Ninth Development Plan of Türkiye covering the years 2007-2013. Providing public services in electronic environment brings great convenience to daily life. As a matter of fact, criminal organizations also benefit from information technology (Dokuzuncu Kalkınma Planı (2007- 2013) p. 53, article 323). After the Ninth Development Plan, two sections under the subject of "development axes of the program period" and "increasing the quality and efficiency in public

[2] The Tunisia Report draws attention to the following points; "Information sources and technologies are used for crime. Terrorism uses information technologies effectively." Therefore, misuse of information technologies should be prevented, but human rights should be taken into account while preventing abuse.

[3] In addition to the rule of law, development is defined with a multidimensional understanding that includes concepts such as economic growth, advancement in information and communication technologies, increased international competition, sustainable growth and human development. It is seen that growth and development efforts will continue with a holistic perspective that fits this definition. For detailed information. Dokuzuncu Kalkınma Planı (2007- 2013), Access date is 22.06.2023, [https://www.sbb.gov.tr/kalkinma-planlari/]. Promoting e-government applications is included in Dokuzuncu Kalkınma Plan (p. 51, article 314).

services" are the other steps taken towards cyber security (Official Gazette, Decision 2007/12300; Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Orta Vadeli Program (2012-2014)).

England presented its first national strategy, England Cyber Security Strategy, in 2009: "Security, Security and Resilience in Cyberspace" (Cabinet Office, June 2009). It then created a second strategy, England Cyber Security Strategy for the period 2011-2015: "Protecting and Promoting England in a Digital World" (Cabinet Office, 2011). In this context, the strategy, which points to a change in England's cyber security policy and strategies in 2016, has also created the current framework that indicates England's targets for national cyber security policy.

In the 2011 cyber security strategy document, England aimed to develop cyber security policies related to cybercrime, to be one of the safest countries and to protect the national critical infrastructure (Cabinet Office, *The UK Cyber Security Strategy,* 2011).

In England National Cyber Security Strategy Document covering the years 2016-2021, it aimed to be safer, more resilient, more stable against cyber risks and threats and to protect its interests in the cyber field. There are three broad objectives in the Strategy Document (England 2016-2021, "UK National Cyber Security Strategy"):

- The first is Defense; Defending England against emerging cyber threats
- Secondly, Deterrence: Tracking down and prosecuting criminals. By gaining the ability to understand, detect and investigate cyber attackers, it is to ensure that England is resilient against all kinds of aggression in the cyber space, and thus hold the criminals accountable.
- Third Development: Investments should be made in public/private institutions and organizations for sustainable development and skills protection. It should also encourage cyber security efforts to overcome future threats and challenges.

These comprehensive aims are supportive studies for international activities and cooperation. That's why international activities and partnerships are important to invest in cyberspace that aligns with England's security and economic interests. England's strategy document covering the years 2016-2021 aimed to simplify the approach to cyber security, thus encouraging national and international partnerships (Silfversten (et al.), 2020: 146-147).

Regular scenario and real-time cyber drills on cyber security are held in England. It has a mechanism to implement the national cyber security strategy, especially at the local level. Moreover, there is no mechanism yet to implement it fully. The UK Computer Emergency Response Teams (CERT-UK) maintain a national record of cyber incidents. Furthermore, central responsibility for incident response rests with the National Cyber Security Center (NCSC). It acts as part of the Government Communications Headquarters (GCHQ). It is the authority that monitors all incidents, ensures that they are reported, disseminates information, gives early warnings, makes cyber threat evaluations and ensures technic assistance to authorities. England Cybersecurity Information Sharing Partnership (CiSP), supported by CERT-UK, is still developing in the country and is expected to help support knowledge sharing between public/private institutions and organizations. More mechanisms are needed to build capacity, particularly to help Critical National Infrastructure (CNI) organizations strengthen their security posture and collaborate in the field that can strengthen England national security posture. In this context, it is necessary to give priority to national coordination among all institutions and organizations related to incident response and reporting at the national and international level in England, to create a draft regulation and develop the mechanism (Bada, 2016: 7-8).

Individuals become more conscious of cyber threats. Moreover, there is a difference between individuals' understanding of defense against cyber threats and users' routine practices on the Internet. Most of the users do not use the good applications of the internet very often in their daily life. Although it is known that there are many initiatives that are generally managed by the industry, it is natural to see that they have a limited impact on society as these initiatives do not target all groups of society. In addition, there has been a concern among experts and internet users about how the gap between cyber security concepts can be bridged and how this gap can affect applications. In general, experts have utopian expectations from the ordinary internet user. Institutions and organizations should work in coordination against cyber threats and attacks and increase awareness activities such as the "Cyber Essentials" (NCSC "Cyber Essentials: Requirements for IT Infrastructure": 1-17) program supported by the government and industry. Programmes and necessaries are presented existing to develop cyber security implementations (Bada, 2016: 10-11).

Presenting cyber security approaches as a comparative analysis and analyzing the five main elements over states can lead to a better understanding of cyber security policies. This understanding is given and analyzed in the following five titles in this study.

Policy and Strategy

Strategic plans are evaluated as a road map to reach the targets set in the national strategy. In addition to the strategic plans, official reports containing the subjects that form the basis of these plans are among the tools used by nations to ensure security in the cyber field. In this context, the following documents were published by the State Planning Organization along with the development process of Türkiye's National Cyber Security Strategy Document (Karabacak and Özkan, 2009):

- E-Türkiye Initiative Action Plan (2002),
- E-Transformation Türkiye Project Short-Term Action Plan (2003-2004),
- E-Transformation Türkiye Project 2005 Action Plan, Information Society Strategy (2006-2010),
- Information Society Strategy Action Plan (2006-2010),
- National Cyber Security Strategy and Action Plan (2013-2014),
- National Cyber Security Strategy and Action Plan (2016-2019) and
- National Cyber Security Strategy and Action Plan (2020-2023).

In this period, cyber security education and training were given as activity reports in many workshops, seminars, symposiums and lessons. The Information Society Strategy and Additional Action Plan, approved by the High Planning Council on July 11, 2006, was published in the Official Gazette on July 28, 2006 in its issue numbered 26242 (SPO, 2006-2010).

Cyber security issues have been given importance at the state level in Türkiye for more than twenty years, and official applications and actions have been tried to be initiated until 2003 with the "E-Transformation Turkey Project". The Telecommunication Union was established in Türkiye in 2000 and was transformed into the Information and Communication Technologies Authority (ICTA or BTK in Turkish) in 2008 (Bıçakçı, Ergun and Çelikpala, 2016: 26). Informatics and Information Security Advanced Technologies Research Center (BILGEM-Information Technolohies Institute) was established within TÜBİTAK. Cyber Security Institute (CSI/SGE), which was opened in 2012 within BILGEM, continues its activities today. "National Cyber Security Policy" is another official document. This document was prepared in 2008 with the cooperation of nineteen state institutions and presented to the Prime Ministry in 2009 ("E-dönüşüm Türkiye").

"Cyber Security Strategy Workshop" was made on 16 June 2012 in Ankara with initiatives of the Information Security Association. In this context, the association's members arranged a outline document. Then, the members of the association shared the document with public/private institutions and organizations. This document has been updated in a workshop with upward of eighty IT security proficients. The revised text has been submitted to the Ministry of Transport, Maritime Affairs and Communications. Expressed here is the National Cyber Security Strategy and Action Plan;

- Detailed analysis of the information technology infrastructure of public institutions and organizations in order to ensure the security of all kinds of services, processes and data,
- Improving the security of information systems used by the public or private sector as a result of the analysis,
- Determining the infrastructure that will keep cyber risks and threats at a low level, quickly establishing cyber security response responses in case of threats and ensuring the safe operation of the system,
- It can enable the competent authorities to carry out effective investigations.

The most prominent and important steps regarding cyber security are National Cyber Security Strategy and Action Plan 2013-2014, National Cyber Security Strategy and Action Plan 2016-2019 and National Cyber Security Strategy and Action Plan 2020-2023. The said strategy and action plans; It has been by organizing conferences, seminars, workshops and meetings with experts from corporations and organizations representing public corporations, ICT sector, universities, critical infrastructure operatives and non-governmental organizations. Collaboration and consensus from a range of stakeholders is required to appropriately develop the strategy and action plan. The Tunisia report, the Ninth Development Plan and the Medium Term Program (2012-2014), as an example, shows that the issue of cyber security is considered as an important area both nationally and internationally.

TÜBİTAK designed a project called "Vizyon 2023" to determine new technology and science policies containing the years 2003-2023. In this scope aimed to identify strategic technologies and priority research and development spaces (TÜBİTAK, "National Science and Technology Policies 2003-2023 Strategy Document", 2004).

Cyberspace and England National Security provides an overview of the cyber security issue. Society is becoming more and more dependent on information and communication

technology in every field. With addiction comes vulnerability to exposure and abuse, crime and even attack. Criminals and extremists can take advantage of the same global technological partnerships that society has become so dependent on. Even though cyber security is a system that requires a coordinated, capable and mutually reinforcing response from all who benefit from the global information and communication technology infrastructure, it also brings with it a rapidly evolving and complex security challenge. England, which has given importance cyber policy researches since the 1990s, published England cyber-related foresight program in 1994 to support policy and planning (Schmidt, 2015: 489-511).

England government's foresight work on cyber affairs is carried out by a central government agency that reports directly to the cabinet. England Department of Defense realizes prescience events under the "Development, Concepts and Doctrine Center" and the "Defense Science and Technology Laboratory" (Cabinet Office, 2011; Çiftçi, 2019: 48).

Cyber Trust and Crime Prevention Project was carried out in 2004 under the Ministry of Interior Ministry of Crime Reduction, Policing, Community Security and Anti-Terrorism with the participation of scientists and a total of 260 experts from various sectors. The goal of the project is to conduct research on future technologies, establish cyber trust and create actions to prevent cybercrime (Ünver, 2023: 162).

In the report of Digital Britain (UK Government, 2009) issued by England, it has been stated that the British society needs the services and information provided in the cyber space(United Kingdom Cabinet Office, 2009a). In June 2009, the British government wanted to achieve the goal of "becoming one of the leading digital information economies in the world" and published its first strategy document in this context in the same year. With the national strategy document, the British government wanted to provide cyber security and benefit from the occasions provided by the cyber space (United Kingdom Cabinet Office, 2009a).

While listing the actors that could threaten (unstable countries, transnational organized crime, international conflicts and natural disasters) national security in England strategy document, it also listed the areas that could threaten (public opinion, nuclear weapons, cyber space, culture, knowledge) it (UK Cabinet Office, 2009b). In its 2009 cyber security strategy, the British government highlights four objectives. These purposes are:

- To make England one of the safest countries, to prevent cybercrime and to do business in the cyberspace,

- Being resistant to cyber threats and attacks and protecting the country's interests,
- Creating an open, stable, robust and secure cyberspace for the British public,
- To have the knowledge, skills and capacity to achieve cyber security goals.

England has a comprehensive cyber security strategy. This strategy is finished by a robust cyber security legitimate framework and two CERTs. United Kingdom Computer Emergency Response Teams (CERT-UK) mainly support critical infrastructure operators, whereas GovCertUK supports government institutions. Other concerned institutions add the Cyber Security and Information Assurance Department and the National Security Council. England also has a well-developed public/private partnership system. This co-conspirator approach is also strongly promoted by the cyber security strategy. For example, the Center for the Protection of National Infrastructure (CPNI) provides industry-specific information exchange across the industry ("EU Cybersecurity Dashboard A Path to a Secure European Cyberspace", 2015). The existence of such centers is a reference for countries that want to make progress in the area of cyber security.

The strategy includes a strong statement of principles and an assessment of cyber security threats facing England. The implementation plan included in the strategy is based on the basic set targets. CPNI is tasked with protecting England's critical infrastructure. CPNI's central document is the Strategic Framework and Policy Statement on Increasing the Resilience of Critical Infrastructure to Natural Hazards, adopted in 2010 (Cabinet Office, 2010: 8).

Cyber security policy and strategy in England is crucial to promoting a cybersecurity agenda across government. Because prioritizing cyber security over other key policy areas, it is important to disseminate and fundamentally analyze a state-wide cyber security agenda, as it determines the mandate of key cyber security state actors and resources help address existing cyber security issues as they arise. Some organizations in England have a cyber security responsibility that can be largely structured around three principles (Silfversten (et al.), 2020: 147):

- Developing and implementing policy coordination under the Cabinet Office;
- National security subordinate to the Government Communications Headquarters (GCHQ);
- Cyber defense managed by the Ministry of Intelligence and Defense.

In the 2016-2021 National Cyber Security Strategy, England National Cyber Security Center (NCSC) is specified as the authority with the main cyber security responsibility (England

NCSS (2016-2021)). NCSC is the organization responsible for monitoring and responding to cyber incidents, sharing information and preventing vulnerabilities (Mali, 2016: 5).

There is a review and renewal process for England National Cyber Security Strategy Paper. But this renewal process, is not on an annual basis. The National Cyber Security Center (NCSC) was established in 2017 as part of GCHQ's national authority on cybersecurity. Accordingly, information participating, handling systemic security vulnerabilities and ensuring leadership on national cyber security subjects were among the important elements. The British government in the "UK National Cybersecurity Strategy Document" covering the years 2022-2030 (Cabinet Office, 2022):

- Understanding threats,
- Making and enforcing laws,
- It is stated to be in a unique position to gather the intelligence necessary to counter threats from hostile actors, including setting national standards and conducting offensive cyber operations. The government has emphasized that it will invest in strengthening national cyber capabilities through this strategy.

In England, government departments and public sector organizations are responsible for maintaining their networks and systems. Because the government is the service provider of important data, it takes strict measures to protect information and assets. Additionally, the government has an major liability to recommend and inform citizens, businesses and organizations about what they should do to protect themselves online. Most areas of cyber policy and most of the measures outlined in this strategy relate to issues such as national security, foreign relations and defence, telecommunications, product standards and safety, consumer protection (Cabinet Office, 2022).

Culture and Society

Cyber security culture expresses the attitudes, knowledge, assumptions, norms and values of corporate employees in Turkey regarding cyber security. A good cyber security culture is one in which the organizational determinants of culture (policy, lead, course, social norms, etc.) and the individual determinants of culture (manners, information, assumptions, etc.) are consistent with the organization's approach to cyber security as manifested in cyber security behaviors.

The sum of symbols, habits, rules, artifacts and other social abilities are the characteristics of human culture in Türkiye. In Türkiye, cultural information in cyberspace is coded for sign systems. Thoughts and concepts expressed in these systems are separated from the individual and gain an independent, impersonal existence. Through culture, civilizations can document and create their histories for generations. It has been about the symbolic elements of culture and the way these symbols give socio-historical meanings. Culture in Türkiye refers to various forms of knowledge, beliefs and ethical codes that reinforce a society. Many elements such as positive and negative slogans and actions, expressing thoughts with symbols and shapes, revealing traditional knowledge, religious discourses, rules, partisanship and the like fall into the subject of culture and society.

The United Nations General Assembly in 2003 determined a decision to create a global cyber security culture (UNGA, 2003; UNGA, 2018). Public/private institutions and organizations that use, develop, provide and manage information systems have carried out studies to increase the cyber security culture for users in the application and use of information technologies. The global understanding on cyber security culture reflects the universality of approach, its institutionalism, wide scope of domestic and transnational levels of cyber security.

The activities, programs and projects specified in the cyber security policies subserve a mutual purpose to provide national cyber security. Reaching this, cultural bond, social structure, great harmony and cooperation requires. In particular, international cooperation is needed to protect critical infrastructures against cyber attacks. To give an instance of national collaboration, draft plan against spam e-mail was carried out by ICTA in 2009 with the participation of many public/private institutions. As a result of draft plan, the number of IP addresses forwarding spam mails decreased by 99 percent and the total number of daily spam mails decreased from 6.5 billion to 394 million (Ulaşoğlu (et al.), 2010: 34). In order to establish cyber security in Türkiye, it is necessary to form a national cyber security culture, raise awareness in society about this issue.

Seventy-eight percent of England population in 2013 told they used the internet. Is this percentage of internet users in England an indication that the common internet culture has increased? or Is this percentage due to the diversity of beliefs, attitudes and opinions about the internet among British people? According to 2013 OxIS research survey data, most of the British population gave similar answers to questions about internet attitudes, beliefs and

opinions. In the light of the answers given, he showed that it can be divided into five characteristics or cultures and that each culture can have its own characteristics. These are defined as follows (Ünver, 2023: 170-171; Dutton, 2013: 4):

- E-Mersives; This user group has connect to internet as piece of their daily life and work. They made up just twelve percent of internet users in England.
- Techno-pragmatists; Focusing on using internet to make their lives easier and save time, this group of users, they accounted for around seventeen percent of England users. Compared to e-mersives group, this group does not just use the internet for fun and they do not see internet as a place of escape.
- Cyber savvy (knowledge of computers or the internet; technologically savvy); This group of users stated that they have some ambivalent views, mixed feelings and beliefs about internet. This user group thinks that they will lose control (anxiety of taking away from time and privacy) as opposed to feeling in control. Only nineteen percent of the British population is in this group.
- Cyber moderates; This user group sees internet as a good place to spend time, obtain information and continue social relations. In this context, they display a moderate approach in their attitudes, beliefs and views about internet. They make up thirty-seven percent of the British population.
- A-digital; This user group claims that internet is audited by others, likely beyond their control. This digital culture covers around fourteen percent of England's online population.

Education, Training and Skills

The main indicator that ensures the implementation of strategic plans related to cyber security to certain programs and national projects is Cyber Security Programs. Training programs for education and skills, informative academic events, cyber security exercises, research and development projects, risk management, critical infrastructure preservation programs, workshop meetings are some of the subjects that can be evaluated within this scope.

According to the Information Society Strategy Fifth Action Plan, cyber security trainings were given in Türkiye. Online trainings such as TR-BOME user awareness training, training on CERT installation and function, system analysis, CIRT training were provided. In addition, technical articles on cyber security, information security documents and guidance documents within the scope of standards and organizations are published within the extent of the

National Information Security Gate Project on (https://bilgiguvenligi.org.tr/) website. There are also free programs on information security and experiences on the website (http://www.CEHTurkiye.com), an online bookcase and administered by ethical hackers (Burlu (vd.) Certified Ethical Hacker).

The first CERT exercise, which was held within the scope of cyber security in Türkiye on 20-21 November 2008, started with the participation of eight public institutions. On February 23, 2010, the first security awareness day was organized to increase public awareness of cyber security. On 25-28 January 2011, the second CERT exercise was done under the title of Information Systems Security Exercise. In this context, it was realized with the attendance of forty-one public/private institutions from various sectors such as economy and finance, education, communication, and ensuring internal security. With this exercise, a booklet providing useful information about using information systems safely has been published by the Turkish government.

In Türkiye, conferences and symposiums are held within the scope of cyber security. The International Information Security and Cryptology (ISC) Conference has been going on since 2008. The ISC, which is held annually, held its fifteenth organization on 19-20 October 2022. All of the presentations and articles presented at the conference are issued on the web address (http://www.iscturkey.org) (ISC Turkey). More examples that started in Türkiye were the Public Institutions Information Technologies Security Conference in 2011 (sixth panel), the National Cyber Security Workshop in September, the Cyber Security Conference in December and the Cyber Security Law Workshop in 2012 (Ünver, 2023: 133).

The 2006-2010 Information Society Strategy and Action Plan was published in the Official Gazette dated 28 July 2006. With this action plan, it was mentioned that there is a five-year reference document in the field of cyber security since 2010 and that it should shed light on future studies. “Cyber Security Board” was founded in Türkiye with the decision of the Council of Ministers dated 11 June 2012 in the Official Gazette (Official Gazette, 20.09.2012). It was decided to prepare a national cyber security strategy and action plan with Cyber Security Board. This decision is the most effective step taken in the scope of cyber security. With the relevant document, it is recommended that universities train cyber security experts so as to maintain cyber security.

The 2015-2018 Information Society Strategy and Action Plan was issued in the Official Gazette (Official Gazette, 06. 03.2015). This document, seen as an umbrella, covered the

issues of both the 2016-2019 National Cyber Security Strategy and Action Plan and the 2016-2019 National e-Government Strategy and Action Plan. In the 2015-2018 Action Plan, education, training and skills are mentioned under the sub-title of "Information Security and User Trust". Accordingly;

- To carry out training activities in order to increase qualified human resources and to raise awareness about safe internet use in the society,
- To provide cooperation between institutions and organizations and to provide cyber security trainings,
- It envisaged the rapid determination of minimum standards in the scope of cyber security with the provision of the legal infrastructure.

In 2020-2023 the National Strategy Document and Action Plan, it is stated that a "National Cybercrime Strategy" will be prepared to combat cybercrime. Information regarding the establishment of specialized courts for cybercrimes is included in this Action Plan (Ministry of Justice, 2021). In order to provide cyber security in Türkiye, it is important to establish the legal infrastructure, to establish courts, to train experts in this field and to carry out training activities.

"Cybercrime and Internet Security, Cyberbullying, Social Networks, Cyberspace Awareness, Cyber Attacks, etc." education is given to students at primary and high school level. Many postgraduate programs such as cyber security, cyber field studies, information security have been started in many universities in Türkiye. In these fields, it has been decided by Council of Higher Education (CoHe or YÖK) to grant scholarships to some of the students who will do master's and doctorate in Türkiye, and a commission has been established for this. TÜBİTAK organizes summer camps and inter-university cyber security competitions within the scope of cyber security. Students who are successful in the competitions are given job opportunities at USOM. Research and development studies, master's and doctoral thesis studies are carried out at the national and international level. In addition, products/methods are developed, current publications are made, and workshops/conferences are organized.

In England, various government stakeholders and the private sector are examining the availability and quality of cyber security education, training and skills to raise awareness. The development of cyber security education in England and efforts to raise awareness of education and training in the public and private sectors are important. In the dimension of education, training and skills, England implements high cyber security education and training

in the private sector, public institutions and organizations, schools and universities in order to provide information security and cyber security.

Cyber Champions is a non-profit organization created to promote best practices in digital literacy and online safety awareness to England schools, youth organizations and interest groups. ("Cyber Champions", [https://www.cyberchampions.org/]). The program is supported by networks of Cyber Champions, young professional volunteers, and a growing number of private and public sector organizations that encourage their local communities to make a difference and increase the skills of future generations. England Cybersecurity Challenges create learning and development opportunities that raise awareness of cyber security as a rewarding career and encourage more people to join the profession ("Cybersecurity Challenge UK", [https://cybersecuritychallenge.org.uk/]).

England strategy addresses the skills gap through various levels of education and training, including incorporating cyber security skills into the education system, balancing the gender gap in cyber-related occupations, providing education and training programs for 14-18 year olds, among other initiatives. England Department of Education has invested in promoting computing skills in schools. This will provide a better understanding of the subject area.

Public and private sector education cooperates. It adapts to the ever changing environment because it tries to build on skill sets in both sectors. In addition, the government establishes partnerships with other sectors and funds activities to train law enforcement. There is a difference between education and skills. While there are specialist staff trained in cyber security skills, this staff is too small to adequately meet the needs of British society. As a result, there is currently a perceived skill shortage that highlights the need to combine education and practical training ("Cybersecurity Challenge UK", [https://cybersecuritychallenge.org.uk/]). Therefore, more investment in cyber security and skills development programs is required.

The internet and the digital education and communication built on it are helping to bring great benefits to England and its educational activities. Moreover, both criminal and state-run malicious actors continue to actively exploit vulnerabilities in England's cyber defenses. The risk of intentional or accidental cyber incidents is multiplying in threats due to the increasingly interconnected networks, systems and devices used by organizations and individuals, and the increasing use of digital services.

Organizations, and especially educational organizations, need to take steps to reduce their cyber risks. Although the Cyber Awareness training campaign has been successful in England, it has not yet reached enough institutions and people. The British government needs to do more and increase this reach to understand why advice and guidance is not reaching enough audiences. In its National Strategy Document published in June 2022, England highlighted the importance of strengthening the structures, partnerships and networks necessary to support the cyber society approach (Cabinet Office, 2022).

Legal and Regulatory Frameworks

The Law No. 2012/3842, which was published in the Official Gazette on 20 October 2012 and entered into force, determined the duties to be carried out by the responsible institution affiliated to the Ministry of Transport, Maritime Affairs and Communications regarding the practice, management and coordination of national cyber security activities (Official Gazette, Decision Number 2012/3842). The resolution also creates the National Cyber Security Board.

The "Electronic Communications Law" No. 5809 assigns the Information Technologies and Communication Institute responsibilities including the following items (Official Gazette, "Electronic Communication Law No. 5809"): "To protect the confidentiality of information security and communication", "To provide a counter system against unauthorized access", "to take the measures ordered by legal regulations for the implementation of national security in the service quality and electronic communication sector, public order and services". The duty of taking the necessary measures stipulated by the regulations is carried out by the Turkish National Information Technologies and Communications Authority.

Türkiye does not have specific legislation that addresses cyber threats to critical infrastructure. In this context, special regulations for sectors are encouraged to protect critical infrastructure in various sectors such as fiscal services. Moreover, it is obligatory to use the ISO/IEC 27001 standard for organizations providing infrastructure and energy facilities, electronic networks, and electronic communication services. Furthermore, in the banking sector, the Communiqué requires the use of two-factor authentication process for data protection and requires risk analysis to be carried out by the relevant unit of the bank. In accordance with the legislation, providing cyber security education should also turn into mandatory (Turkish Standards Institute, "ISO/IEC 27001 Personal Data Protection Law & ISO 27701 Personal Data Management System").

The Turkish Penal Code criminalizes accessing or recording phone calls or interfering with and opening private mail (Turkish Penal Code, Protection of Personal Data TCK No. 5237, Articles 135 and 136). While this should cover electronic communication in principle, there are no clear provisions on this subject in the legislation. In addition, it is generally accepted that the privacy of electronic communications is also maintained. This is hoped to be explicitly ensured under the recent cyber security law.

The Legal and Regulatory Frameworks related to cybersecurity in England have been updated to better reflect material law. Based on the recommendations of the Telecommunications Development Bureau Management Advisory Group, in GCI, procedural law is no more measured. Instead greater aperture is stressed in various areas, online harassment, including identity theft, racialism, xenophobia. International experience confirms the important role that legal and regulatory frameworks play in promoting cyber security across industries, while providing prevention, mitigation and conflict mechanisms to individuals and organizations affected by cyber threats. This dimension places a special emphasis on the British government's ICT security issues. It also examines the capacity to design and enact national legislation and accompanying regulations directly and indirectly related to cyber security.

In 1990, the first legal regulation for computer crimes was the Computer Misuse Act, which was enacted by England government. Situations related to many crimes such as computer software, unauthorized access or entry of data, unauthorized access to computer are considered crimes within the scope of this legislation. England Data Protection Act was enacted in 1998. It published its first cyber security strategy document in 2009 by order of the Queen of England. Subsequently, the Cyber Security Office was established.

In 2010, she worked on the review of strategy and defense in the cyber field, which will cover the five-year period. The Cyber Crime Strategy has been published to document these studies. In 2011, England published a new strategy document to keep up with the digitalizing age and move the kingdom to this cyberspace. With the Defense Strategy Document, it was planned to work in the military field and it was aimed to establish two main centers. These centers are the Security Control Center for Global Operations and the Cyber Operations Working Group. Then, England published the progress report on the objectives given in the cyber security strategy document in 2012, the National Cyber Security Strategy Paper in 2013 (future plans and achievements), and the National Cyber Security Strategy Paper (progress and

development plans) in 2014. In 2015, England published the study "Government Policy from 2010 to 2015: Cyber Security".

The Crown Prosecution Service (CPS) developed the 2013-2014 CPS security and information risk management policy. This policy aims to integrate information risk management into existing business and project risk as much as possible. Certain threats are managed through an ISO 27001 assurance program ("Audit and Risk Committee Minutes", 11.2020).

The National Crime Agency (NCA) continues to lead and coordinate England's fight against cybercrime, working closely with various local and international cyber security partners (NCA, 2017). Comprehensive ICT security has been implemented in England. In this regard, legislation on rights in the digital field has been adopted, and steps have been taken to protect the British people, public/private institutions and organizations. There are distinct legal initiatives regarding cybercrime.

Improvements in cyber risk management have been achieved through advice and guidance from the National Cyber Security Center and implementation of the General Data Protection Regulation, the Network and Information Systems Regulation 2018 and the Data Protection Act 2018. With the Covid-19 outbreak, the use and dependence of digital services used to meet basic corporate needs such as information storage, shared communication and security in England has increased across the entire economy and society. This has brought significant benefits to England. But it has also increased the scope of cyber risks to organizations and the broader economy.

ICT security legislation, with significant limitations in comparison, is advanced as universal ICT security legal and regulatory frameworks addressing cyber security have been performed and legislation has been adopted in England protecting the rights of individuals and organizations in the digital medium. For Türkiye, this legislation can be used with some revisions on a micro scale and if it is brought to a sustainable structure, it will bring important inclusiveness towards human rights and freedoms. A detailed section exists within the criminal justice system to struggle computer related crime on human rights. In this regard, work continues with international organizations on confidentiality and data preservation, and draft legislation is updated. In England, it has ratified international treaties such as the Human Rights Act and other treaties to adopt appropriate legislation to combat crimes against confidentiality and data preservation, facilitating their detection, inquiry and proceedings

(Bada, 2016: 44-45). In this regard, Türkiye needs to be able to follow legal agreements in accordance with the general structure regarding the relevant legislation.

Cyber security threats are not limited to damaging computer systems. Threats can also damage a country's computer systems, communications and communications systems, and critical infrastructure systems such as energy, transportation, military command and control. Cyber threats can emerge as a type of asymmetric warfare. For this reason, the idea that cyber threats are one of the important threats has begun to be accepted by world leaders. Therefore, it can be said that the approaches of nations to cyber security are far ahead of information security. The concept of cyber security has been defined by ITU as a set of measures to be taken against cyber attacks. Countries should produce and develop tools, policies and practices especially to protect the assets and values of the private sector, institutions, organizations and individuals (ITU-T Recommendation, 2018: 8-12).

Standards, Organizations and Technologies

Since Türkiye is a member of the International Organization for Standardization (ISO), the requirements specified in the ISO/IEC 27001 standard in the field of data security should be complied with. ISO/IEC 27001 is a mutual standard that is also valid and obligatory in Turkish law for organizations providing electronic networks, infrastructure and energy facilities and electronic communication services (Turkish Standards Institute, ISO/IEC 27001). Since Türkiye is a member of ISO, it is necessary to comply with the conditions specified in the ISO/IEC 27001 standard in the field of data security.

The government has published various strategies and development plans to ensure cybersecurity and improve information technology in terms of standards, organizations and technologies in many sectors. Due to the increasing trend towards digitalization in Turkey, Turkish public/private institutions and organizations have started to use digital platforms to ensure confidentiality, integrity and accessibility. The electronic apostille services supplied by the Post, Telegraph and Telephone Institution can be one of the most new instances in this context ("Elektronik Apostil Sistemi", 2018).

The Turkish government encourages public institutions to improve cyber security and works to increase cyber security standards and awareness. In this direction, under the leadership of the Presidency of Defense Industries, "Türkiye Siber Güvenlik Kümelenmesi" was

established with the additive of all public/private institutions and organizations, academia to develop the Turkish cyber security ecosystem ("Türkiye Siber Güvenlik Kümelenmesi").

TÜBİTAK was the institution responsible for cyber security in Türkiye until 2012. The Ministry of Transport, Maritime Affairs and Communications became the responsible authority, published in the Official Gazette of the Council of Ministers Decision No 2012/3842 on 20 October 2012. The decision also consists of the memberships of the Ministries of Foreign Affairs and Foreign Affairs, as well as the National Cyber Security Council, Ministry of Interior and Defense, National Intelligence Organization, General Staff, Public Order and the Telecommunications and Communications Commission, Security, Financial Crimes Investigation Board, TÜBİTAK, ICTA and other undersecretaries and senior managers deemed necessary by the Ministry.

There are two accredited CERTs as the State-run Türkiye Computer Incidents Response Team Coordination Center (TR-BOME), and the Computer Security Incident Response Team (ULAK-CSIRT) owned by TÜBİTAK, which is operated for research and education purposes (Official Gazette, 20.10.2012). TR-BOME also operates in the international arena (TR-BOME KM (Ed. Mehmet Eriş): 118). TR-BOME represented Türkiye in the "International Cyber Defense Workshop, Fall 09- ICDW09" exercise and the 2009 NATO Cyber Coalition Exercise. CERT coordination center in Türkiye, established within the scope of National Information Systems Security Programs, helps private/public institutions and organizations acquire the ability to reply to computer events in the scope of security.

Cyber Shield Exercises were organized by ICTA in 2012, 2013, 2014, 2019 and 2022 so as to develop international cooperation, improve response capabilities against cyber attacks, inter-agency and international cooperation, increase the capacity in the field of cyber security, to improve internal, ensure coordination and raise awareness on this issue.

In general, more strategies, plans and projects need to be prepared for the cyber security ecosystem in Türkiye, especially in the public and banking sectors, than in critical private sectors such as telecommunications, energy and health. In addition, Turkish public authorities dealing with cyber security issues need to be very open to receiving feedback from market players and involving them in shaping new regulations. In this area, it is important to contact regulatory authorities as soon as possible during the transaction process, communicate their needs to them, and supply feedback on proposed regulations. Türkiye's commitment encompasses all the driving forces involved in Türkiye's desire, determination and real steps

to achieve its cyber security vision. It is stated in the action plan that cyber threats can adversely affect all sectors including communication, transportation, energy, banking, finance and health. For this reason, it is important to speed up the measures to combat the increasing threats in cyberspace.

ICT development and use can be successful in a security environment. Therefore, countries are required to establish and establish accepted minimum security criteria and accreditation schemes for software applications and systems. These efforts need to be complemented by the implementation of a national body dealing with cyber incidents, a competent government agency, and a national framework for monitoring, alerting and responding to incidents.

In England, the focal point and official reports are a key indicator of analyzing whether the country has established the organizational structures necessary for national cyber security. The determination of a single central authority to be responsible for national cyber security is one of the important issues for England. England should regulate all its efforts and activities in institutions and organizations with cyber security duties such as strategies, standards, critical infrastructures, accreditation, control, agreement, protection and defence.

Within the scope of this study, the examples of Türkiye and England were analyzed in depth based on five predetermined dimensions. In this analysis, political and strategic approaches to cyber security were taken into account. The two states in question have tried to create an effective cyber defense and attack capacity in order to develop their political, economic and military capacities within the scope of network technologies in the short and medium term. It has been observed that the official cyber security strategy documents and doctrines, which started to take shape with the beginning of the 2000s, benefit from the globalizing, commercializing and civilianizing internet technology. In this way, the legal infrastructure and activities of the national cyber security institutions that control the national cyber security areas have been examined and evaluated.

Conclusion and Contributions

Strategy documents related to cyber security in Türkiye have given importance to protect the confidentiality, integrity and accessibility of the information systems that constitute the cyberspace. It also focuses on cyber security on detecting attacks and response mechanisms against them and taking precautions.

Decisions taken as a result of the meetings held on national cyber security strategies in Türkiye are shared on the official website of NCS. As a result of a meeting held on October 27, 2010, the issue of cyber security was mentioned for the first time. In this meeting, cyber threat and its global dimension were examined and the effects of this threat on national security were discussed.

AFAD in Türkiye touched upon cyber threats and damage to critical infrastructure as a human-made technological disaster. According to AFAD, critical infrastructure; It is the whole of assets, systems, networks and structures that will have significant impacts on the safety, economy and health of users as a result of the social order, environment and public services being adversely affected when they are not able to fulfill their duties, either limited or completely. National Cyber Security Strategy Document, Information Security Management in Critical Infrastructure Project was included in the Ministry of Development Investment Program in 2012. There is no legal arrangement on the preservation of critical infrastructures against peripheral threats and dangers such as earthquakes, floods, epidemics (AFAD, 2014). In this context, the task of establishing CERT and CIRT in the Fourth Action Plan of the National Cyber Security Strategy was given to the institutions under the responsibility of NCSC.

Cyber security in England includes the creation of a broader and more comprehensive cyber security policy to protect interests and take advantage of the many opportunities in the cyberspace.

In England, critical infrastructure is defined as assets, systems and services that deeply affect political, economic and social life. Critical infrastructure is classified in nine sectors; Emergency Services, Communications, Transportation, Health, Energy, Financial Services, Utilities, Food and Water (CPNI, 2020). Protection of critical infrastructures rests with the England Home Office. There are also mandate agencies coordinated by the CPNI to provide expert support and contribution. England Computer Security Incident Response Team (CSIRT-UK) has been set up by CPNI to respond to cyber security threats, manage incidents and provide advice. In the National Cyber Security Strategy Document, the responsibilities of the state, public institutions and organizations and the private sector are clearly stated (United Kingdom Cabinet Office, 2009a; Ünver, 2023: 193-194).

In England, activities have been developed in relation to the cyber security strategy on education and skills, capacity building and awareness raising. Cyber security strategies are

included in the curriculum especially in intercollegiate cooperation studies, military institutions, research centers, primary and high school equivalent schools, and awareness-oriented trainings are aimed. In this scope, the British government has given importance to providing resource support and increasing the budget allocated in this area.

England has chosen the approach of examining threats, risks and security vulnerabilities in detail in achieving its goals, with the knowledge, capacity and capability to underpin its security goals (United Kingdom Cabinet Office, 2011). In this scope, three research institutes; England Cybersecurity Science Research Institute, the Reliable Industrial Control Systems Research Institute, the Automated Program Analysis and Verification Research Institute were established with funding from the British government (CPNI, 2020).

Table 2: Comparative Analysis of Türkiye and England Cyber Security Policies

Comparison Criteria	**Türkiye**	**England**
Preparation and implementation of national strategy documents	Yes	Yes
Providing cyber security trainings and strengthening training programs	Yes	Yes
Conducting cyber security exercises	Yes	Yes
User awareness	No	Yes
Ensuring international cooperation and public-private partnership	Yes	Yes
Giving cyber security awareness trainings to private sector and public institutions-organizations	Yes	Yes
Protection of critical infrastructure and national crisis management	Yes	Yes
Establishment of Computer Emergency Response Teams (CERT) Establishment of Computer Incident Response Teams (CIRT)	Yes	Yes
A sensitive network of military, intelligence and other government agencies involved in cyber policy and activities that deal with both international and national security	Yes	Yes
Domestic and foreign policy coordination	Yes	Yes
Legal gaps in information security	Yes	Yes
It focuses more on technical and organizational measures.	Yes	No
It focuses more on cyber space as the prevention of cyber attacks.	No	Yes
The priority of this country is the safety of the public and the state.	Yes	No
The priority of this country is the security of the individual and human rights.	No	Yes
Fighting cybercrime	Yes	Yes
This country gives priority to monitoring national risk assessment	No	Yes

approaches.		
It takes into account existing policies, legal framework and cyber security capabilities.	Yes	Yes
Balancing security and privacy	Yes	Yes
Ensuring the physical security of cyber networks and communication systems	Yes	Yes

Source: Ünver, 2023: 195-196.

Across countries, critical infrastructures are located in both the private and public sectors. For this reason, it is beneficial for both parties to produce top-level strategies for maximum cooperation. The Cyber Security Strategy Documents agree that the government cannot take on cyber security responsibilities alone and should be a joint effort of all stakeholders.

Table 2 above summarizes the strategic objectives of both countries. Although common themes cover a variety of objectives, each strategy has its own specific objectives. For example, Türkiye's strategy aims to help individuals understand the risks associated with their use of technology and be able to use it safely to meet future challenges related to inclusive changes in the digitization of Turkish society. The basis of the national strategy in England is education and international cooperation to promote the economy, citizens and national values. Türkiye's strategy is to ensure that critical infrastructures are resistant to cyber attacks. Türkiye's strategy aims to promote and raise awareness of cyber security. Türkiye's cyber security principles are efficiency, resilience and foresight. England's principles are broad and some focus on protection, accountability and cooperation.

The problems created by cybercrime are global and require the cooperation of stakeholders at both the national and international levels. This can be achieved through different means, such as international forums, bilateral and multilateral agreements, and public-private partnerships among others. In addition, Türkiye and England have similar strengths in promoting international cooperation, public-private partnerships, capacity building, research and development among other countries. Having a sensitive network of military, intelligence and other government agencies involved in cyber policy and activities that deal with both international and national security is another important factor in ensuring cyber security. International cooperation; The global internet is sustainable with the right balance between freedom, security, openness and robustness. Türkiye and England have openly expressed their current or future action plans to promote global cooperation. Strong inter-ministerial

collaboration is vital, as government opinions play an important role in countries' cyber security. A good way to demonstrate the connectivity of government ministries is to design an organizational structure.

Türkiye's cyber-network has faced several unique risks, such as increased local cybercrime levels, widespread dependence on Western software, and unequal legal regimes and sanctions. On the national security front, both states are evolving in how best to design and adapt new technical possibilities to support their national security interests in cyberspace. In addition, there is a lack of protection for privacy and data in the micro-scale internet environment. There are legal loopholes in public information security. The current information security emphasis of countries is not enough. Its institutions and legal system are lacking. Information security strategies and plans are insufficient. Internet technologies need to be further developed. More international cooperation is needed. Security of cyberspace is a widespread, international issue. Moreover, since there are differences between countries, it is not possible for every country to do everything in the same way. Every country has its own problems regarding internet security. Since the issue of cyber security is very sensitive, the discussions so far are not comprehensive enough. It is important to be able to determine the basic principles and rules and to establish the mechanism that will work thanks to international cooperation. Topics to focus on may include cyber security, privacy and data protection.

One of the findings obtained in this article is that Turkey and England prioritize and develop their strategies according to their needs. The other is that public/private institutions and organizations have not fully grasped the necessity of planning their cyber security strategies. In this context, studies on the cyber security policies of countries are required. When cyber security policies of Türkiye and England are examined comparatively;

- The purpose, basic principles, mission, vision and strategic targets could not be determined in Türkiye when compared with England,
- The functions of individuals, public/private institutions and organizations in the planning and implementation of cyber security strategies are not fully explained,
- Compared to England, cyber security strategies and action plans in Türkiye are not made within the required time limit (exceeding the time required for implementation),
- Insufficient existing laws in the fight against cybercrime in Türkiye compared to England,

- While the military and judicial personnel of the trainings on combating cybercrime are given in detail in England, it is limited in Türkiye,
- When compared to England, public-private sector cooperation is not given enough importance in Türkiye,
- The issues related to education and awareness raising were not in Türkiye in the early 2000s, but they became popular especially in the post-2020 period by focusing on these issues,
- It is important to set product development standards for software and hardware in Türkiye and England,
- There is no budgeting to realize strategic planning in Türkiye, but England has made and is making a certain budgeting for strategic planning.
- Reports showing the in-depth progress of strategic documents have not been published in the period from the date of NCSC preparation in Türkiye until 2020. A more comprehensive reporting is made with the 2020-2023 National Cyber Security Strategy Document.

There is a need to explore the reasons behind trends in cyber security in international politics and to anticipate scenarios of international discourse on global cyber security culture. In this context, according to the 2020 Global Cyber Security Index, England ranks 2nd among the countries participating in the survey with 99.54 points (ITU, 2020: 25). When the survey studies at the regional level are examined, England ranks first with the same score this time (ITU, 2020:30). Türkiye is in the 6th place in the regional ranking. Her overall score is 97.50. While England got full points from four of the five dimensions included in the evaluation in this survey study, Türkiye was able to get full points from only three of these five dimensions. Here, England is in a more advanced position in the cyber security capacity maturity model compared to Türkiye.

It is seen that Türkiye and England focus on various aspects within their cyber security policy actions. In the light of the information given based on the information given in Table 2; Policies implemented in Türkiye and England support a more flexible approach and emphasize the economic and individual dimensions of cyber security policy. In this context, cyber security in these two countries can be characterized as civilian-oriented. In terms of standards, organizations and technologies, England is more active in coordinating and implementing cyber security policies.

Türkiye and England also have cognitive differences in the field of cyber security policies. While the British government defines cyber security from a "threat" perspective, the Turkish government tends to define it from a "development" perspective. Threat approach states it from the perspective "others". The development approach, on the other hand, tends to focus on the need of society to increase the development of cyberspace and ensure its own national stability. Thus, social-political stability is accepted as Türkiye's main national interest. The difference between Türkiye's cyber security demands and its actual capacity to provide cyber security causes Türkiye to take a defensive stance against cyber security.

The study will guide countries that plan to prepare or update a national cyber security strategy. This study has made comparative analyzes for academic purposes and can serve as a stepping stone to close gaps in cyber security policies. When it comes to developing, implementing and updating policy action plans, it has been observed that England is better than Türkiye in terms of implementing strategies. Even after taking a defensive approach to its security strategy, it has managed to use its abilities very well. Both countries have the expertise to ensure their assets are protected against aggressive threats. Therefore, they are successfully trying to ensure that their resources are better protected from volatile, uncertain, complex and vulnerable cyber threats in this new cyber world compared to other countries.

When designing and developing a National Cyber Security Strategy Document, countries should identify gaps in the national framework; should develop lines of action to overcome gaps in policy, regulation, legislation, the roles and responsibilities of stakeholders. All these may differ from country to country.

In the legislation and regulations, it is seen that cyber security is taken more seriously in England, unlike Türkiye, and the suitability of laws and processes are reviewed. In addition, key factors critical to the success of a strategy, such as the implementation plan, assessment plan, resource allocation, risk management, and annual strategy assessment, were found to be either incomplete or under-stated. England has made reference to using the General Data Protection Regulation to guide cyber security standards in its strategy.

An overview of national cyber security strategies in Türkiye reveals that the cyber security strategy has become integrated and comprehensive. Strategies approach cyber security with a collective approach and cover the economic, social, legal, political, strategic and organizational aspects of cyber security.

It is stated that England focuses on various aspects within its cyber security policy actions. In this context, it is seen that England has put forward an advanced vision in the cyber field.

In general, this study examined the main features of cyber security policy through its description in the literature and analysis of policy documents. The study shows that cyber security policy is diverse and it is important to examine the Global Cyber Security Index in the light of five main dimensions when comparing states. The concept of security, which is examined theoretically, is reflected to the present day through the historically developing state and details it with examples from the field of cyber security as a sub-branch. Recognition of the diversity of government action (strategy s issued by governments and activities in this regard) provides a solid basis for the development of strategic options that can then lead to an overall strategy. An overall strategy for cyber security policy should establish clear relationships in how the various goals are argued against each other and clearly define the goal that the state fulfills in its various roles. Although the results look different in each country, the tension areas in the cyber security policy remain the same.

Some supporting questions were included in *Introduction* of the study. It has been tried to find answers to these questions in the text. Considering the originality and original value of the study, especially the evaluations in which the approaches of the two countries are compared gain importance. It is an informative study about the current situation and possible cyber security moves that countries with two different development levels can make in the future. In this respect, it has a guiding quality.

The Council of Europe Convention on Cybercrime of 23 November 2001, which basically sheds light on global cooperation, provides the opportunity to use the most appropriate legal standard for different national laws. On 29 December 2020, Türkiye and England signed a Free Trade Agreement (Ticaret Bakanlığı, 10.03.2022). The Turkish and British governments have agreed to liberalize trade. It will be beneficial for both countries to work together in defense, industrial sector and especially in high value-added technology projects such as warplanes and unmanned aerial vehicles.

In the light of the data obtained, the following can be said: The results of this study, presenting cyber security approaches as a comparative analysis and analyzing them on five main elements will lead to a better understanding of cyber security. It will contribute to explaining the barriers to cooperation between states dealing with cyber security issues at the international level.

References

"2010 to 2015 Government Policy: Cyber Security", [https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security].

AFAD (2014). *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi,* Ankara: T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı.

"Audit and Risk Committee Minutes" (11.2020), [https://www.cps.gov.uk/publication/minutes-cps-audit-and-risk-committee/arc-minutes-october-2020].

Burlu, Kâmil (et al.) Certified Ethical Hacker, [http://www.CEHTurkiye.com].

Cabinet Office (2010). *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, [http://www.cabinetoffice.gov.uk/].

Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, [https://www.gov.uk/government/].

Cabinet Office (2022). *Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022-2030.*

"Computer Misuse Act 1990", [https://www.legislation.gov.uk/ukpga/1990/18/contents].

CPNI (2020). "Center for the Protection of National Infrastructure".

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, *Orta Vadeli Program (2012- 2014),* [https://www.sbb.gov.tr/wp-content/uploads/2018/11/Orta_Vadeli_Program2012-2014.pdf].

"Cyber Champions", [https://www.cyberchampions.org/].

"Cybersecurity Challenge UK", [https://cybersecuritychallenge.org.uk/].

Çiftçi, Hasan (2019). *Technology Foresight and Modeling: Turkish Cybersecurity Foresight 2040*, PhD Thesis, Ankara: METU.

"Data Protection Act 1998", [https://www.legislation.gov.uk/ukpga/1998/29/contents].

Dokuzuncu Kalkınma Planı (2007- 2013). [https://www.sbb.gov.tr/kalkinma-planlari/].

"E-dönüşüm Türkiye", [http://www.bilgitoplumu.gov.tr/bilgi-toplumu/e-donusum-projesi/].

"Elektronik Apostil Sistemi" (2018). [https://www.ptt.gov.tr/Sayfalar/Kurumsal/DuyuruDetay.aspx?DetayId=26]

England (2016-2021). "UK National Cyber Security Strategy".

Erik Silfversten (vd.) (2020). "Cybersecurity A State-of-the-art Review: Phase 2", *Final Report,* UK: RAND Europe.

"EU Cybersecurity Dashboard A Path to a Secure European Cyberspace" (2015), [https://cybersecurity.bsa.org/].

International Telecommunication Union (2008). "Series X: Data Networks, Open System Communications and Security, Overview of Cybersecurity", *ITU-T Recommendation*, 10 (1).

ISC Turkey, [http://iscturkey.org/].

ITU (2018). *Global Cybersecurity Index*.

ITU (2020). *Global Cybersecurity Index*.

Karabacak, Bilge ve Sevgi Özkan (2009). "Critical Infrastructure Protection Status and Action Items of Turkey", *International Conference on E-Government Sharing Experiences*, [https://fuse.franklin.edu/facstaff-pub/40/].

Mali, Prashant (2016). "Critical Analysis of National Cyber Security Policies of UK, India, USA&Germany", Chevening Fellowship in Cybersecurity Project, pp. 1-19.

Maria Bada (ed.) (2016). *Cybersecurity Capacity Review of the United Kingdom*, Oxford: Oxford University.

National Crime Agency (NCA), (2017). *Annual Report and Accounts 2016–17*, London: OGL, [https://assets.publishing.service.gov.uk/].

NCSC (04.2021). "Cyber Essentials: Requirements for IT Infrastructure", UK: Cyber Essentials, pp. 1-17.

Official Gazette, "5809 Sayılı Elektronik Haberleşme Kanunu", [https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm].

Official Gazette (20.10.2012). "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Decision No. 2012/3842, issue 28447, [https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm].

Official Gazette, Decision 2007/12300, [https://resmigazete.gov.tr/eskiler/2007/06/20070621-2.htm].

Official Gazette (6 Mart 2015). "2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı", Decision No 2015/4.

Salih Bıçakçı, D. Ergun ve M. Çelikpala (2016). "Türkiye'de Siber Güvenlik", (ed. Sinan Ülgen), *Türkiye'de Siber Güvenlik ve Nükleer Enerji*, İstanbul: EDAM.

Schmidt, John Michael (2015). "Policy, Planning, Intelligence and Foresight in Government Organizations", *Foresight*, 17(5), pp. 489-511.

SPO Information Society Strategy Action Plan (2006-2010). *Assessment Report*, No 5, Ankara.

T.C. Adalet Bakanlığı (Nisan 2021). *İnsan Hakları Eylem Planı Uygulama Takvimi*, s. 54, 60, 104, 106.

TR-BOME KM (Türkiye Bilgisayar Olayları Müdahale Ekibi- Koordinasyon Merkezi), (Ed. Mehmet Eriş) [http://ulakbim.tubitak.gov.tr] (er. tar. 15.06.2022); H. Şentürk vd. (2012). "Cyber Security…", s. 118.

Turkish Standards Institute, "ISO/IEC 27001 Personal Data Protection Law & ISO 27701 Personal Data Management System", [https://tse.org.tr/IcerikDetay?ID=2311&ParentID=9423].

TÜBİTAK (2004). "National Science and Technology Policies 2003-2023 Strategy Document".

"Türkiye Siber Güvenlik Kümelenmesi", [https://www.siberkume.org.tr/Index].

Turkish Penal Code, Protection of Personal Data TCK No. 5237, Articles 135 and 136, [https://www.kisiselverilerinkorunmasi.org/mevzuat/5237-sayili-turk-ceza-kanunu/].

Ulaşanoğlu, Emin (vd.) (2010). "Bilgi güvenliği: Riskler ve Öneriler", *Bilgi Teknolojileri ve İletişim Kurumu*.

UNGA (2003). "Creation of a Global Culture of Cybersecurity", [https://digitallibrary.un.org/record/482184].

UNGA (2018). "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", [https://undocs.org/A/C.1/73/L.37].

United Kingdom Cabinet Office (2009a). *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber space*, London: United Kingdom Government.

United Kingdom Cabinet Office (2009b). *The National Security Strategy of the United Kingdom: Update 2009, Security for the Next Generation*, London: United Kingdom Government.

United Kingdom Cabinet Office (2011). *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London: United Kingdom Government.

Ünver Gül Nazik, (2017). "Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları", *Cyberpolitik Journal 2 (4)*, pp. 104-129.

Ünver, Gül Nazik (2018). "Siber Çatışmaların Tanımlanma Sorunu", *Cyberpolitik Journal*, 3 (5), 23-44.

Ünver, Gül Nazik (2023). *Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği*, PhD Thesis, Konya: Selcuk University.

WSIS (2005). *Report of the Tunis phase of the World Summit on the Information Society* (WSIS), Tunis: WSIS.

Yılmaz, Sacit (2011). "5237 Sayılı Türk Ceza Kanunu'nun 244. Maddesi'nde Düzenlenen Bilişim Alanındaki Suçlar", *TBB Dergisi*, Sayı 92, ss. 62-100.

A HUMAN RIGHTS-BASED DIGITAL CITIZENSHIP EDUCATION: ETHICS FOR CYBER PEACE

Nezir AKYEŞİLMEN[*]

ORCID: 0000-0001-8184-5280

Abstract

The objective of this essay is to to propose a human rights-based model for digital citizenship education. Digitalization offers great opportunities to human beings but also poses significant risks and threats. Therefore, acquiring new competences, knowledge, and concepts are essential for utilizing cyber tools accurately, efficiently, and ensuring protection against potential threats. There have been studies on the subject but those focusing on human rights approach of DCE are a few. Thus this work tries to contribute in filling up this gap. Literature review is the primary research tool for the study. The article puts forward that global society has developed different measures for ensuring security at different levels in digital age. For instance global cyber governance and international law at the global level, national cybersecurity strategies at the national level and implementation of digital citizenship education (DCE) programs at the indvidual level are measures so far devloped. It concludes that a human rights-based DCE is inferred from human rights and ethical principles and seeks to promote safety, responsibility, and ethical behaviors in digital domain.

Introduction

Digital citizenship education, envisions effectively managing the opportunities and threats presented by cyberspace, which have emerged with the spread of cyber technology, and acting responsibly in the digital world. DCE is, indeed, a kind of peace education and human rights education. It is a peace education since it promotes peaceful coexistence in the digital realm, where individuals refrain from causing harm to one another. It is also a human rights education since it empowers individuals and safeguard their human dignity by considering their freedom and rights online. [♠]

[*] Prof. Dr., Department of International Relations, Selçuk University- Konya – Türkiye. E-mail: nezmen@yahoo.com

[♠] The early version f of this study was submitted to "5th İstanbul Bosphorus International Conference Oncybersecurity, Cyberpolitics And Social Sciences", 10-12, 2021, istanbul, https://drive.google.com/file/d/19UQ2t0U-9IR-q9SgU0XZjUx66Pjm9xsh/view [Access date: 06.01.2024]. and Turkish version with some changes was published in Akyeşilmen, Nezir. (2018). *Siber politika ve Siber Güvenlik.*Ankara: Orion.

In this work, after defining digital citizenship (DE), the stakeholders, challenges, and functions and characteristics of DCE will be evaluated. Then, the "Ethics phor Peace" model, a human rights-based approach, will be emphasized.

Exploring Digital Citizenship

If you ask someone, "Are you a digital citizen?", many people will say no without thinking. However, when they consider activities such as the time spent on the phone and computer, online communication, email, research, media monitoring, banking transactions, online shopping, and paying bills, they will realize that they are actually digital citizens (Dorothy, 2016:10). In this case, everyone who is active in the digital environment becomes a digital citizen in some way. However, citizenship legally requires a special status, rights, and responsibilities. Developing a globally binding legal regulation in cyberspace, especially rules binding individuals, other than a set of technical rules and codes, is contrary to the nature, anarchic structure, and spirit of international law. Despite this, in this study, an attempt will be made to define digital citizenship based on traditional citizenship, and suggestions will be developed to ensure security measures in cyber peace, taking into account its uniqueness.

Today, most of citizen in the developed world uses the internet and carries out most of their daily activities and transactions through cyber technology tools. Traditional knowledge and skills are not sufficient to use cyberspace effectively. The digital age requires specific digital education and skills. According to Rahm and Fejes, a digital society exists worldwide today. The digital society has transcended the boundaries of ethnicity, religion, gender, philosophy, and traditional citizenship. Digital society is global by definition and nature (Rahm and Fejes, 2017:22). In this global digital society, it is vital that sensitive issues such as risks, threats, security, and privacy are understood and kept at a manageable level. Even though measures such as encryption, digital identity, antivirus programs, parental control, and firewalls technically provide relative security, the only way to ensure real security in cyberspace is to ensure ethical behavior online. It is important for computer ethics to become widespread because data, information, and computer systems and networks are always open to internal, external, and global threats. Governments, decision-makers, professionals, public and private institutions and organizations, experts, and citizens should feel responsible in this context and strive to contribute to it (Gnarto, 2011:1).

Digital Citizenship: Navigating the Digital Landscape Responsibly

Multiple definitions of digital citizenship can be found in the literature. Although certain factors may be shared among various definitions, it is also conceivable to come across distinct elements. One of the primary factor is the active involvement or engagement with the digital realm, which refers to the utilization of digital technologies. Another prevalent aspect involves having a thorough understanding of your rights and responsibilities while engaging in the digital world. Another crucial aspect is the competences and abilities in utilizing digital tools. Lastly, there is belonging to a society. Here, it refers to being a member of global digital community. Nevertheless, nearly all of these notions necessitate a clear definition and the establishment of their limits. Can we discuss the concept of a digital society, for instance? Does society consist just of the people, or is it a framework characterized by a shared culture, history, traditions, and norms?

Optus defines dijital citizenship as "the knowledge, attitudes, and skills required to maximize the benefits of digital tools and minimize their threats to oneself and others." If citizenship means being part of society, digital citizenship means being part of a digital society (Optus, 2017:12). The elements exist in this definition, are digital skills, belonging to a society, and, albeit indirectly, protection. Richardson and Milodiv, however, place greater emphasis on active participation in online democracy in their definitions. They define digital citizenship as "the capacity to apply a set of skills deemed necessary for effective participation in the culture of online democracy" (Richardson and Milovidov, 2017:11). In parallel, MiraMedia also emphasized active participation and responsibilities in its definition. It is the willingness of citizens to participate actively and democratically in the digital society. This participation also includes the appropriate, responsible, and respectful use of technology (MiraMedia, 2017:9). According to Frau-Meigs et al., digital citizenship refers to "lifelong learning processes (formal, informal); at all levels (political, economic, social, cultural, and intercultural); to society (local, national, global); active and responsible participation (value, ability, knowledge, and critical understanding of behavior) and the ability to use digital technologies adequately and positively to protect human rights and dignity (establishing, working, sharing, socializing, researching, playing, communicating, and learning)" (Frau-Meigs et al., 2017:11-12).

Tamayo also pointed out the responsible and ethical behavior of citizens in the digital society and defined digital citizenship as follows: "Digital citizens recognize and value the opportunities, responsibilities, and rights to work and learn for everyone in the interconnected

digital world and get involved in this world legally, safely, and ethically." (Tamayo, 2016:3). Tamayo expands on his definition and claims: Digital citizenship is the principles of responsible and appropriate use of technology and can be divided into eight strategic areas. These are ethics, communication, literacy, business, law, access, security, rights, and responsibilities. Digital citizenship is not something that can only be taught in the curriculum. It is the process of continuously preparing young people for a technology-based society (Tamayo, 2016:5).

Sometimes I wonder if we, as academics, are going too far. We are going crazy trying to define cyber citizenship. Sometimes the picture becomes so complicated that after a point we cannot even understand what we have written. Why?

Despite all the complex definitions we have made above, while discussing these issues with my daughter Elif, who has just finished secondary school, I asked her how she would define digital citizenship. She said, "I think everyone who uses the internet is a digital citizen." Then, as if mocking all the academic definitions we have made, "Will digital citizens also be given IDs?" she asked. The truth is that Elif's definition, although partially incomplete, is more comprehensive and realistic than most of the above definitions. Therefore, the working definition to be used in this work will be Elif's definition, which I also agree.

Components of Digital Citizenship

Dorothy identifies three fundamental components of digital citizenship: belonging, participation, and protection. Digital citizens belong to the digital society. They develop relations with society by using technology and try to preserve the benefits provided by the digital world (Dorothy, 2016:11). Digital citizenship is essentially interactive and participatory. Digital citizens not only consume digital assets and content but also produce content, applications, software, and tools (Dorothy, 2016:11-12). Citizenship, by definition, requires protection by the state to which it relates. Protection and security are also people's rights when online. Digital access not only exposes citizens to some digital risks but also improves their digital skills, literacy, and security capabilities. Active users also become resilient users. For this reason, decision-makers, educators, and families should develop special strategies so that they do not limit children's participation and access rights while trying to protect them (Dorothy, 2016:12-13).

Alberta tries to explain digital citizenship with the concept of traditional citizenship and determines several rules within this framework. According to him, the basis of digital citizenship lies in the nature of citizenship. Citizenship is the state of being a citizen of a defined social, political, and national society and entails certain rights and responsibilities. Some of these rights and responsibilities are as follows: a. Citizenship requires acquiring moral principles. In order for society to maintain a healthy and harmonious existence, every citizen must respect the rights of others. Since digital citizens are considered to be members of the global digital society, it is essential that people comply with moral principles when online for this society to exist and function properly. b. Citizenship requires a balance between the empowerment of individuals and their responsibilities to society. In other words, the benefit of the individual and the benefit of society should be balanced. In the digital world, individuals can cause great harm to the digital society, which is independent of time and place, and to other individuals, with unpredictable consequences. Therefore, individuals must be careful in their behavior. c. Citizenship requires participation. Active participation of citizens is essential for society to develop and gain meaning. Likewise, digital citizenship requires active participation. Although the digital world by its nature requires active participation, some digital skills and knowledge are still needed for active participation. d. Citizenship requires education. Acquiring high moral values in social relations does not occur automatically. Guidance, and training from elders (teachers) are needed. Likewise, education in the digital field is much more necessary and more difficult due to its abstract nature. e. Because citizenship is constantly evolving, it requires constant communication and discussion. As social relations constantly change, social communication and behavioral codes also change. This situation is faster and more complex in the digital world. Therefore, preparing citizens for this complex world is a social duty. f. Citizenship should be inclusive. Just as traditional citizenship requires evaluating all citizens equally and fairly, digital citizenship should be accepted to include all people, without any discrimination. Because there are no borders and distances there. Cultures, beliefs, and local values cannot be grounds for discrimination. Otherwise, everyone will be harmed. g. Citizenship is closely related to the development of media. Social communication and relations are both affected by and influenced by the media. Since the digital world actually consists almost entirely of media (social media, tools, space), the development of cyberspace technology will directly affect digital citizenship. h. Citizenship is related to society (Alberta, 2012:8-9).

Netsafe defines a digital citizen as someone who possesses adequate knowledge and competences in information and communication technologies, demonstrates ethical and responsible behavior in their use of technology, and upholds principles of privacy and freedom of expression. Netsafe (2010:3) outlines the attributes of a digital citizen as follows:

- Uses ICT effectively.
- Participates in the economy using technology to engage in cultural and educational activities.
- Develops and uses critical thinking abilities in cyberspace.
- Knows texts, symbols, and languages related to digital technologies.
- Is aware of ICT-related threats and knows how to manage them effectively.
- Uses ICT to relate to others in positive and meaningful ways.
- Acts sincerely, holistically, and ethically when using ICT.
- Respects privacy and freedom of expression in the digital world.
- Contributes to digital citizenship values and actively defends them (Netsafe, 2010:3).

Comparing traditional citizenship, which is based on shared norms and values established through legal, historical, and cultural means, with digital citizenship is challenging due to the absence of common standards and values in the latter, except for a set of technological regulations and protocols. However, it is possible to develop strategies for establishing or protecting digital citizenship by drawing upon traditional concepts of citizenship. Global citizenship education is the only method for creating a digital society and digital citizenship that conform to common principles and standards, and for fostering a sense of belonging and protection. Therefore, it is crucial for the progress of the digital society and humanity that all stake holders including regional and global international organizations, states, decision-makers, non-governmental organizations, families, and experts give priority to digital citizenship education and acknowledge their responsibilities and rights in promoting it.

Digital Citizenship Education: Ethics and Conduct in the Digital World

The education system of most countries aims to raise responsible citizens who contribute to the development, identity, and integrity of society. UNESCO aims to provide citizenship education by educating people from a young age and equipping them with the necessary ideas and knowledge to participate in decisions about society. This education has three main purposes: a) to educate citizens about citizenship and human rights so that they understand

social institutions and rules; b) to learn to use critical thinking and judgment; and c) to achieve individual and social responsibilities (UNESCO, 2017:18).

Although digital citizenship education is a less complex issue compared to digital citizenship, its importance and application are not yet fully understood worldwide. Digital citizenship and education are nourished by two different disciplines in terms of both their conceptual and theoretical development. They both carry a common logic and a common ideal; to secure freedom, prosperity, and a dignified life for all. For this reason, these two concepts have begun to be frequently emphasized together in the international cyberspace literature in recent years.

If we are to establish a working definition for digital citizenship education, it can be described as the process of acquiring necessary competences and abilities to use technology aeffectively, safely, ethically and positively. This concept, highlighted in the digital citizenship definitions discussed earlier, involves being aware of one's rights and responsibilities in the digital world, acting accordingly, and always upholding human rights and dignity. Digital citizenship education is a universal, inclusive, and lifelong learning process encompassing formal and informal education for everyone, regardless of whether they are of school age or not, who uses cyberspace.

Education is emphasized in nearly all National Cyber Security Strategy Documents to protect cyberspace and make it a safe domain. Although not explicitly named as cyber citizenship training, these documents acknowledge the need for training at all levels to raise societal awareness, ensure cyber security, develop necessary skills and abilities, and meet the need for social expertise. For instance, the US Department of Homeland Security Cyber Security Strategy Document highlights public awareness and training as key objectives for achieving cyber security goals (US Homeland Strategy, 2015:24-25). The UK Cyber Security Strategy Document (2016-2021) includes education under many headings and emphasizes the importance of integrating cyber security education into the entire UK education system, from primary school to master's degree (UK, 2016:57).

Turkey's 2016-2019 National Cyber Security Strategy Document emphasizes educating all stakeholders (Turkey, 2016:11) and "creating cyber security awareness in all segments of society" (Turkey, 2016:13). Similarly, the Trinidad and Togo National Cyber Security

Strategy Document outlines five priority areas, including governance, incident response, collaboration, legislation, and raising awareness and training on cybersecurity throughout the country (Trinidad, 2012:4). The Finnish Cyber Security Strategy Document also highlights the importance of education, stating that cyber security education should be included at every stage of the Finnish education system to develop society's needed skills (Finland, 2013:31).

Although digital citizenship education is largely seen as specific to school-age children (from kindergarten to high school), preschool children and adults also need this education. Following Elif's definition, digital citizenship education should encompass everyone present in the digital world. This is because digital citizenship education, like human rights and peace education, is needed by all generations throughout their lives. The famous philosopher Ludwig Wittgenstein's statement, "The limits of my language mean the limits of my world," aptly illustrates the necessity of learning the language, rules, and codes of the newly formed digital world to properly understand and benefit from it (Dorothy, 2016:57). This involves using technology adequately and positively, ensuring active and responsible participation at all societal levels, protecting human dignity, and promoting lifelong learning (CoE, 2016).

Commonsense defines the concept of digital literacy, often used synonymously with digital education, as "the ability to use technology adequately, to understand and interpret digital content and assets, and to create, research, and communicate with appropriate tools" (Commonsense, 2009:1). Strategies for digital citizenship education include:

- Redesigning every school and every formal and informal educational activity to include digital literacy and citizenship.
- Delivering publications containing ethical standards of behavior to educators, families, and students on digital platforms.
- Training and empowering teachers to teach digital literacy and citizenship.
- Educating and empowering families in the use of technology and digital media (Commonsense, 2009:4).

Navigating the Digital World: The Importance of Digital Citizenship Education

Digital citizenship education is crucial for ensuring a peaceful cyberspace and for the global technological revolution to contribute to humanity's welfare and happiness. This type of education creates awareness and knowledge among people, protecting them from their own

mistakes and shielding others from malicious behavior. Without education, everyone is vulnerable in the inherently global cyberspace. The current situation clearly demonstrates the necessity of such education.

The GoogPlay Project developed by Harvard University highlights several reasons for the need for EDC. Firstly, young people often act on the internet with only their interests in mind, leading to unwanted sharing, illegal activities, file downloads, and cyberbullying. Second, young people are less likely to act ethically in cyberspace due to a sense of anonymity (Alberta, 2012:10). Other reasons include the newness and dynamism of cyberspace, which encompasses powerful media and technologies, thus requiring new and comprehensive skills, knowledge, and codes of conduct for responsible and ethical use. The instantaneous and fast nature of many relationships and communications in this field means that cause-effect and action-effect rules may not fully apply. The sense of anonymity and invisibility in the virtual world, along with the absence of immediate reactions to actions taken, can sometimes lead individuals towards immoral and even illegal behaviors (Optus, 2017:14; Commonsense, 2009:1; Purdue, 2018). For instance, a study in Australia found that 40% of children have seen friends behave badly online (Optus, 2017:19). Similarly, a study in Japan listed illegal information found on the Internet, including fake and fraudulent information, violation of privacy, false rumors, sexually explicit content, slander, civil rights violations, gambling, drug information, sexual knowledge, and violence. Cyber citizenship education provides skills such as avoiding risks, thinking before acting, protecting privacy, leaving a positive digital footprint, communicating with mutual respect, conducting effective research, evaluating website credibility, avoiding plagiarism, and respecting copyrights (Dema-Mar Union, 2016).

United Nations Reports recognize internet access as a human right (UN, 2011). However, while approximately 5.5 billion people use the internet worldwide (internetlivestats.com, 2018), the global population is around eight billion (worldometers.info, 2023). This means that 2.5 billion people worldwide either lack access to the internet or choose not to use it for various reasons. This disparity, known as the “digital gap” or “digital divide” (Optus, 2017:28), is a significant issue, particularly in developing or underdeveloped societies. Closing this gap requires a global community effort.

The Principles of Digital Citizenship Education

Digital citizenship education should have a significant impact on societal transformation. Transformative digital citizenship education should be globally implemented to ensure cyber safety, stability, and sustainability, similar to UNESCO's Principles of Peace Cooperation and Human Rights Education (1974). These principles were adopted to prevent the repetition of global destruction caused by two world wars. This education should adhere to UNESCO's principles of inclusivity and comprehensiveness, which embrace various aspects such as development education, multicultural education, disarmament education, human rights education, peace education, and values education (UNESCO, 1974).

The books "Computer Ethics and Expert Relations" (1993) and "Principles of Computer Ethics" both highlight comparable ethical guidelines. The principles encompassed in this list involve promoting the well-being of individuals and society, refraining from causing harm to others, displaying genuineness and dependability, treating others fairly and without prejudice, upholding the rights to intellectual property such as patents and copyrights, recognizing the importance of copyrights, respecting the privacy of others, and giving priority to maintaining confidentiality (Vesna and Niveditha, 2012:2). Alberta proposes that digital citizenship education should enhance awareness in nine distinct domains:

- Digital Access: Electronic participation.
- Digital Commerce: Online shopping.
- Digital Communication: Electronic information sharing.
- Digital Literacy: Education and training related to technology use.
- Digital Ethics: Standards for online relationships.
- Digital Law: Responsibility for actions and electronic use.
- Digital Security: Electronic protection measures.
- Digital Health: Physical and psychological health in the digital world.
- Digital Rights and Responsibilities: Freedoms in the digital world. (Alberta, 2012:1)

The European Council has identified 10 specific digital domains that should be prioritized when operating online. These domains have been categorized into three distinct clusters.

Being Online:

- Access and inclusion.
- Learning and creativity.
- Media and Information literacy.

Well-being online:

- Ethics and empathy.
- Health and well-being

- E-presence and Communication.

Rights online:

- Active participation.
- Rights and responsibilities.
- Privacy and security.
- Consumer awareness (Coe, 2017:11).

The implementation of digital citizenship education should be carried out using a multi-stakeholder method, similar to the approach used in traditional education. It is the shared responsibility of all individuals and organizations involved in education, such as students, teachers, school administrators, parent-teacher associations, education policymakers at local and national levels, universities, education NGOs, and digital education communities, to prioritize security measures and encourage ethical, legal, and positive conduct (Rainbow, 2017:3-4).

A comprehensive Digital Citizenship Education (DCE) should incorporate the application of human rights principles and ethical rules in cyber domain. Acquiring this type of education would help protect cyberspace and its various elements, such as people, information, logical framework, and physical infrastructure (Akyeşilmen, 2018:55).

A Human Rights-Based Approach to DCE: Ethics Phor Peace Model

An education that is inclusive, pluralistic, respects differences, enables active participation in social and political life, and aims for a democratic and prosperous society is possible with the presence of individuals who are aware of their fundamental rights and freedoms and internalize them, and who regard the rights of others as sacred as their own. A human rights-based education can be a significant tool for nurturing active, participatory citizens and generations who understand their freedoms. According to the European Human Rights Education Systems report, rights-based education ensures equality, participation, and inclusion, as well as preventing and resolving conflicts. In summary, rights-based education is deemed the most effective tool for building a society where everyone's rights are respected, protected, and ensured (OSCE, Council of Europe, UNHCHR, and UNESCO, 2008:7).

While international human rights documents prohibit discrimination and exclusion in education, they support the creation of an environment that is inclusive, pluralistic, participatory, and conducive to the full development of the human personality. Countries that

are parties to international human rights treaties are obliged to implement the universal, scientific, and human-oriented education model defined in these instruments, in accordance with international human rights law. As stated in Article 26 of the Universal Declaration of Human Rights (UDHR) "Education should be aimed at the full development of the human personality and strengthening respect for human rights and fundamental freedoms." Similarly, the Council of Europe Charter on Education for Democratic Citizenship and Human Rights (2010) states that education plays a central role in promoting human rights, democracy, and the rule of law, which is the Council's main aim. One of tthe most important steps to achieve this is DCE. Digital citizenship education, if based on a human rights-based approach, then can contribute to peace and security in cyberspace.

There are various education systems in the world, some discriminatory and some inclusive, each with different characteristics. Naturally, while some adhere to international human rights standards, others may involve human rights violations. There are different methods for measuring and evaluating whether an education system is rights-based. However, one of the rare methods that evaluates both democratic participation and transparency as well as human rights dimensions such as freedom, non-discrimination, and equality in a digital citizenship education model can be the ***Ethics for Peace Model***. Consisting of components such as Equality, Time, Health, Information, Critical thinking, Security, Participation, Human Rights, Opportunity, Responsibility, Privacy, Empowerment, Accountability, Creativity, and Empathy, the Ethics for Peace model includes human rights-based elements in measuring and evaluating a digital citizenship education. Ethics phor peace model also implies that the only way for a true cybersecurity, a peaceful, stable, sustainable cyberspace is ethics. That means if digita citizens are aware of ethical principles online and internalize them they will not harm the others. Therefore, a true DCE needs to teach learners human rights and ethical principes.

Elisabeth Bachman and Bernard Trafford base democratic, participatory, and transparent education on several moral and political foundations. Morally, they emphasize the principle of equality, "all people are born equal and free in terms of their dignity and rights," as stated in the first article of the ECHR, while politically, they argue that democratic values must be taught and practiced from an early age for democracy to be established and sustained in a country. It is believed that citizens who understand the importance of participation and democracy from a young age will value active participation and decision-making in later years.

Each of these concepts has overlapping but sometimes conflicting meanings for everyone. But what do each of these components mean in the digital world and within the framework of digital education? Alberta, Commonsense, and the Council of Europe have developed different domains, formulas, and compositions within the framework of the features that digital citizenship education should have. Within the scope of this study, the features that DCE should have were combined in the ***Ethics for Peace*** formula. A DCE paradigm that encompasses all components of the ***ethics Phor Peace*** model will help to ensure a safe, stable and sustanable cyberspace.

Equality: A crucial feature of rights-based education is that it does not exclude or discriminate against anyone. Human rights regulations emphasize that no one can be discriminated against in their enjoyment of civil, political, social, economic, and cultural rights. While the first article of the UDHR focuses on equality, the second article prohibits all forms of discrimination: "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without discrimination" (UDHR, 2). Education should function to eliminate discrimination against women, children, disabled people, ethnic, cultural, or religious minorities, and other vulnerable groups. Particularly the UDHR, the Convention on Combating All Forms of Racial Discrimination, the Convention on Combating All Forms of Discrimination against Women, and the Convention on the Rights of the Child prohibit discrimination on any basis.

Non-discrimination in education means ensuring that everyone has equal access to education and that no one is subjected to discriminatory treatment during the education process. All children should have the equal right to education, and no one should be deprived of this right due to financial or other difficulties. The principle of equality means not only that the state and administrators treat everyone equally, but this principle must also be followed in our private relations with others. The principle of equality and non-discrimination entails not only having these rights but also recognizing that others have the same rights (OSCE, Council of Europe, UNHCHR, and UNESCO, 2008, 227). An ideal DCE or a rights-based DCE should teach that all users in the cyber world are equal and free, and that they have certain rights and responsibilities when using cyber technology. As the first article of the Universal Declaration of Human Rights (UDHR) states, "All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a

spirit of brotherhood." A person who adopts and internalizes this understanding will not easily think of harming anyone or victimizing people in cyberspace, on social and on other online platforms.

Time: Time is another significant factor in the context of digital citizenship education. It can denote both velocity and assessment. It can save time for digital citizens in the context of acquiring certain technological skills and abilities and using cyber technologies effectively. Citizens can follow fast-changing cyber technologies more easily. Conversely, cyberspace can serve as a platform for entertainment, business, study, and various other purposes. Cyber tools, similar to other instruments, has a neutral nature. If individuals utilize them for good, they give positive results; if they use them for evil, they yield negative outcomes. While cyber tools can be used for research and development, education and progress, they can also be used to produce malware, entertainment only, and to waste time. Therefore, making good use of time in cyberspace, allocating as much time as needed for games and entertainment, and dedicating other time for useful work should be the basic strategy. The DCE should have the capacity to cultivate this well-rounded comprehension among internet users.

Health: Engaging in digital technology activities may have adverse effects on both users physical and emotional well-being. Safeguarding users physical health can be accomplished by the adoption of ergonomically appropriate practices and the enforcement of regulations on the utilization of electronic devices, such as mobile phones, computers, and other digital gadgets. However, excessive exposure to ideological, tense, and horror materials can threaten people's psychological health. Thus DCE needs to directs us to use cyber tools correctly and be selective in contents that does not jeopardize our well-being.

Information: DCE should convey to digital citizens that cyberspace is fundamentally an information and communication technology whose main purpose is information sharing and transparency.The Internet represents a significant paradigm shift in the history of global information dissemination. On a daily basis, the internet alone generates an average of about 10 billion gigabytes of information. Considering the entire digital space, it could be double or triple that amount. The cyber world, as an information platform, is an important tool for personal, social and economic development. Therefore, the idea that citizens can use it beneficially should be one of the main aims and features of DCE.

Critical Thinking: Users are exposed to a huge amount of information in the digital world. Tons of different information on every subject is produced and put on the market. It is necessary to have critical thinking in order to realize which of the information produced and presented to the user may be useful and which may be accurate and ethical. Various competencies are necessary in the realm of digital technology, however, critical thinking stands out as one of the utmost essential. Individuals lacking critical thinking skills will have challenges in both accessing valuable knowledge and safeguarding their mental and psychological well-being. Consequently, a digital citizenship education that incorporates instruction in critical thinking will contribute to the development of well-adjusted citizens in the digital world.

Security: Cyber security has become one of the most fundamental agenda items since the 2000s. People have serious security concerns due to increasing cyber attacks, the great and devastating damage caused to society by attacks on critical infrastructures, efforts by governments and cyber security companies to secure cyberspace, and the unpredictable consequences of cybercrimes. What makes cyberspace unsafe is the people themselves. As has been emphasized many times, the weakest link in cybersecurity is the user. Therefore, to avoid becoming a security problem for oneself and others, DCE should provide users with a good understanding of cyber security. Cybersecurity awareness and culture of cybersecurity need to be provided for the lerners in order to protect them from the harms of the digital world. Since both cybersecurity awareness and culture of cybersecurity feed positive security understanding that balances security and freedoms online. Otherwise, just focus on security and prioritizing prevention of negativity in digital realsm prevails negative security which indeed, might have negative impacts on online freedoms and rights. Thus prevailing positive security approach needs to be priority of DCE in general. If the understanding of ECHR Article 3 "Everyone has the right to life, liberty, and security of person" is well integrated with other goals and features of DCE, a significant portion of the learners will become more ethical digital citizens.

Privacy: Privacy is a fundamental human right. Article 12 of the UDHR explains private life and its elements as follows: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” It is vital to teach the importance of private life in terms of individual and human dignity and that

violating it is a legal and constitutional crime. Many actors can violate someone else's right to privacy even for different purposes. To raise awareness and perception to prevent such violations, DCE needs to be disseminated and included in all school curricula. The fact that cyber security is a whole at all levels, that every actors security is interconnected, and that cyber peace is only possible with moral and peaceful use of cyberspace should be disseminated and included among the most basic features of DCE.

Human Rights: In the globalized and digitalized world, actors violating human rights have increased. Traditionally, only states could violate human rights, but today it is understood that non-state actors commit violations quite easily. If the traditional approach is maintained, which is still largely dominant in international human rights law, it will be very difficult to protect human rights in the near future. Because cyberspace is under the domination of non-state actors and states do not have the power or authority to change this reality. Then, to protect all human rights, especially the right to privacy, freedom of expression, and the rights of association and assembly, which are most affected by cyber activities, new international agreements are needed to ensure that non-state actors are held accountable for violations. To ensure cyber security, it is essential for all citizens to know their human rights well, to accept that other citizens have the same rights, and to internalize that their rights are as sacred and valuable as their own. In such a framework, there will be the opportunity to make a serious contribution to cyber security. Therefore, DCE should adopt a rights-based approach that centers on human rights and freedoms at every stage.

DCE is designed to protect human rights, well-being, security, and dignity (UDHR, 1948, preamble), ensuring that people have freedom of expression, freedom of religion and conscience, the right to participate, a fair trial, the right to association and assembly, and the right to food, clothing, shelter, health, and safety, as well as paid holidays. Education aims to protect and develop all the rights and freedoms specified in international human rights instruments, as expressed in the Council of Europe Charter on Education for Democratic Citizenship and Human Rights.

According to human rights instruments, education should be designed to ensure the protection and development of fundamental rights and freedoms and democratic values that enable the full development of the human person. In this context, the aim of DCE policy should be to create an environment for citizens to develop their individual, intellectual, and professional

capacities. Education legislation should be limited to a technical regulation. If a value is to be ascribed, these value(s) must be universal, scientific, human-centered, and include human rights and freedoms.

Opportunity: Cyberspace is a noteworthy tool for individual and social development. Access to the internet, which is the basis and backbone of cyberspace, offers a great opportunity in this sense. There is a serious inequality of opportunity between those who have access to the internet and those who do not. While 5,5 billion people in the world have access to the internet today, 2,5 billion people lack this opportunity and are thus disadvantaged. UN bodies, which define access to the Internet as a human right, actually impose a great responsibility on UN members in this sense. This is our responsibility to provide this opportunity to the 2,5 billion people who do not have internet access. The international community, especially the UN, must fulfill this responsibility as soon as possible. All citizens should be given the understanding that access to the Internet is the right of everyone and that ensuring it is the responsibility of the international community. If this understanding prevails, citizens of the developed world can be a serious driving force in ensuring global internet access by putting pressure on decision-makers. The people in develping countries can be provided with the internet through staellites for instance. Although technically this is not impossible, governments of underdeveloped countries may not desire this due to political and sovereign limitations. While access to the internet empowers citizens, it increases the ability to monitor governments. This is one of the things that non-democratic regimes do not want most. Citizens of the free world must be made aware to change this unfortunate situation and serve to undermine dictatorship on a global scale.

Responsibility: Digital citizens should be aware of their responsibilities in every action they take in this area for a safe cyberspace. Due to its anonymity and global nature, people can behave more irresponsibly in cyberspace. However, it should be well understood that everyone navigates the cyberspace with a digital identity (such as an IP address). Apart from measures such as TOR and VPN, everyone should know that their every move need to be compatible with moral constrains. While cyberspace, like physical life, provides us with some rights, it also imposes some responsibilities on us. There is no infinite freedom there, just like there is not in physical life. It is vital for everyone to act responsibly for a peaceful cyberspace.

***Participation*:** Participation is evident in every aspect of life, with the type and level varying across sectors. What does participation mean, and how is it achieved? Specifically, what does participation entail in the realm of education? Who should be involved, and how can this be practically realized?

Creating a conceptual framework for participation is challenging. However, in the context of education, we can formulate a specific definition based on theoretical assumptions and human rights instruments. Like other social science concepts, participation conveys different meanings and encompasses various processes. In education, participation as an inclusive concept envisions the involvement of all education stakeholders at each stage of the process (Jennifer-Morgan, 2006, pp. 340-348). Similarly, participation in the digital world refers to our democratic and responsible engagement on digital platforms. Active participation also fosters the development of our cyber competences.

In education, particularly in DCE, participation implies open dialogue channels between families, students, teachers, and administrators, where all parties collaboratively engage in educational processes and decision-making (Aref, 2010, p. 1). The World Bank defines participation as "the process by which stakeholders influence and control developments, decisions, and resources related to themselves" (Atanasio, 2002). To enhance education quality and meet international standards, participation has become increasingly crucial in international literature, regulations, and practices (Jennifer-Morgan, 2006, pp. 340-346).

Participation is a vital indicator of democracy and an essential part of education. Numerous structural, legal, and socio-cultural barriers limit the participation of parents, students, and teachers in shaping and directing educational processes. This challenge is compounded in societies with lower levels of democratic culture and development. This may be due to the lack of cultural acceptance of democratic participation, structural disincentives, economic barriers, and the varying significance stakeholders attach to education. Moreover, inadequate analysis of the changing socio-cultural dimensions of education, misunderstandings in decision-making processes, and lack of information are major obstacles to participation (Aref, 2010, pp. 1-2). In this context, digital participation primarily involves acquiring and utilizing digital skills within the framework of safe cyber principles.

Empowerment: Education is a multidimensional process that empowers individuals to shape their own destinies (Aref, 2010, p. 1). For this, access to information, economic resources, and decision-making mechanisms is necessary (Girvan, 1993, p. 3). Digital citizenship education is a process that enables individuals to control their destinies. Empowerment in education should extend beyond material benefits to include competent use of cyber tools.

Empowerment also entails liberating individuals to think critically, express freely, and develop fully, free from indoctrination. Such education fosters free and active citizens. An education that fails to nurture personal, mental, intellectual, and professional growth cannot strengthen individuals or contribute to a democratic society. Empowering education liberates individuals from coercion, oppression, ideology, and indoctrination. Pluralism is essential for a democratic society. The European Court of Human Rights in the Catan and Others vs. Moldova and Russia case (2012) highlighted the need to protect educational pluralism to safeguard a "democratic society" envisioned in the Convention. Therefore, states must ensure that their curricula are objective, critical, and pluralistic, avoiding indoctrination that conflicts with families' religious and philosophical beliefs. Thus, DCE indeed, need to equip learners with competences that empower them in digital realm.

Accountability and Transparency: The digital world is founded on transparency, but accountability is more complex. Ensuring accountability in cyberspace is challenging due to anonymity, global reach, and technological intricacy. As technology advances, accountability mechanisms will improve, but current challenges remain significant. DCE can promote responsibility and transparency by holding individuals accountable for these values. True accountability relies on transparent processes, encompassing goals, evaluations, rules, resources, and rewards. While these criteria remain relevant, recent studies emphasize capacity development and public accountability (Perie, 2007, pp. 2-4).

Accountability and transparency are crucial for a democratic structure. In DCE, they facilitate the participation and empowerment of educational stakeholders. Accountability curtails rulers' power (Diamond, 1996, p. 117), while strengthening citizens. Participation and transparency underscore a system's democratic nature (Lijphart, 1996, p. 165). Effective transparency and accountability require good governance.

Creativity: The development of cyber competences and the freedom and security in cyberspace will also foster originality and creativity. Minds that are not free cannot think freely or develop original ideas.DCEDC should teach citizens to think critically, view issues from multiple perspectives, and express themselves without feeling pressured or causing harm. This will enable the creation of original, creative products.

Empathy: Integrating all components of the DCE expressed in Ethics Phor Peace model will naturally cultivate empathy. An individual who is egalitarian, authentic, responsible, security-conscious, and guided by human rights in cyberspace will naturally develop empathy, valuing all digital citizens. In this context, they will be mindful of not causing harm.

Conclusion

Digital citizenship education is crucial for creating a safe, stable and sustainable cyberspace for everyone. Often, people are technically and morally unprepared in cyberspace. A rights-based education that adheres to peace standards can significantly enhance these capabilities. International organizations, particularly the Council of Europe, are actively contributing in this area. The International Telecommunications Union (ITU) recommends building the value base of the information society on principles derived from internationally accepted conventions, agreements, and declarations. They emphasize equal, fair, and open access to knowledge and information, regardless of the technical means used for storage and transmission. Technological, financial, and regulatory aspects must align with these principles. Transparent and accountable governance, ethical business and accounting practices, and ethical media practices in the communications sector are crucial. Ethical rules and standards, along with mechanisms for monitoring their implementation and sanctions for violations, are imperative. Respect for differences should be central to establishing principles and mechanisms for resolving conflicts in information societies. Such societies can contribute to world peace if built on values like cooperation, equality, honesty, respect, and solidarity (ITU, 2003).

Richardson and Milovidov (2017, pp. 4045) suggest integrating digital citizenship into formal education by defining its concepts and expectations, determining the administrative and legal responsibilities of families, students, teachers, and school management, integrating families into the digital citizenship education process, appointing a digital policies officer in each

school, preparing comprehensive lesson plans, establishing a robust control mechanism, and emphasizing research.

UNESCO (2016:. 6-7) recommends developing a balanced approach towards ICT, providing all children with basic ICT capabilities, going beyond basic skills, developing appropriate technical infrastructure for young children's education, including digital citizenship in teacher qualification standards, allocating resources for improving ICT security systems, establishing mechanisms to evaluate and monitor national digital citizenship, developing locally appropriate programs and projects, and adopting a multi-stakeholder and multi-sectoral approach.

In conclusion, a Digital citizenship education that includes Ethics for Peace components and is based on a human rights-based approach is necessary to protect and develop cyberspace as a beneficial area for the entire human family. This education should encompass all digital citizens, including out-of-school children, adults, and the elderly. As expressed by the Council of Europe DCE understanding, a holistic approach should be adopted to include all stakeholders and sectors (CoE, 2019).

Resources

- Akyeşilmen, N.(2018).*Siber Politika ve Siber Güvenlik.*Ankara:Orion.
- Alberta.(2012).*Digital Citizenship Policy Development Guide*.Boulevard: Alberta Education. https://education.alberta.ca/media/3227621/digital-citizenship-policy-development-guide.pdf [Erişim tarihi: 02.08.2016].
- CDE.(2014). *Empowering Learning A Blueprint for California Education Technology 2014–2017*. https://www.cde.ca.gov/eo/in/documents/yr14bp0418.pdf [Erişim tarihi: 02.08.2016].
- CoE.(2016).*Digital Citizenship Education(DCE):10 Domains*. https://rm.coe.int/10-domains-dce/168077668e([Erişim tarihi: 03.08.2016].
- CoE.(2017).Digital Citizenship Education: Working Conference. https://rm.coe.int/digital-citizenship-education-working-conference-empowering-digital-ci/1680745545 ([Erişim tarihi: 03.08.2016].

- Del-Mar Union(2916).Creating a Culture of Digital Citizenship. https://www.dmusd.org/cms/lib02/CA01001898/Centricity/Domain/64/Common%20Sense%20Education%20Del%20Mar%20Presentation.pdf [Erişim tarihi: 03.08.2016].
- Dorothy, C.(2016).*Growing Digital Citizens.*Brussels: Central Support Service for eTwinning. https://www.etwinning.net/eun-files/book2016/eTwinningBook_2016.pdf [Erişim tarihi: 02.08.2016].
- Finlandiya.(2013).*Finland's Cyber Security Strategy*. www.yhteiskunnanturvallisuus.fi/en [Erişim tarihi: 07.07.2018].
- Frau-Meigs, D. ve Diğerleri.(2017). Digital Citizenship Education: Overview and New Perspectives.file:///C:/Users/Dell/Documents/cyber_security_human_rights/book_cyber/digitalo.pdf[Erişim tarihi: 03.08.2016].
- Gunarto, H.(2011).Ethical Issues in Cyberspace and IT Society.https://www.apu.ac.jp/~gunarto/it1.pdf [Erişim tarihi: 01.08.2018].
- Internetlivestats.com.(2018).internetlvestats. http://www.internetlivestats.com/ [Erişim tarihi: 04.08.2018].
- ITU.(2003). Civil Society Declaration to the World Summit on the Information Society. https://www.itu.int/net/wsis/docs/geneva/civil-society-declaration.pdf [Erişim tarihi: 19.08.2018].
- Miramedia.(2017).*Intercultural Dgştal Citizenship in the Community*. http://www.miramedia.nl/media/file/DGGMLF/Intercultural-digital-citizenship-in-the-community.pdf [Erişim tarihi: 03.08.2016].
- Netsafe.(2010)Digital Citizenship in New Zealand Schools. https://www.netsafe.org.nz/wp-content/uploads/2015/09/Digital_Citizenship_in_New_Zealand_Schools_Overview.pdf [Erişim tarihi: 02.08.2016].
- Optus.(2017).*Digital Citizenship: Research Findings and Recommendations 2017.* http://www.digitalthumbprint.com.au/wp-content/uploads/2017/12/Digital_citizenship-Research_Report_2017.pdf[Erişim [Erişim tarihi: 01.08.2016].
- Purdue.(2018).Cyber Ethics. https://www.cerias.purdue.edu/assets/pdf/k-12/infosec_newsletters/07cyberethics.pdf[Erişim tarihi: 02.08.2016].
- Rahm, L. ve Fejes, A.(2019). Popular education and the digital citizen: a genealogical analysis. *European Journal for Research on the Education and Learning of Adults,*

Vol.8, No.1 2017, ss. 21-36. http://www.rela.ep.liu.se/_issues/10.3384_rela.2000-7426.201681/02/rela_9113%20.pdf [Erişim tarihi: 02.08.2016].

- Rainbow.(2017).Digital Citizenship. https://www.rainbowschools.ca/wp-content/uploads/2016/04/Administrative-Procedure-Digital-Citizenship.pdf [Erişim tarihi: 03.08.2016].
- Richardson, J ve Milovidov, E.(2017). Digital Citizenship Education: Multi-stakeholder Consultation Report. https://rm.coe.int/prems-187217-gbr-2511-digital-citizenchip-education-8433-web-16x24/168077bbe4 [Erişim tarihi: 03.08.2016].
- Tamayo,P.D.(2016).*Report to the Legislature: Digital Citizenship Recommendations*. http://www.k12.wa.us/LegisGov/2016documents/2016-12-DigitalCitizenship-LegislativeReport.pdf[Erişim tarihi: 03.08.2016].
- Trinidad.(2012).*National Cyber Security Strategy*. https://www.sites.oas.org/cyber/ Documents/ Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf [Erişim tarihi: 06.08.2018].
- Türkiye.(2016).*Ulusal Siber Güvenlik Stratejisi(2016-2019)*. http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf [Erişim tarihi: 06.08.2018].
- UK.(2016).*National Cyber Security Strategy 2016-2021*. https://assets.publishing. service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [Erişim tarihi: 06.08.2018].
- UN.2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [Erişim tarihi: 04.08.2016].
- UNESCO.(1974). Recommendation concerning Education for International Understanding, Co-operation and Peace and Education relating to Human Rights and Fundamental Freedoms.http://portal.unesco.org/en/ev.php-URL_ID=13088&URL_DO=DO_TOPIC&URL_ SECTION=201.html [Erişim tarihi: 06.08.2016].
- UNESCO.(2016). *A Policy Review: Building Digital Citizenship in Asia-Paci_c through Safe, E_ective and Responsible Use of ICT*. http://unesdoc.unesco.org/images/0024/002468/246813E.pdf [Erişim tarihi: 02.08.2016].

- UNESCO.(2017). Preparing Teachers for Global Citizenship Education: A Template. https://bangkok.unesco.org/sites/default/files/assets/article/Teachers%20Education/GCED062017/Template-GCED-June2017.pdf [Erişim tarihi: 02.08.2016].
- US Homeland Strateji.(2015). *U.S. Department of Homeland security Cebersecurity Strategy, May 2015.* https://www.dhs.gov/sites/default/ files/publications/DHS-Cybersecurity-Strategy_1.pdf[Erişim tarihi: 06.08.2018].
- Vesna, L.J. ve Niveditha,D. (2012).Ethics in Cyberspace a Phylosophical Approach. *International Journal of Advancements in Research & Technology*, Volume 1, Issue3,ss.1-5. http://www.ijoart.org/docs/Ethics-in-cyberspace-a-philosophical-approach.pdf [Erişim tarihi: 02.08.2016].
- Worldometers.info.(2018).Current World Population. http://www.worldometers.info/world-population/ [Erişim tarihi: 02.08.2016].
- WSIS.(2003).Declaration of Principles for Building the Information Society: a global challenge in the new Millennium. http://www.itu.int/net/wsis/docs/geneva/official/dop.html [Erişim tarihi: 19.08.2018].

SİBER UZAYDA ABD-RUSYA REKABETİ: ESKİ AKTÖRLER, YENİ ARAÇLAR

Gizem DEDE*

ORCID: 0000-0002-0001-5443

ÖZET

ABD ve Rusya egemen olma yarışında güç mücadeleleriyle son bir asırda karşı karşıya gelmiş iki devlettir. Her alanda yarış halinde olan iki ülke internetin gelişimine katkı sağlamış ve teknolojinin ilerlemesi konusunda rekabet etmişlerdir. Siber dünyanın gelişmesine karşılıklı çaba ve rekabetle katkı sağlayan iki devletin savunma ve saldırı alanında etkili oldukları görülmektedir. İki kutuplu sistemin getirileriyle geniş çaplı ağ teknolojileri ve siber savunma araçları gelişmiştir. Bu çalışmanın amacı, siber alanın kozmopolit yapısına rağmen hala devlet eksenli çatışmaları içinde nasıl barındırdığı sorusunun cevaplanması ve ulus devlet geleneğinden kalma, dünya hakimiyeti peşindeki iki büyük gücün rekabetini incelemektir. Kozmopolit sistem ile ulus devlet geleneğinin çakıştığı dinamikler siber alan üzerinden değerlendirilmiştir.

Anahtar Kelimeler: Siber Uzay, Güvenlik, Hegemonya, ABD, Rusya, Siber Saldırı.

ABSTRACT

The USA and Russia are two states that have faced power struggles throughout history in the race to become hegemon. The two countries, which are competing in every field, contributed to the development of the internet and competed in the advancement of technology. It is seen that the two states, which contribute to the development of the cyber world with mutual efforts and competition, are effective in the field of defense and attack. With the benefits of the bipolar system, wide-scale network technologies and cyber defense tools have developed. The aim of this study is to answer the question of how cyberspace still hosts state-based conflicts despite its cosmopolitan structure, and to examine the competition of two superpowers pursuing world domination, inherited from the nation-state tradition. The dynamics in which the cosmopolitan system and the nation-state tradition coincide have been evaluated through cyberspace.

Keywords: Cyber Space, Security, Hegemony, USA, Russia, Cyber Attack.

Giriş

Dünya üzerinde teknolojinin küresel düzeyde ilerlemesi, siber alan kullanımının artmasıyla birlikte çatışmalar farklı bir boyuta ulaşmış ve genişleyen ağ teknolojisi mevcut sistem okumalarını beraberinde getirmiştir. Ulus devletin gerektirdiği sınırlar teknoloji çağıyla birlikte ortadan kalkmaya başlamıştır. Eski geleneklerin yıkılması, dinamiklerin alaşağı

*Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Ana Bilim Dalı, Doktora Öğrencisi,

edilmesi gibi etkileri beraberinde getiren siber alan, evrensel olarak kutsal görülen devlet geleneğini de etkilemiştir. Tabu yıkıcı altyapısı ile siber düzen, her insanın ulaştığı ve bunun ötesinde devletler, şirketler ve bireylerin erişebildiği, saldırılar düzenleyebildiği, caydırıcılık modülü geliştirebildiği bir alan haline gelmiştir. Devlet dışı aktörler her ne kadar etkinlik alanını genişletse de devlet hala siber güvenlik alanında olduğu gibi siber tehdit veya saldırı alanında da büyük ölçüde güç sahibidir.

Thomas Rid'e göre politik siber saldırılar üç şekilde gerçekleşebilir: *sabotaj, casusluk ve yıkım*. Sabotaj, hedef ülkeye yönelik fiziksel bir saldırıyı tamamlamak ya da istenmeyen bir avantaj elde etmesini önlemek için ekonomik veya askeri bir sistemi zayıflatmayı veya yok etmeyi amaçlamaktadır. Siber casusluk, bir hükümet veya kuruluşa ait gizli bilgileri elde etmek için bilgisayar ağlarına yetkisiz erişimi içermektedir. Burada doğrudan hedefe ulaşmak yerine bilgilere erişim hedeflenmektedir. Son olarak da yıkım, belirli bir otoriteyi baltalamak için resmî web sitelerine veya medya kaynaklarına yapılan tahribat veya DDoS (Dağıtılmış Hizmet Reddi) saldırıları anlamına gelmektedir (Rid, 2013). ABD-Rusya arasındaki siber çatışmalarda uluslararası ilişkilerde hegemonluk savaşı vererek bu üç saldırı biçimini de yaygın olarak kullandığı görülmektedir.

Ulus-devletin katı kurallarına karşı birey bazında da yıkıcı etkilere sahip olabilecek siber saldırılarla kozmopolit yeni bir dünyanın kapıları açılmıştır. Kozmopolitan bir dünya içerisinde renk, dil, din ayrımsız, sınırları belirsiz pek çok saldırı gerçekleşmekte ve suçlusu bulunamamaktadır. Yeni dünya içerisinde sadece devletler tehdidi ile gerçekleşmeyen saldırılar olsa bile devlet destekli pek çok çatışma da yürütülmektedir. Faillerin meçhullüğü, sistemin erişilebilirliği, kozmopolit ulaşım ağları ile çatışmanın boyutlarında ivmeler meydana gelmektedir.

Soğuk Savaş beraberinde oluşan iki kutuplu sistemle SSCB ve ABD arasında süregelen rekabet tüm koşullarda gerçekleştiği gibi siber alanda da gerçekleşmiş, teknolojinin hızla gelişimine sebep olarak gösterilebilecek bu rekabet bilgisayarlar, ağ teknolojileri, siber uzay gereçlerini içerisine alarak dünyayı büyük bir devrime doğru götürmüştür. Rekabetin boyutu arttığı gibi siber alandaki gelişimden sonra tehdit seviyeleri ve unsurları da artmıştır. Siber caydırıcılığın karanlık bölümlerine doğru yayılan bu gelişmelerin yeterli kalmadığı zamanlar olmuş ve dünya böylelikle siber çatışmalara sahne olmuştur.

Siber çatışmalar daha başka pek çok devlet arasında yaşansa da teknolojinin ilerlemesinde rol almış iki ana aktörün rekabeti siber alandaki çatışmaların çoğunda kendinden söz ettirmiştir. Soğuk Savaş sona erse de ABD ve Rusya arasında gizli iki kutuplu çekişme devam etmiştir. Tarihin çatışma dinamikleri günümüzde hala geçerliliğini korumuş, ABD-Rusya arasındaki gerginlik iki kutuplu sistemin devamı niteliğinde günümüze kadar devam etmiştir. Gerek ABD gerekse Rusya siber çatışmanın tarafları olurken, faili belirsiz pek çok saldırı için birbirlerini suçlamışlardır.

Siber güvenlik çerçevesinde ABD ile Rusya arasındaki siber çatışmaların ve gerilimlerin iki ülkede nasıl karşılandığının irdelendiği çalışmada, siber saldırılara karşı oluşturulan strateji belgelerinden ve savunma stratejilerinden bahsedilecektir. Tarih boyunca mücadelelere sahne olan sistem dinamikleri içerisinde birbirleriyle güç yarışında, rekabet halinde bulunan bu iki süper gücün sadece ekonomik, askeri ve siyasi alanda değil siber alanda da karşı karşıya gelmesi kaçınılmaz olmuştur.

Siber Alanda Hegemonya Gelişimi

Devletlerin kapasitelerinin ürünleri ve askeri alandaki ilerlemesi, siber uzay merkezli teknolojik gelişmelerle birlikte değişimi beraberinde getirmekte ve devletleri yapısal olarak bazen zorlayan şartlar incelendiğinde bu durumun daha etkili bir şekilde birbirleriyle rekabetlerine yansıdığı görülmektedir. Siber uzay teknolojilerinde meydana gelen dönüşüm devletleri rekabet motivasyonuna sürüklemiştir. Tarih boyunca askeri alanda çatışma içerisinde olan devletler teknolojik gelişmelerle birlikte aynı özeni siber alanlarına da göstermişlerdir. Devletlerin ağ teknolojilerindeki hızla artan gelişimi geleneksel olarak uluslararası alandaki çatışma unsurları ve rekabetle değerlendirilmektedir.

1982 yılında bilim kurgu alanında yazar olan William Gibson tarafından Neuromancer adıyla yayınlanan romanda ortaya atılan siber nosyonu Gibson'ın ifadeleriyle "insanlık sistemindeki her bir bilgisayardan alınan verilerin grafik gösterimi, tasavvur edilemez karmaşa, veri kümeleri ve takımyıldızları" şeklinde tanımlanmıştır (Singer & Friedman, 2014: 14). Siber alan oldukça kapsamlı, karmaşık bir ağ sistemini oluşturmaktadır. Kompleksli statüsünden dolayı saldırı sistemleri ve çözümlemesi aynı oranda karmaşık bir yapıyı oluşturmaktadır.

Teknolojinin gelişimi, siber alanı oldukça güvensiz, saldırgan bir merkez haline getirmiştir. Gizlilik ihlalleri, birey ve kurumları tehlikeye atabilecek düzeylere gelmesi, değerli bilgilere

ve altyapılara olan saldırılar, suçlularının sanal ortamı manipülatif amaçlar için kullanmasıyla birlikte güvensiz bir ortama dönüştürülmüştür (Saavedra, 2015: 11). Siber saldırılar ve siber girişimler ülkelere ait değerli bilgileri edinmek için birer fırsata dönüşebilmektedir. Bundan dolayı ülkeler, özellikle ABD gibi süper güçler bu tehditlere karşı siber güvenlik alanlarını geliştirmekte ve saldırılara savunma güçleriyle cevap vermektedir (Minto-Coy & Henlin, 2018: 26).

Teknolojinin gelişimi ve siber uzay imkanlarının artması devlet dışı aktörlerin çeşitliliğini artırmış ve aktörel bazda gelişime yol açmıştır (Singer & Friedman, 2014). Siber alanın her insana açık olması, bilgilere rahatlıkla erişilmesi devletlerin temel anlamda aktör statüsünün sarsılmasına sebep olmuştur. Fakat sarsılma yaşayan aktör yapısı devletlerin rollerinde onulmaz bir değişim oluşturmamıştır. Aktör sayısındaki artış ivmelense de devletler hala temel aktör ve oyun kurucu olarak görünmektedir. Siber kapsamda birçok devlet kendi siber güvenliğini sağlayacak çeşitli argümanlar oluşturmuştur (Nye, 2011: 127-132).

Ulusal güvenlik politikaları da bu düzlemde sahneye getirilen bir argüman olarak karşımıza çıkmıştır. Diğer aktörlerden gelecek olan tehditlere karşı siber strateji belgeleriyle politikalar oluşturulmuş buna ek olarak üretim imkanı genişleyen özel şirketler siber uzayın yayılmasıyla kötücül yazılımlar geliştirmişlerdir. Siber silahlar konusunda da tartışma alanı oluşmuştur. Siber silahların yıkıcı etkileri ve boyutları belirsizliğini korumaktadır. Bilgi edinme amacıyla istihbarat için kullanılan siber saldırı silahları fiziksel zararı büyük olan Stuxnet olayı ile boyut değiştirmiştir. Stuxnet saldırısında bir yazılımın parçası olarak siber silahlar fiziksel zarar için kullanılmıştır (Jenkins, 2013: 68).

Siber suçlar oldukça pahalıya mal olmaktadır. 2012 yılında çeşitli sektörlerde faaliyet gösteren ABD merkezli kuruluş üzerine yapılan çalışmalar ile siber tehditlerin bu işletmeler için yıllık 8.9 milyon ABD doları maliyeti olduğunu ve önceki yıla oranla 8.4 milyon dolar artışıyla maliyetin epey yükseldiği ortaya konmuştur. (Minto-Coy& Henlin, 2018: 29). Bunun yanı sıra siber suçlara karşı savunma maliyeti azken failinin bulunup cezalandırılması için gereken maliyet oldukça fazladır. Cezasız kalan siber ortamda ise suç birleşenleri çoğalmaktadır (Anderson, 2019: 26).

Dünya sistemsel olarak değişim yaşarken suç artışları da aynı değişim sürecinden geçmektedir. Siber alanda suç teşebbüslerinde artış yaşanmaktadır. 2020 Cybercrime

raporuna göre FBI Siber Bölüm Şefi Herb Stapleton'ın yaptığı açıklamaya bakılacak olursa Covid salgını süreci siber suça teşviki artışmış olarak görülmekle birlikte 2020 yılı ABD genelinde de oluşan saldırı maliyetinin çokça arttığı söylenebilir (Morgan, 2020). "Evde kal" çağrısıyla pek çok suç kapsamına giren alanda genişleme görülmüş, insanların rutin hayatı kökten bir değişikliğe gitmiş ve insanlar evde oldukları süre içerisinde suça eğilim gösterdiği istatistikler arasında yer almıştır (Hawdan, 2020: 547).

Geçmişten günümüze askeri saldırıların yanında siber alan yeni bir harp sahası ortaya koymuştur. Hakim saldırı rotalarına bir yenisi daha eklenerek çatışmaların boyutu artırılmış aynı zamanda siber uzay eklentileriyle çatışma sahası da aynı etkiden nemalanmıştır Dünya düzeninin çatışma unsurları siber alan ile birlikte genişlemiştir. Geleneksel hakim saldırı rotalarından gelebilecek her türlü saldırıda suçluların tespiti, siber ortamdaki saldırganların kimliğinin tespitinden çok daha kolay olmaktadır.

Siber saldırılar günümüzde oldukça yaygın bir hale gelmesi, özellikle saldırgan kimliğinin belirlenmesinde yaşanan zorluklar siber saldırılara yönelik cezayi işlem uygulamasının henüz gelişememesi ve ceza olasılıklarının düşük olduğunun algılanması, saldırıların boyutunu ve şiddetini çoğu zaman artırmaktadır. Sanıklar ve sivil yargılamanın zorluğu, hukuki boyutu ile ilgili eksikliklerin bulunması bu alanda büyük çaplı optimal caydırıcılık unsurlarının kullanılmasına dair ihtiyacı da beraberinde getirmiştir (Kobayashi, 2016: 262).

SSCB tarafından yapay uydunun üretilmesi ve geliştirilmesinin ardından Sputnik'in uzaya fırlatması ile her alanda yaşanan rakip güç algısına bir yenisi daha eklenmiştir. Sputnik ile hegemonik güç olmak isteyen ABD ve SSCB karşı karşıya gelmiştir. Rekabet yarışındaki iki ülke bu algıya bir başka alan olan siberi de eklemiştir. Siber alandaki rekabet unsurları teknolojik gelişmelere sebep olmuş ve dünya 1950'li yıllardan itibaren hegemonyanın yarışına şahitlik etmiştir. ABD'nin SSCB karşısında tehdit algısı içerisine düşmesi kendi teknolojik araçlarını geliştirmesine sebebiyet vermiştir (Schmid, 2018: 39).

1957 yılında SSCB, ilk yapay uydu olan '*Sputnik II'* icadı ile dünya tarihine geçecek bir dönüm noktasına imza atmıştır. İki kutuplu sistemin bir diğer adayı olan ABD ise bu girişimle birlikte nükleer tehdit algısı hissetmiş ve ABD dönem başkanı olarak görev yapan Eisenhower'ın bilim başdanışmanı James Killian ise bu gelişme ile "Amerika'nın bilimine, teknolojisine ve eğitimine itimadın aniden buharlaştığını söylemiştir." (Bıçakçı, 2014: 104).

Siber teknoloji alanında genişleme sürecinin başlangıcı ABD için 1930'lar olarak alınabilmektedir. Fakat ABD ve SSCB arasındaki rekabetin teknolojik alana yansımış olmasına örnek olarak, Sputnik II'nin ardından, ABD'nin Şubat 1958 yılında İleri Araştırma Projeleri Ajansı'nı (Advanced Research Projects Agency/ARPA) kurmuş olması verilebilir (Bıçakçı, 2014: 104).

Genişleyen siber teknoloji çatışmayı da beraberinde getirmiş ve büyük güçler strateji belgeleri ile kendilerini siber uzayın bilinmezliğinden korumak ve gerekirse çatışmayı kendileri başlatmak için, kısacası hem savunma hem de saldırı amaçlı, kendi kurumsal statülerini genişletmişlerdir. ABD, siber uzay teknolojilerini geliştirmek isteyen aktörlerden biri olarak karşımıza çıkmaktadır.

ABD Rusya Hegemonya Yarışında Siber Alanın Kapsamı

ABD 1900'lerin başında pek çok alanda kazandığı yükselme ivmesiyle birlikte teknolojik gelişmelerde de dünya liderleri arasına yerleşmiştir. Soğuk Savaş döneminin getirmiş olduğu karşılıklılık ortamında SSCB ile kurduğu askeri ve ideolojik rekabeti (Akyeşilmen, 2018: 25) uzay ve daha başka stratejik alanları da etkilemiştir. Devletler için yeni bir güvenlik açığı oluşturan siber alanda özellikle 1960 yıllarında artan devrim niteliğinde teknolojik gelişmeler noktasında ABD öncü devlet rolünü üstlenmiştir ve hala sektörde lider ülke olmaya da devam etmektedir (Nye, 2011: 20).

İki ülke arasında gerilimi tırmandıran Küba Füze Krizi olarak bilinen olayda rekabet algısının boyutları gözler önüne serilmiştir. SSCB'nin füze teknolojisindeki büyük gelişmelere imza atması ABD'nin güvenlik politikalarını artırmasına sebep olmuştur. Nükleer silahlara yönelik "İkinci vuruş yeteneği" bağlamında topyekûn bir saldırıyı niteleyen, (Crosston 2011: 101) *Karşılıklı Kesin Yıkım/Caydırıcılık/İmha- Mutually Assured Destruction- MAD* silah kullanımını caydırmak için bir girişim olarak güvenlik politikalarına gündem olmuştur (Bıçakçı, 2014: 104). MAD politikasının işe yaradığı Küba Krizi ile görülmüştür (Nye, 2011: 24). Daha hesap edilebilir hale getirdiği nükleer savaşın tahribatını en aza indirmeyi planlayan *Esnek Karşılık- Flexible Response: FR* ise savaşın yıkıcılığına daha sert bir tepki ile değil, rakip ülkenin faaliyetlerine uygun olarak hesap edilen bir karşılık verme olarak bilinen savunma stratejisidir (Poole, 2013: 10).

MAD politikasıyla birlikte gündeme gelen konulardan biri nükleer saldırıyla çökmesi muhtemel görülen iletişim hatları olmuştur. Bu iletişim hatlarındaki tahribatın az olması için çalışmalar başlatılmıştır. Herhangi bir nükleer savaş durumunda ARPANET'in çalışmaya devam etmesi için yapılması gerekenler incelenmiştir. İletişim hatlarının çalışmaya devam edebileceği ağ yapısını ortaya çıkarmak ARPANET'in ilerlemesini ve kullanımının yayılmasını sağlamıştır. İnternetin ilk oluşumu sayılan ARPANET 1970'lerde birleştirilmiştir. Böylece uluslararası bilgisayar ağları ortaya çıkmıştır (Bıçakçı, 2014: 105).

ABD üstün teknolojik gelişmelere imza attığı gibi siber altyapısını da güçlendirmiştir. ABD Savunma Bakanlığı "siber savaşçılar için dört aşamalı eğitim" modülünü geliştirerek askeri personel için kapsamlı bir geliştirme stratejisi eğitimi vermiştir. (Charmonman& Trichachawanwong, 2014: 8). ABD ordusu Aralık 2013'te Washington'da siber komuta operasyonlarını pekiştirmiştir. Gürcistan'dan siber ve ağ operasyonlarını taşımış ve üzerine çalışmalar gerçekleştirmiştir. (Charmonman& Trichachawanwong, 2014: 9). Soğuk Savaş sonuna doğru teknolojinin gelişimi oldukça hızlanmış ve bu gelişmeler dünya geneline yayılmıştır. Siber alandaki bu muazzam ilerleme beraberinde siber güvenlik çalışmalarını da getirmiş ve devletler güvenlik gibi önemli bir nosyonu her alanda olası tehditler için geliştirmek zorunda kalmıştır.

ABD ve Rusya Federasyonu arasında Soğuk Savaş zamanı karşılıklı ilerleme ve gücü elinde tutmaya dayalı rekabet yarışının içerisinde ağ teknolojisinin gelişimi de yerini almıştır. İki kutuplu sistemde süper güçlerin girdiği mücadele aslında tüm dünyada devrim niteliğinde olan dönüşümler silsilesini beraberinde getirmiştir. İstikrar kazandıran iki kutuplu düzende dünya savaşlardan arınmıştır. Her konuda gelişim ve ilerlemeye iki ülke tarafından ivme kazandırılmıştır. Ülkeler planlı ilerlemese dahi sistem içerisinde kendini göstermek ve güvenliklerini sağlamak için güç üstünlüğünü kazanmanın peşine düşmüşlerdir.

1980 yılında dönemin ABD başkanı olan Reagan tarafından geliştirilmiş Stratejik Savunma Girişimi/Strategic Defense Initiative (SDI) olarak pek çok yerde tanımlanmış olan Yıldız Savaşları o döneme damgasını vurmuş bir askeri proje olarak karşımıza çıkmaktadır. Bu proje hayata geçmemiş olsa da SSCB tarafından herhangi bir saldırı durumuna karşı üstün savunma ürünü olarak tasarlanmıştır (Lambeth, 1986: 1). Rekabetin boyutlarını gözler önüne seren bu proje dönemin şartları ve SSCB'nin kullandığı silahlanmayı uzaydan yok etmesi (Snyder, 1986: 4) temeline kurulu fikri tasarısıyla iki kutuplu sistemin realist açıdan dengelemesini

bozacağına dair bir inanç içinde rafa kaldırılmıştır. Kısa bir zaman sonra SSCB dağılarak iki kutuplu sistemin sonunu getirmiştir. Teknolojinin ve siber alanın geldiği ürkütücü bir noktayı hedefleyen proje şartlar dahilinde hayata geçirilirse pek çok devlet için olduğu kadar uluslararası sistemin yapısı içinde büyük tehditler oluşturabilir.

Sovyetler ABD'den daha uzun süredir savunma mekanizmalarına, askeri teknolojilere büyük önem vermiş gibi görünse de ABD savunma teknolojilerinde çok daha önemli ilerlemeler ve savunma mekanizmalarında daha kilit gelişmeler görülmüştür. Saldırı konusunda da paralel bir gelişim gösteren ABD boyutunu ve gücünü artırmıştır. Sovyetlerin temel anlayışı ise karşı saldırıyı savunma amaçlı bir destek olarak görmektir. Saldırı Sovyetlerin stratejik planlamasının dinamiklerini oluşturmaktadır (Lambeth, 1986: 47).

Kritik altyapı da siber güvenlik için oldukça önemlidir. Siber uzay ülkelerin yaşam destek sistemlerinin kritik altyapılarını desteklemektedir. Altyapıyı, ülke için gerekli mal ve hizmetler ve hem özel sektör hem de devletler için temel bağımsız sistemler ağı olarak tanımlanmaktadır. Bu altyapıların çoğu oldukça büyük öneme sahiptir. Altyapıların güvenliği ulusal güvenlik ile bir tutulmuş ve gelebilecek her türlü zararın ulusal güvenliği de aynı şekilde zayıflatacağı söylenmiştir (Veazie, 2003: 2). Devletler ulusal ve uluslararası düzeyde altyapılar üzerinde oluşan siber tehditlerden endişe duymaktadır (Watney, 2013: 131).

ABD'de gerçekleşen 9/11 olaylarında Dünya Ticaret Merkezi (WTC) ve Pentagon'da ülkenin kritik altyapısı ciddi şekilde etkilenmiştir. Havacılık sektörüyle ilgili pek çok kuruluş kapatılırken ABD ekonomisi hasara uğramış ve 9/11'de siber alana saldırı iddiaları pek çok zaman tartışmanın gündemini oluşturmuştur. Ana tabloya bakıldığında 9/11 olayları öncesinde de ABD siber alanda güvenlikle ilgili altyapıyı iyileştirici çalışmalara önem vermiştir (Veazie, 2003: 2).

Rusya Sovyetler Birliği'nin çökmesi ile gücünü kaybetmiş ve ABD'de herhangi bir denge olmadan hareket etmekte özgür hale gelmiştir. Putin başkan olmasıyla uluslararası ilişkiler sistemi içerisinde hedefi eski ihtişamlı günlerine Rusya'yı geri döndürmek olmuştur. 9/11 sonrası Rusya Batı'ya hiç olmadığı kadar yaklaşmış ancak uzun sürmemiştir. 2003 yılında ABD'nin Irak müdahalesi ile gerginlik tekrar başlamıştır. 2008'de Kafkasya'daki çatışma, Rusya'nın askeri harekâtı bir dış politika aracı olarak kullanmaya hazır olduğunu tüm dünyaya göstermiştir (Baezner & Robin, 2018: 6).

ABD ile tekrar arası açılan Rusya rekabet dinamiklerini teknolojik gelişmeler alanında olduğu gibi siber alandaki saldırı potansiyelinde de göstermiştir. Dünya sisteminin Soğuk Savaş sonrası değişimiyle birlikte fiziki çatışmaların sanal ortamda sürdürülen saldırılara dönüştüğü sistematik düzende Rusya hızla eski gücüne kavuşmuştur.

Siber Güvenlik Argümanlarının Gelişimine Kısa Bir Bakış

1950 yılında DPA/ Defense Protection Act- Beyaz Saray tarafından kritik altyapıyı destekleyecek bir çerçeve oluşturulmuş Savunma ve Koruma Yasası çıkarılmıştır. Ulusal savunmayı geliştirmek ve koruma altına almak için girişimler gerçekleştirilmiştir. 1987 yılında ise The Computer Security Act of 1987- Bilgisayar Güvenliği Yasası geliştirilmiştir. Böylece devlet tarafından federal bilgisayar sistemleri güvence altına alınmıştır (Veazie, 2003: 2). 1988 yılında Robert Tappan Morris'in kendi soyadından oluşan Morris internet solucanını denemesiyle CERT oluşturulmuştur (Killcrece, 2003: 8).

ABD'nin siber güvenlik alanında yaptığı atılımları ve siber alanın güvenliğiyle ilgili kurumsal yapılanmaları ABD Savunma Bakanlığı/DoD, ABD İç Güvenlik Bakanlığı/DHS, Gizli Servis Sağlayıcıları/FBI-CIA olarak sıralanmaktadır. Saldırılar esnasında kritik alanları belirleyebilmek adına üç temel siber savunma kurumu önem taşımaktadır. Ayrıca Ulusal Güvenlik Ajansı olarak bilinen NSA'de İç Güvenlik Bakanlığı/DHS tarafından yürütülen programlar ile de siber güvenlik için gerekli çalışmalar yürütülmektedir (Conklin, 2014: 2007).

ABD geçmişten günümüze siber ile ilgili gelişmelerde altyapısını güçlendirecek argümanlara gitse de asıl hamlesini 2003 yılında gerçekleştirerek kendisine güvenli bir alan oluşturmaya çalışmıştır. Siber alan üzerinde hakimiyet oluşturmak isteyen ülkelerden biri olan ABD ilk belgesini 2003 yılında yayınlamıştır. Secure Cyberspace isimli belge Beyaz Saray tarafından yayınlanmış ve güvenlik açısından önemli siber uzay tanımlarının yer aldığı belgede altyapı işleyişi önemli bir meseleyi oluşturmuştur (The White House, 2003).

Rusya'nın ise siber alanda değişimi ve ilerleyişi oldukça hızlı olmuş, Soğuk Savaş bitiminde iki kutuplu sistemin yıkılmasına rağmen Rusya siyasi alanda hızlı şekilde kendisini toparlayabilmiştir. Tüm gelişmelerin yanı sıra siber alanda da aynı hızla küllerinden doğmayı başarmıştır. Rusya stratejilerini ve siber saldırılarını küçük alanlarda yapmaktan ziyade daha geniş coğrafyalarda kullanmayı tercih etmiştir (Lilly & Cheravitch, 2020: 130). Bu da

Rusya'nın hâkim strateji izleyerek büyük güç politikasına katkı sağlamasından kaynaklanmaktadır.

Aslında Rusya'nın "bilgi savaşı" üç amacı içermektedir. Bu amaçlar siber operasyonlarla elde edilen gizli verilerin toparlanması, hükümet yetkilileri hakkında bilgilerin toplanması ve bilgilerin gerçeğinden çarptırılarak kamuoyuna sunulmasından oluşmaktadır (Shad, 2018: 47). ABD ve Birleşik Krallığın açıklaması ile örtüşen bu teoriye göre Rusya siyasetçiler ve resmî kurumları hedef alan siber saldırılar yapmaktadır (News Wires, 2023). Savunma ve saldırı amacıyla gerçekleştirilen bilgi toplama işlemi Rusya'nın siber yol haritasını oluşturmaktadır.

ABD Aleyhine Rusya Tarafından Gerçekleştirilen Siber Saldırılar ve Etkileri

Dünya genelinde 2000 ve sonrasında siber saldırı oranları artmış, 11 Eylül sonrası ABD Afganistan'da fiziksel bir güvenlik alanı ihtiyacı oluştururken bunun yanında siber teknoloji de yaygın şekilde kullanılmaya başlanmıştır (Singer & Friedman, 2014: 100). Özellikle 2011 yılına gelindiğinde terör olarak nitelendirilebilecek siber alan saldırılarını yükseltmiş, etkilerini ise Suriye'de yaşanan iç savaş sırasında rejimin haber sitelerine yönelik saldırısı ile göstermiştir (Singer & Friedman, 2014: 112). İzinsiz olarak gerçekleşen bu girişimler tehdit olarak algılanarak ABD'nin siber tehdit konusunda kendisini geliştirmesine de sebebiyet vermiştir.

ABD ve Rusya'nın hem saldırı hem de savunma üzerindeki etkinliğine değinmek bu iki ülke arasındaki siber saldırıların şiddeti ve ABD aleyhine gerçekleştirilen saldırılarda savunma ve saldırı düzeylerini incelemek açısından oldukça önemlidir. Öncelikle ABD'nin savunma ve saldırı kapasiteleri incelendiğinde siber alan içinde ABD saldırıda orta, savunmada güçlü bir mekanizmaya sahiptir. Rusya ise güçlü bir saldırıyla birlikte güçlü bir siber savunma yaparak etkinlik alanını düzenlemiştir (Göçoğlu & Aydın, 2019: 247).

İki hegemon ülke tarihte pek çok kez karşı karşıya gelmiştir. Siber alanda ise ilk karşılaşmaları aslında Rusya aleyhine gerçekleştirilmiş bir atak olarak literatüre geçmiştir. O döneme kadar yaşanmış ilk siber saldırı olmasının yanında Sibirya'da gerçekleşen patlama, siber alanın fiziksel zarara yol açtığı ilk olay olarak değerlendirilmiştir (Brown & Keira, 2012).

The Economist gazetesinin 2017 yılında yayınladığı bir habere göre yaklaşık iki yüzyıl önce tarihin ilk siber saldırısı Fransa'ya karşı gerçekleştirilmiştir (Standage, 2017). Fakat

çoğunluğun kabul ettiği ilk siber girişim Sovyetlerin ABD'de bulunan doğal gaz hattına zarar vermek isterken SSCB Sibirya gaz hattının patlatılması olarak tarihe geçmiştir. Logic bomb/Mantık bombası olarak adlandırılan bu saldırıyla Sovyetlere karşı siber saldırı düzenlenmiştir (Cornish, 2010: 7). Tarihin en şiddetli saldırısı olarak kabul gören ve zararı büyük yıkımlara yol açan girişim CIA tarafından doğal gaz hattına konumlandırılan kötü amaçlı yazılımlarla gerçekleştirilmiştir (Rid, 2013: 4).

2008 yılına gelindiğinde ABD askeri sistemlerine nüfuz eden "BTZ" saldırısı gerçekleştirilmiştir. ABD sistemine yönelik siber saldırı Rusça metin parçaları içeren kodlarla yürütülmüştür (Jones, 2014). Irak ve Afganistan'da savaş yürüten ABD Merkez Komutanlığına sızan kötü amaçlı yazılım ise Savunma Bakanı Yardımcısı olan William Lynn tarafından verileri çalma teşebbüsü olarak nitelendirilmiştir. Casus yazılım ile bilgisayarlara sızılmasıyla oluşan siber saldırının o dönem içerisinde Rus istihbaratı tarafından gerçekleştirildiğinden şüphelenilmiştir (Stewart, 2011).

Rusya'da 2011 yılında gerçekleşen seçimler esnasında devlet başkanı Vladimir Putin seçimleri kazanmış fakat karşıt gruplar tarafından bu seçim protestolara sebebiyet vermiştir. DDos saldırıları gerçekleştirilerek Rusya'da halkın sosyal medya platformları üzerinden seçim karşıtı protestolarda bulunması engellenerek Rus halkına karşı siber güç kullanılmıştır. Rusya başkanı Putin ise halkın protestoları ve toplu şekilde oluşan ayaklanmalara karşı ABD Dış İşleri Başkanı Hillary Clinton'ı hedef göstermiş ve sosyal medya platformlarında siber alanda protestolara katkıda bulunduğunu iddia etmiştir (Baezner & Robin, 2018: 6). Rusya'nın bu iddialarının ardından karşılıklı ilerleyen ve dengeli yol izleyen saldırıların bir sonraki durağı ABD hükümetinin seçimlerine yapılan müdahale olmuştur.

ABD Rusya'yı seçimlere yaptıkları müdahaleden dolayı suçlarken Rusya Democratic National Committee-DNC hackleme suçlarını yalanlamıştır. Olayla ilgili soruşturma yürüten müfettişlerin iddiaları olaylardaki iddianın asılsız olmadığına işaret etmiştir. Özellikle IP adresleri ve kullanılan kodların dili gibi bulgular saldırıdan sorumlu faillerin Rus hackerları APT28 ve APT29 olduğu yönündeki olasılıkları çoğaltmıştır (Connel&Vogler, 2016: 24). Rusya hükümeti suçlamaları reddetse de olaylara bu grupların katkısından şüphelenilmiş ve Rusya'nın bu olayda vekil olduğu yönünde iddialar ortaya konmuştur (Baezner & Robin, 2018: 10). ABD'nin Putin'e karşıt görüşleri desteklediği iddiasında olan Rusya, 2016

seçimlerine müdahalesi konusunda da bir intikam niteliği güden saldırıların boyutunu genişletmiştir.

2013 yılına gelindiğinde istihbarat sızıntılarına karşı gelişmişliğin ve dünya çapında hedeflere karşı internet gözetiminin ölçütlerinin altını çizen ve "Snowden olayı" olarak bilinen bir siber saldırı yaşanmıştır (Lindsay, 2014: 7). ABD Rusya ilişkilerini gerilime sürükleyen Edward Snowden olayıyla birlikte iki ülke arasındaki siyasi politika karmaşık bir süreçten geçmiştir. Snowden NSA'da çalışmakta olan bir uzmanken 2013 yılında ABD'ye ait gizli bilgileri The Guardian gazetesine vererek deşifre etmiştir (House Report, 2016: 15). Bunun üzerine önce Çin Halk Cumhuriyeti'ne ardından Rusya'ya kaçan Snowden, burada ABD'nin iade talebine rağmen kalmış ve Rusya tarafından sığınması onaylanmıştır. Trump'ın af çağrısına uymayan, ABD'nin istihbarat bilgilerini sızdıran casusa sığınma hakkı verilmesi gerilimi artırmıştır (Alhinnawi, 2015: 6). Bu olayın ardından gizli belgelerle birlikte NSA'nın Çin ve Hong-Kong bilgisayarlarına sızdığı ayrıca 2009 G-20 zirvesinde bulunan devlet adamlarını dinlediği açığa çıkmıştır (Singer & Friedman, 2014: 93). Edward Snowden olayının bir diğer önemli yanı ise ABD'nin Avrupa ve diğer ülkelere karşı gerçekleştirmiş olduğu siber saldırıların ortaya çıkması olmuştur (Shad, 2018: 47).

Snowden olayının ardından iki ülke arasındaki siber gerilim durmamıştır. 2015 yılında Washington CNN'de yayımlanan bir habere göre Rusya, White House'a bir siber saldırı girişimi gerçekleştirmiştir. Rus korsanlar tarafından gerçekleşen bu saldırıda White House bilgisayarları üzerinden ABD sisteminin hassas bölümlerine erişilmeye çalışılmıştır. FBI, Gizli servisler ve ABD istihbarat birimleri tarafından o döneme kadar yaşanmış en karmaşık saldırı olduğu iddiaları yayılmıştır. ABD saldırıda tüm dünya ülkelerinin bu faili meçhul saldırı için şüpheli olduğu konusunda inceleme başlatsa da kullanılan kodlar ile Rusya'nın hackerları arasında bir bağ olduğu düşünülmüştür (Perez&Prokepecz, 2020).

İlk olarak White House saldırısı öncesinde 2014 yılında Dışişleri Bakanlığı'na ait ağlara erişim sağlamak için kötü niyetli yazılım içeren şüpheli bulgulara sahip e-mailler gönderilmiştir. Ardından White House verilerine erişilmiştir. Saldırının korkutucu dereceye ulaşan boyutu ise bilgisayar korsanlarının White House ağları üzerinde etkinliği uzun süreli ve yıpratıcı olmasa da Dışişleri Bakanlığının ağlarında kalıcılık elde etmeyi başarmış olması ve 2015 yılında yayınlanan habere göre veri sızıntısının o dönem için sürekli olabileceği yönünde gerçekleşen iddialardır (Brewster, 2015).

2015 yılında “The Dukes” isimli yazılımla ABD ve NATO genelinde siyasi konularla aktif olarak ilgilendikleri ve dış politika düşünce kuruluşlarını hedef alan kampanyalar yürüttükleri iddia edilen hacker grubunun (Hyvärinen, 2015: 6) yedi yıl gibi bir süre boyunca siber saldırı gerçekleştirdikleri ve Rusya istihbaratına bağlı olduğu ortaya atılmıştır (Brewster, 2015).
ABD ve Rusya arasında büyük krizlere sebebiyet veren bir başka siber çatışma ise 2016 yılında ABD seçimlerine yönelik Rusya’nın müdahalesi iddialarının büyümesi olmuştur. Washington’daki seçimlerde Moskova’nın suçlanması iki ülke arasında tarihsel gerilimi siber alana taşımıştır. Hillary Clinton’a ait seçim kampanyasında e-maillerin sızdırılmasına yönelik saldırı ABD genelinde yankı bulmuştur (Yönak, 2017). 2016 seçimleri sırasında kullandıkları araçlarla ilgili ise “The Dukes” adlı kötü amaçlı yazılımların kullanıldığı öne sürülmüştür. Siber olaylara müdahale şirketi olan Volexity’nin raporuna göre; seçimlere yönelik saldırı, Cosy Bear, APT29 ve The Dukes olarak bilinen Rus kötü amaçlı yazılım geliştirme çetesinin faaliyetleriyle yakından benzerlik göstermektedir (Adair, 2016).

2016 yılında ABD başkanlık seçim kampanyası esnasında Rusya destekli hackerlar, Demokrat Parti yetkililerine yönelik geniş çaplı bir etki operasyonunun ardından bazıları tarafından "Soğuk Savaş 2.0" olarak nitelendirilen ABD-Rusya siber gerilimleri ağırlaşmıştır. Gizli materyaller, 2015 ve 2016 döneminde Demokratik Ulusal Kongre'nin (DNC) bilgisayar ağlarına siber müdahale ve personelinin e-posta hesaplarına siber saldırı yoluyla toplanmıştır. Hacktivist Guccifer 2.0 ve gizlilik karşıtı web sitesi WikiLeaks aracılığıyla internete sızdırılmıştır. Sızdırılan bilgiler arasında DNC'nin dahili kampanya iletişimi, Donald Trump'a karşı "muhalefet araştırması" ve Hillary Clinton'ın kampanya başkanı John Podesta'ya gönderilen e-posta mesajları yer almaktadır (Shad, 2018: 48).

Clinton’a karşı Trump lehine sürdürülen siber saldırıyla mültecilerle ilgili çekincelerin, Trans-Pasifik dahil bir takım ticari anlaşmaların sızması ve daha pek çok gizli belgenin açığa çıkması 2016 seçimlerini etkilemiştir. WikiLeaks tarafından “Ekim Sürprizi” adıyla sızdırılan emailler ABD gündemini uzun süre meşgul etmiştir. (Shad, 2018: 49). Ekim 2016'da ABD, Rusya'yı başkanlık seçimlerine müdahale etmek amacıyla DNC'nin bilgisayar ağlarına sızma girişiminde rol almakla suçlamıştır (Ackerman& Thielman, 2017). İddialar kanıtsız olsa da Rusya’nın seçimlere müdahalesi konusunda pek çok argüman bulunmuş fakat faillerin meçhullüğü ile somut verilere ulaşılamamıştır. Belirsizliğin mevcut olduğu siber alanda da hukuka uygun bir yargılama yapılamamıştır.

2020 yılında ise ABD ve Rusya arasındaki siber gerilim sürmüş "Şüpheli Rus Bilgisayar Korsanları" başlıklarıyla açılan haberler pek çok gazetenin manşetini oluşturmuştur. Sonuçları hala bilinmeyen ABD Hazine ve Ticaret bakanlığı üzerine gerçekleşen saldırıda FireEye şirketinden bilgi sızdırılmıştır (Harding& Sabbagh, 2020; Bertrand& Desiderio, 2020). ABD Başkanı Joseph Biden olayın failleri bulunduğunda üzerine ağır sorumlulukları yükleyeceği yönünde açıklama yaparken, eski Başkan Trump ilk başta olaylarla ilgili sessiz kalmıştır. Biden ayrıca uluslararası alanda devletlere risk oluşturan siber saldırılar ile ilgili; "İyi bir savunma yeterli değildir; düşmanlarımızı en başta önemli siber saldırılar yapmaktan alıkoymalı ve caydırmalıyız." demiştir. Rus bilgisayar korsanlarının tahmini 40 tane devlet kurumu, düşünce kuruluşu ve şirkete sızdığı belirlenmiştir (Sanger&Perlroth, 2020). Hazine ve Ticaret departmanlarındaki e-posta sistemlerinin ihlal edildiği siber saldırının federal sistemlere yönelik son beş yılın en karmaşık ve tahmini olarak en büyük saldırılarından biri olduğu iddia edilmiştir (Sanger, 2020). FBI, İç Güvenlik Bakanlığı ve Ulusal Güvenlik Ajansı tarafından ortak yapılan açıklamada hacker hareketinin Rus kökenli olmasının mümkün olduğuna değinmişlerdir (Johnson, 2021).

2022 yılına gelindiğinde ise gerilim sürmüş Ukrayna'ya karşı sık sık siber saldırı gerçekleşmesinin ardından açıklama yapan Biden, Rusya'nın ABD'ye yönelik saldırı planladığını ve her türlü siber girişime karşılık vereceklerini söylemiştir (Tidy, 2022). Ardından Rusya, Ukrayna'nın kendi ülkelerine düzenlediği siber saldırıların ABD destekli yapıldığını iddia etmiştir (Pempel, 2022).

2023 yılına gelindiğinde Russia's Federal Security Service (FSB) tarafından en etkili siber casusluk aracı olan ve gizli bilgilere erişim için kullanılan "Snake" (NSA, 2023) ABD şirketlerini hedef almıştır. Casus programı etkisiz hale getirdiklerini açıklayan FBI, Rusya'nın siber casusluk için kullandıkları en etkili kalesini tamamen çökerttiklerini duyurmuştur (Euronews, 2023). Rusya'nın ABD aleyhine gerçekleştirdiği saldırılar ve ABD'nin aynı oranda karşılık vermesi hegemonya yarışındaki iki devleti tarih boyunca mücadele içerisinde bırakmıştır.

Sonuç

21. yüzyılda gelişen ağ teknolojilerinin getirileri arasında birçok olumlu nokta olduğu gibi kötüye kullanımın oluşturduğu olumsuz yönler de vardır. Siber saldırı kapsamının her geçen gün genişlemesi yıkıcılığı artırmıştır. Siber saldırıların tahmin edilmesi güç boyutlara

ulaşması negatif bir teknoloji algısı sunmaktadır. Uluslararası alanda devletlerin güvenlik açıklarını hızlı ve etkili bir şekilde yakalayan tehditleri beraberinde getiren saldırıların karşısında savunma güçlerini geliştirmek oldukça önemli görülmektedir. Sistemde oluşan güvensizlik, herhangi bir engelleyici üst otoritenin bulunmamasıyla artmaktadır. Anarşinin hâkim olduğu uluslararası ortama benzer bir yapılanma siber alan içerisinde de görülmektedir. Kural koyucu otoriter bir üst merciinin olmamasıyla birlikte caydırıcılık unsurlarının da yeterince bulunmaması siber güvenlik alanlarını tehlikeye atmaktadır.

Devletlerin yanı sıra pek çok hackerın sivil olarak bulunduğu siber ortam, devlet otoritesini, devletlerin sistemdeki varlıklarını belirsizliğe sürüklemektedir. Böylece sınırlardan bağımsız kozmopolit bir dünyanın kapılarını aralayan siber alan, tüm dünya ile saniyeler içerisinde irtibatı kolaylaştırdığı gibi din, dil, sınıf ayrımını ortadan kaldırmıştır. Sivil bir vatandaşın eskiden üst kademe kişilere erişmesi, devletin yönetim merkezi ile haberleşmesi oldukça zorken şimdiki durum için yapılan değerlendirmede her insan sınıf ayrımı olmadan öteki ile iletişime rahatlıkla geçmektedir. Bu durum sınırları görünmezliğe, belirsizliğe ve kaosa sürükleyen önemli göstergelerdendir.

Kozmopolit bir siber alanda savaş ve iletişim algısı ve bu algının kullanım yetkisi her geçen gün değişse de hala devletler tarafından veya devletler eliyle pek çok saldırı gerçekleştirilmektedir. Özellikle büyük güçler arasında üstün kodlama ve teknolojiyi kullanabilme kapasitesinin fazla oluşu geçmiş husumetleri sürdürmekte önemli bir rol oynamıştır. Soğuk Savaş sonrası sistem dinamiklerinde çatışma nosyonunun okumaları dikkate alındığında tarihi oldukça eskiye dayanan saldırıların özellikle ABD ve Rusya arasında bir hegemon yarışına döndüğü görülmektedir. Uluslararası sisteme hâkim olmak için yürütülen mücadeleler günümüze kadar devam ederek yeni gelişmelerle mevcut düzene devrim niteliğinde görülen siber alanda da sürmüştür.

Tek taraflı bir çatışma analizinden oluşan araştırmada Rusya'nın ABD aleyhine gerçekleştirdiği siber saldırılar ve bu saldırıların boyutları ele alınmıştır. Bahsi geçen ülkeler casus yazılımlardan elde ettikleri kodlar ve bu kodlara yönelik suçlamalarıyla birbirlerinin aleyhinde pek çok diplomatik diyalog gerçekleştirmiştir. Faillerin belirsizliği iki ülkeye de gerçekleştirilen saldırıların tespitini zorlaştırmaktadır.

Kaynakça

ACKERMAN, Spencer&THIELMAN Sam. (2017). *US Officially Accuses Russia of Hacking DNC and Interfering with Election*.

ADAIR, Steven (2016). *PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs* "Volexity Report". https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/ [Erişim Tarihi: 17.10.2023]

AKYEŞİLMEN, Nezir. (2018). *Disiplinler Arası Yaklaşımla: Siber Politika& Siber Güvenlik,* Ankara: Orion Kitabevi.

ALHINNAWI, Bahaa. (2015). "The Snowden Revelations and Their Effects on Eurupean it-Related Decisions and Decision-Making Processes", *Proceedings of the 2015/16 Course on Enterprise Governance and Digital Transformation*.

ANDERSON, Ross. vd. (2019). "Measuring The Changing Cost Of Cybercrime", *Workshop on the Economics of Information Security*.

BEAZNER Marie &ROBIN Patrice (2018). "Cyber-Conflict between the United Stets of America and Russia", *Risk and Resilience Team Center for Security Studies*.

BERTRAND, Natasha& DESIDERIO, Andrew (2020) "How Suspected Russian Hackers Outed Their Massive Cyberattack" *https://www.politico.com/news/2020/12/16/russian-hackers-fireeye-cyberattack-447226* [Erişim Tarihi: 15.12.2023]

BIÇAKCI, Salih (2014). "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, 10(40).

BREWSTER, Thomas. (2015). Russians Hacked White House Via State Department, Claims Report. https://www.forbes.com/sites/thomasbrewster/2015/04/08/russians-hacked-white-house-cnn/?sh=791b2d9260cb [Erişim Tarihi: 17.12.2023]

BROWN, Gary &POELLET, Keira, (2012). "The Customary International Law of Cyberspace." *Strategic Studies Quarterly*, 6(3).

CHARMONMAN, Srisakdi & TRICHACHAWANWONG, Chatpawee (2014), "Training of Interdisciplinary Cyber Warriors", International Journal of the Computer, *the Internet and Management*.

CONELL, Michael & VOGLER, Sarah, (2016) *Russia's Approach to Cyber Warfare*, Washington: CNA.

CONKLIN, Arthur vd. (2014). Re-engneering Cybersecurity Education in the US: AN Analysis of the Critical, *47th Hawaii International Conference on System Sciences*, Waikoloa,

HI.

CORNISH, Paul. vd., (2010). *On Cyber Warfare, A Chatham House Report*, London: The Royal Institute of International Affairs.

CROSSTON, Matthew D. (2011). "World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence", *Strategic Studies Quarterly*, *5*(1).

EURONEWS (2023), "FBI, Elit Rus Casusların Kullandığı 'Yılan Yazılımını' Sabote Ettiğini Duyurdu" https://tr.euronews.com/2023/05/09/fbi-elit-rus-casuslarin-kullandigi-yilan-yazilimini-sabote-ettigini-duyurdu#:~:text=Amerika%20Birleşik%20Devletleri%20Federal%20Soruşturma,ederek%20etkisiz%20hale%20getirdiklerini%20duyurdu. [Erişim Tarihi: 17.01.2024]

GÖÇOĞLU, Volkan, AYDIN, Mehmet Devrim, (2019). "Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırmalı Analiz", *Güvenlik Bilimleri Dergisi*, 2019, 8(2).

HARDING, Luke& SABBAGH Dan, (2020). "Suspected Russian Hackers Spied on US Federal Agencies" https://www.theguardian.com/world/2020/dec/14/suspected-russian-hackers-spied-on-us-federal-agencies [Erişim Tarihi: 15.12.2023]

HAWDON James vd. (2020). *Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment*, American Journal of Criminal Justice.

HOUSE REPORT, Review of the Unauthorized Disclosures of Former National Security Agency Contractor *Edward Snowden, United States, Congress House Permanent Select Committee on Intelligence*, (15). https://www.congress.gov/congressional-report/114th-congress/house-report/891/1?s=1&r=20 [Erişim Tarihi: 10.12.2023]

HYVÄRINEN, Noora. (2015). *The Dukes: 7 Years of Russian Cyber-Espionage*, "F-Secure" https://blog.f-secure.com/the-dukes-7-years-of-russian-cyber-espionage/

JENKINS, Ryan (2013). "Is Stuxnet PhysİcaI? Does It Matter?" *Journal of Military Ethics*, 12:1, 68-79

JOHNSON, Kevin (2021). *U.S. Formally Links Russia to Massive 'Ongoing' Cyber Attack; Scope of Hacking Unclear*. https://www.usatoday.com/story/news/politics/2021/01/05/u-s-formally-links-russia-massive-cyberattack-hack-ongoing/6552803002/ [Erişim Tarihi:17.10.2023]

JONES, Sam (2014) "Cyber Snake Plagues Ukraine Networks," Financial Times. https://www.ft.com/content/615c29ba-a614-11e3-8a2a-00144feab7de [Erişim Tarihi: 12.12.2023]

KILLCRECE, Georgia vd. (2003). *State of the Practice of Computer Security Incident Response Teams(CSIRTs)*, Networked Systems Survivability.

KOBAYASHI, Bruce (2016). "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods", *Supreme Court Economic Review*, 14.

LAMBETH, Benjamin S. (1986). "The Soviet Union and the Strategic Defense Initiative: Preliminary Finding and Impressions", *The Rand Cooperation*.

LILLY, Bilyana, CHERAVITCH, Joe,(2020). "The Past, Present and Future of Russia's Cyber Strategy and Forces", *12th International Conference on Cyber Conflict*.

LINDSAY, Jon R. (2014). "The Impact of China on Cybersecurity: Fiction and Friction", *International Security*, 38(3).

MINTO-COY, Indianna D., HENLIN, M. Georgia Gibson (2018). The Development of *Cybersecurity Policy and Legislative Landscape in Latin America and Caribbean States*, Michelle Moore ed., Cybersecurity Breaches and Issues Surrounding Online Threat Protection, US: IGI Global.

MORGAN, Steve (2020). "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021"https://cybersecurityventures.com/annual-cybercrime-report-2020/ [Erişim Tarihi: 15.11.2023]

NEW WIRES, (2023). https://www.france24.com/en/europe/20231207-uk-us-accuse-russia-of-cyber-campaign-against-top-politicians [Erişim Tarihi: 15.01.2024]

NSA (2023). "Hunting Russian Intelligence "Snake" Malware", 9 Mayıs, NSA Report.

NYE, Joseph S. Jr. (2011). "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, 5(4).

NYE, Joseph S. Jr. (2011). *The Future of Power*, NY: Public Affairs.

PEMPEL, Kacper. (2022), "Rusya'dan ABD'ye 'Ukrayna'nın Eliyle Siber Saldırı' Suçlaması" *Reuters* https://sputniknews.com.tr/20221025/rusyadan-abdye-ukraynanin-eliyle-siber-saldiri-suclamasi-1062676021.html [Erişim Tarihi: 15.01.2024]

PEREZ, Evan, PROKUPECZ, Shimon. (2015) How the U.S. thinks Russians hacked the White House. https://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html [Erişim Tarihi: 07.07.2023]

POOLE, Walter S. (2013). Adapting to Flexible Response 1960-1968 *Vol. 2*, Washington: Historical Office, Office of the Secretary of Defense

RID, Thomas (2013), "Cyber War Will Not Take Place", NY: Oxford University.

SAAVEDRA, Boris. (2015). *Cybersecurity in Latin America and the Caribbean: The State of Readiness Fort He Defense of Cyberspace*, Center for Hemispheric Defense Studies.

SANGER David E. (2020). *Russian Hackers Broke Into Federal Agencies, U.S. Officials*

Suspect. https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html?action=click&module=RelatedLinks&pgtype=Article [ErişimTarihi 07.01.2024]

SANGER, David E.&PERLROTH, Nicole (2020). *More Hacking Attacks Found as Officials Warn of 'Grave Risk' to U.S. Government.* https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html [Erişim Tarihi 07.01.2024]

SCHMID, Jon. (2018). "Intelligence Innovation: Sputnik, the Soviet Threat, and Innovation in the US Intelligence Community" *Technology and the Intelligence Community: Challenges and Advances for the 21st Century*, 39-53

SHAD, Muhammad Riaz, (2018). "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions." *Policy Perspectives*, 15(2).

SINGER, P.W., FRIEDMAN, Allan (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*, NY: Oxford University Press.

SNYDER, C. (Ed.). (1986). "Star Wars and Nuclear Ideologies" *The Strategic Defense Debate: Can" Star Wars" Make Us Safe?* University of Pennsylvania Press.

STANDAGE, Tom (2017). The Crooked Timber of Humanity https://www.economist.com/1843/2017/10/05/the-crooked-timber-of-humanity [Erişim Tarihi:02.12.2023]

STEWART, Phil, (2011). *"Jim Wolf, Old Worm won't Die After 2008 Attack on Military*" https://www.reuters.com/article/us-usa-cybersecurity-wormidUSTRE75F5TB20110617 [Erişim Tarihi: 07.12.2023]

THE WHITE HOUSE, February (2003). "*The National Strategy to Secure Cyberspace"* https://nsarchive.gwu.edu/document/21412-document-16

TIDY, Joe (2022). "Rusya'nın Ukrayna'yı İşgali: Batı'yı En Çok Korkutan Kremlin Kaynaklı Üç Siber Saldırı Senaryosu" BBC. https://www.bbc.com/turkce/haberler-dunya-60846366 [Erişim Tarihi: 27.12.2023]

VEAZIE, Arnold K. (2003). *U.S. Strategy for Cyberspace, U.S. Army War College, Carlisle Barracks*, Pennsylvania.

WATNEY, Murdoch (2013) "Determining When Conduct in Cyberspace Constitutes Cyber Warfare in Terms of the International Law and Tallinn Manual on the International Law Applicable to Cyber Warfare: A Synopsis", *Digital Forensics and Cyber Crime Fifth International Conference*, Pavel Gladyshev vd.(ed.) ICDF2C 2013 Moscow, Russia, Revised Selected Papers,

YÖNAK, Rüya. (2017). 2016'da Gerçekleştirilen Siber Saldırılar https://www.bbc.com/turkce/haberler-38489376 [Erişim Tarihi: 15.12.2023]

ASKERİ HABERLEŞME SİSTEMLERİNDE TÜRKİYE: SİBER GÜVENLİK VE YERLİLEŞME

Elif GÜRDAL LİMON*

ORCID: 0000-0001-5110-6524

Özet

Askeri haberleşme sistemlerinde dijital yeniliklerin olması devletlere güç sağlayan yeni bir alan olmuştur. Diğer yandan bu dijital dünyada saldırı kaynağının belirsizliği gibi yeni tehditler de ortaya çıkmıştır. Bilginin çalınması, bozulması, değiştirilmesi gibi tehditler bunlardandır. Devletler için siber güç bu tür siber saldırıları bertaraf edebilmek için artık gerekli bir güç biçimi haline gelmiştir. Bu çalışmada Türkiye'deki askeri haberleşme sistemlerinin siber güvenliği konusu ele alınmıştır. Çalışmada askeri haberleşme sistemlerinin siber güvenliğinde iş birliğinin mi ya da devletlerin tekil önlemlerinin mi ön plana çıktığı araştırılmaktadır. Uluslararası iş birliği veya yerlileşme arasında Türkiye'nin tercihi incelenmiştir. Çalışma için askeri haberleşme konusunda savunma sanayi kuruluşlarıyla ve Milli Savunma Bakanlığıyla iletişime geçilmiştir. Bakanlıktan verilerin gizliliği nedeniyle soruların yanıtlanamayacağı yönünde dönüş alınmıştır. Bu yüzden uluslararası enstitü veri indeksleri, savunma sanayi şirketleri açık kaynak verileri, Türkiye Dijital Dönüşüm Ofisi projeleri ve yerli-yabancı açık kaynak verileri taranmıştır. Türkiye'nin siber güvenliğe ulusal güvenlik meselesi olarak yaklaştığı ve bu konudaki iş birliğini uluslararası aktörler arasında değil, çoğunlukla Türkiye içerisinde yerli firmalar ve kurumlar arasında gerçekleştirdiği görülmektedir. Türkiye'nin askeri siber güvenlik stratejisinin yerli siber güvenlik firmalarının sayısını arttırmak, askeri iletişim teknolojilerde yerli ve milli ürünlerin geliştirilip kullanımını sağlamak olduğu görülmektedir. Bu açıdan Türkiye'de siber güvenliğin askeri dijital teknolojilerinde yerlileşmeyi tetiklediği gözlemlenmektedir.

Anahtar Kelimeler: Siber Güvenlik, Siber Savaş, Askeri Haberleşme Sistemleri, Yerlileşme

TÜRKİYE'S MILITARY COMMUNICATION SYSTEMS: CYBER SECURITY AND INDIGENIZATION

Abstract

*Dr. Öğretim Üyesi, Department of International Relation, Gümüşhane University, Accessible via e-mail: elif.gurdal@gumushane.edu.tr

The presence of digital innovations in military communication systems has become a new field that empowers states. On the other hand, new threats such as the uncertainty of the attack source have emerged in this digital world. Threats such as theft, corruption, alteration of information are among them. For states, cyber power has now become a necessary form of power to thwart such cyber attacks. In this study, the issue of cyber security of military communication systems in Türkiye is discussed. The study investigates whether cooperation in the cyber security of military communication systems or individual measures of the states come to the fore. Türkiye's choice between international cooperation or indigenization has been examined. For the study, defense industry organizations and the Ministry of National Defense were contacted on military communications. A response was received from the Ministry that the questions could not be answered due to the confidentiality of the data. Therefore, international institute data indexes, open source data of defense industry companies, Türkiye's Digital Transformation Office projects and domestic and foreign open source data were scanned. It is seen that Türkiye approaches cyber security as a national security issue and cooperates on this issue not between international actors, but mostly between domestic companies and institutions within Türkiye. It is seen that Tirkiye's military cyber security strategy is to increase the number of domestic cyber security companies and to develop and use domestic and national products in military communication technologies. In this respect, it is observed that cyber security triggers the indigenization of military digital technologies in Türkiye.

Keywords: Cyber Security, Cyber War, Military Communication Systems, Indigenization

Giriş

Dijital dönüşüm başarılı kullanıldığı takdirde devletlere güç kazandırabilmektedir. Devletler teknolojiyi takip ederek diğer aktörlere oranla üstünlük sağlama niyetindedirler. İletişimde ve ulaşımda son teknolojiden diğer devletlere oranla gelişmiş şekilde yararlanmak bir üstünlük göstergesi olmaktadır. Gelişmiş bir teknoloji kullanabilen devletin bilimde daha üstün olduğu ve güç bakımından savunma, ekonomi veya siyasette bir etki faktörü yaratabileceği anlamına gelmektedir. Örneğin Aya iniş yapmak Soğuk Savaş'ta ABD ve SSCB arasındaki rekabette önemli bir güç göstergesiyken bu durum günümüzde yeniden canlanmış, Hindistan Çin'den sonra aya yumuşak iniş yapabilen dördüncü ülke olmuştur (Indian Space Research Organisation, 2023)

Devletlerin önemli bir güç kaynağı olan ordusu sürekli teknoloji ile revize edilerek güçlü tutulmaya çalışılmaktadır. Haberleşme sistemleri askeri birimlerin can damarıdır ve teknolojik gelişmeleri yakından takip eden en önemli alanlardandır. Askeri iletişimin başarılı dijital dönüşümü bir güç olduğu kadar bu iletişim ağının korunabilir olması da bir güç gerektirmektedir.

Uluslararası ilişkilerdeki güç rekabeti politik araçların çeşitlenmesi yüzünden yeni alanların eklenmesiyle çoklu bir boyutta yürütülmektedir. Bu konuda önemli bir etken olan dijital dönüşüm savaş alanlarının çeşitlenmesine ve güvenlik alanlarının artmasına neden olmaktadır. Siber tehditler her geçen gün artmakta, saldırı ve savunma yöntemlerindeki çeşitlilik, eşiği bilinmeyen yeni savunma harcamalarını doğurmaktadır. Siber tehditlere karşı bilgiyi korumak da ulusal güvenliğin sorumluluğunda olmaya başlamıştır.

Önemli bir güç olan bilgi dijitalleşmeyle birleşmiştir. Bunun yanı sıra yeni tehditler de doğmuştur. Bilginin çalınması, bozulması, değiştirilmesi gibi tehditler bunlardandır. Dijital ortamlardan bilginin korunması giderek zorlaşmıştır. Siber güvenlik ortamı devletlerin 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. Bu açıdan dijital dönüşümün askeri birimlerde gerçekleşmesi siber güvenliği bir kat daha önemli yapmaktadır.

Bu çalışma Türkiye'deki askeri haberleşme sistemlerinin siber güvenliği konusunu ele almıştır. Makalenin araştırma sorusu şudur: Askeri haberleşme sistemlerinin siber güvenliğinde iş birliği mi ya da devletlerin tekil önlemleri mi öne çıkmaktadır? Haberleşme bir çoklu veri alışverişi olduğundan iş birliğine çoğu zaman ihtiyaç duymaktadır. Ancak siber güvenliğin giderek ulusal güvenliğin önemli bir alanı haline gelmesiyle askeri haberleşme sistemlerinin işleyişinde kimi durumda devletler tekil tedbirlere zorlanmaktadır.

Türkiye stratejik konumu ve NATO üyesi olması bakımından önemli bir askeri güçtür. Bu stratejik konumu ve iş birliğinin bir sonucu olan NATO üyeliği düşünüldüğünde Türkiye'nin yerlileşme veya dışa açılım tercihlerindeki fark güce dönüşebilme potansiyeli taşıdığından diğer aktörleri ve onların seçimlerini etkileyebilecektir. Türkiye'nin askeri iletişiminin siber güvenliği daha önce çalışılmamıştır. Askeri haberleşme sistemleri üzerinden literatürde yeterli veri mevcut değildir. Bu kapsamda çalışma Türkiye'nin askeri dijitalleşmesi örneği üzerinden ele alınmıştır. Türkiye'de askeri birimlerin siber güvenliği incelenirken bir daraltma yapılmış ve askeri haberleşme sistemleri üzerinden bir analiz gerçekleştirilmiştir. Askeri araçların

dijital dönüşümü ve artık dijital destekli olan bu iletişim ağının güvenliği ele alınmıştır. Askeri bir konu olması bakımından verilerin büyük çoğunluğu gizlidir. Bu yüzdendir ki çalışmada veri elde etmede zorluklar yaşanmıştır.

Çalışma için askeri haberleşme konusunda Aselsan, Havelsan ve STM gibi kuruluşlarla, Milli Savunma Bakanlığı (MSB) ile iletişime geçilmiştir. Savunma Sanayi şirketleri dönüş yapmamış, MSB "verilerin gizliliği nedeniyle yanıtlanamayacağı" yönünde dönüş gelmiştir. NATO iletişim birimine sorular yöneltilmiş, sorular yanıtsız kalmıştır. Kurumlara yöneltilen ana sorular şunlardır: 1) Türkiye'nin askeri iletişimde Link-11 ve diğerlerinin NATO bünyesindeki siber güvelik sorumluluğu kime aittir? 2) Askeri haberleşme sistemlerinde yurtdışı sağlayıcısı olan ülkelerin hizmeti alan ülkelerin verilerinin güvenliği konusundaki etik davranışları nasıl belirlenmektedir? Çalışma; savunma sanayi kuruluşlarının açık kaynak verileri, uluslararası enstitü veri indeksler, konu hakkında literatür kitap ve makale kaynaklarından elde edilen verilerle oluşturulmuştur. Ayrıca siber güvenliği mühendislik gözüyle ele almamakta, siber güvenlik kavramını uluslararası güce etkisi bakımından yorumlamaktadır.

Çalışma bu giriş kısmı haricinde üç bölümden oluşmaktadır. İlk olarak siber güvenlik ve yerlileşme bölümünde Türkiye'nin siber güvenliği ulusal güvenlik meselesi olarak gördüğü vurgulanmıştır. Daha sonra askeri haberleşme sistemi ve yerlileşme bölümünde askeri haberleşme biçimine ve Türkiye'nin bu konudaki yerli teknoloji çalışmalarına değinilmiştir. Son olarak sonuç bölümünde elde edilen bulgular tartışılmıştır.

Siber Güvenlik ve Yerlileşme

Siber saldırıda amaç; veri çalmak yani casusluk, veri değiştirmek, veri eklemek, cihazın işlevsiz kalmasını sağlamak, cihazı kontrol etmek veya cihazda bilgileri karmaşıklaştırmak gibi sıralanabilir. Siber saldırıda veri değerli olduğundan veri güvenliği; gizlilik, bütünlük ve kullanılabilirlik üzerine sağlanmaktadır (Hunker, 2010, ss.1-13). Bunlar; veriyi zamanında iletebilme, veriyi olduğu gibi iletebilme, veriyi başkasına geçmeden iletebilme gibi önemli hususlardır.

Siber saldırıların planlanmış bir şekilde bir ülkeden diğer ülke hedefine yönelik yapılması bir savaş ortamını göstermektedir. Siber savaş dijital araçların saldırı ve savunma aracı olarak kullanıldığı devletlerarası bir saldırı-savunma faaliyetidir (Köker, 2021, s. 211). Elbette ki bu siber savaş ortamının diğer savaş ortamlarından en önemli farkı saldırı kaynağının belirlenememe ihtimalidir. Dijital ortam saldırılarının en önemli tehdit kaynaklarından biri

belirsiz çoklu saldırı kaynağıdır. Bu açıdan böylesi risklerle dolu uluslararası ortamda devletler siber güvenliğe her geçen gün daha da önem vermektedir. Bunun için protokoller, uluslararası anlaşmalar gibi iş birlikleri yaparken diğer yandan tekil anlamda kendi gücünü arttırmak için yatırımlar yapmakta, milli teknolojileri imkânlar dâhilinde arttırmaya çalışmaktadır.

Uluslararası iş birliği bağlamından bakıldığında, NATO daha 1998 yılında askeri güvenlik bakımından üyelerinin siber saldırılara karşı tedbirli olması gerektirdiğini dile getirmiştir. Tartışılan konulardan biri, örneğin, BM tüzüğüne göre "kuvvet kullanımı" veya "silahlı saldırı" tespiti olmadığından dolayı siber saldırıların barış zamanında yasal zorlama olarak görülüp konvansiyonel bir karşılığın verilememesidir (Greenberg vd. 1998, s.iii.). Bu açıdan zamanla hem uluslararası ilişkilerdeki savaş etkenleri konusunda hem de uluslararası hukuk bakımından usul düzenlemeleri ihtiyacı doğmuştur. Savunma konusundaki hassasiyeti NATO liderlerinin 2016 Varşova Zirvesindeki kararları da göstermektedir. NATO'nun bu zirvesi siber savaşı resmi olarak ele alan ilk uluslararası görüşmedir. Siber alanın bir savaş alanı olarak görülmesi de yine NATO'nun bu zirvesinde gerçekleşmiştir. Siber savaşın gündem olmasındaki etken NATO bünyesindeki siber saldırıların 2016'da bir önceki yıla oranla %60 artmasıdır (Robinson, 2017).

NATO üyeleri özellikle ne kadar bir harcamanın siber güvenliği sağlamakta yeterli olabileceğinden emin değildir. Ya da siber savaşta etik sınırlar nelerdir? (Cornish, 2017, s. 5). Bu belirsizlik savunma alanını giderek çeşitlendirmektedir. Çünkü diğer savaş ortamlarında en azından askeri personel, donanma gücü veya savaş uçakları gibi hesaplanabilen sert güç dayanakları, siber savaş ortamında sayısal verilere dökülemediğinden tehdit ve savunma harcaması hesaplamasını zorlaştırmaktadır.

Teknik beceri, kabiliyet ve bilgi siber savaşın bir silahı olduğundan caydırıcılık olarak gözle görülür maddi güç kapasiteleri değildir. Maddi bir güç göstergesi olarak hesaplaması zor olduğundan devletlerin ne kadar bir savunma harcaması ile siber güvenliklerini garanti altına alabilecekleri belirgin değildir. Savunma harcamasına dair ortalama bir eşiğin belirlenmesi zorlaşmaktadır. Bu belirsizlik içiresinde savunma harcaması olarak siber saldırı tiplerine yönelik yatırımlar yapmak özellikle son 10 yıldır öncellikli konular olmaya başlamıştır (Robinson, 2017). Kaynağı belirsiz ya da daha önce görülmemiş saldırı tiplerine karşı savunma sağlayabilen devletler siber saldırı yapabilme potansiyeline sahip aktörler olarak görülmelidir.

Siber savaşın bir savaş alanı olarak uluslararası anlamda kabul görmesiyle siber anlamda güvenlik eşiğinin belirgin olmamasına rağmen devletler farklı siber güvenlik refleksleri göstermektedir. Kimi devlet askeri sistemlerin dijital gelişmelerinde en son yeniliği takip edip siber ordular kurmakta, kimi devlet daha güçlü gördüğü devletle iş birliği yapmakta, kimi devlet yabancı güvenlik şirketleri ile protokoller imzalamakta, kimi devlet uluslararası örgütler çatısı altında siber güvenliği sağlamakta kimi devlet ise kendi milli ve yerli teknolojilerine sığınmaktadır (U. S. Cyber Command, 2023; BTK, 2023) En nihayetinde amaç olası siber saldırılara karşı acil bir koruma müdahalesi yapabilmektir.

Siber güçte, güçlü bir savunma setinin yanı sıra ikinci aşamadaki öncelik acil bir müdahale kabiliyeti geliştirilmesidir. Siber saldırıların anlık saldırılar olduğu düşünülürse karşılığının saldırı türünün ve niteliğinin ne olduğunun kısa sürede çözümlenerek verilmesi gerekmektedir. Saldırı türünün belirlenmesi savunma biçimini yönlendirecektir. Dolayısıyla savunma sistemi ve acil müdahale kabiliyeti siber savaşta askeri birimlerin öncelik sıralamasıdır. Bu da askeri birimlere yeni bir savaş ortamının eklendiğini göstermektedir. Bu savaş ortamında aşağıdaki gibi sorunlarla karşılaşılabilir.

Siber Savunmada Olası Sorunlar:

- Bilinmeyen düşman unsur
- Yeri belli olmayan düşman unsur
- Saldırı tipinin belirsizliği
- Savunmanın uygulanmasında bilgisizlik
- Acil müdahale ekibinin yeteneği
- Askeri yetenek dışı yeni kabiliyet ihtiyacı
- Hızlı karar alma
- Siber karşı saldırı kabiliyeti

Siber saldırı tek başına bir saldırı kuvveti olarak kullanılmaktan öte geleneksel yöntemleri destekleyici unsur olarak görülmektedir. Siber saldırı, saldırı ve kaşı saldırıdan ibaret değildir. Ayrıca saldırıya uğrayan taraf aynı saldırı türü, şekli ve zararı ile karşı saldırı yapamayabilir. Bu ya yeteneği ile ilgili bir durum olabilir ya da saldırıya uğradığı türde bilgiler saldırıyı yapanda bulunmayabilir. Örneğin devlet destekli bir siber korsan grubunun bir devletin belirli gizli askeri operasyon verilerini çalıp kamuoyuna paylaşması söz konusu olabilir. Aynı tür

gizli bir operasyon saldırıyı yapan kaynakta olmayabilir. Bu da saldırı ve karşı müdahale farklılaşmasını gösterebilir. Dolayısıyla siber saldırı diğer savaş türlerini destekleyici bir güç olabilir. İlerleyen aşamada devletler gerek Soğuk Savaş konsepti olan caydırıcılık durumunu siber savaşta sağlayabilmek, gerekse siber savunmada tam kabiliyete erişmek gibi bazı aşamalardan sonra siber savaşta ilk saldırı kabiliyetine geçmeye çalışacaklardır (Haggman, 2018).

Devletler siber saldırılara karşı hazırlık için siber ordular oluşturmaktadır. Kimi devlet siber güvenlik sorumluluğunu askeri bir yetenek olarak görmekte, dijital savaş yetenekleri askeri bir yetenek olarak düşünülüp entegre edilmektedir. Bu da siber güvenliğin sorumluluğunu devletlerin askeri birimlerine yüklemektedir ve siber güvenlik askeri bir yetenek olarak algılanmaktadır. Bu yüzden devletlerin oluşturdukları siber ordular Savunma Bakanlıklarına bağlı birimler olarak görülmektedir. Örneğin Avrupa Birliği siber güvenliği askeri birimlerin iş birliklerine atıf yaparak tanımlamaktadır. Siber savunma askeri yeteneklere göre tanımlanmıştır (European Defence Agency, 2023). Kimi devlet ise her kurumun ayrı bir siber birimini oluşturarak siber güvenliği sağlamaya çalışmaktadır. Türkiye bu konuya karma şekilde bakmaktadır.

Siber güvenliğin önemin artmasıyla, örneğin Türkiye'de, Türk Silahlı Kuvvetleri'nin Siber Savunma Komutanlığı oluşturulmuştur. 2013 yılında bu kurum başkanlıktan komutanlığa dönüştürülmüştür. Siber Savunma Komutanlığı'nın Siber Savunma Merkezi (SİSAMER) ise bir askeri birlik niteliğinde olmasa da askeri bir birim olarak yürütülen projedir (Anadolu Ajans, 22.11.2021). Askeri manada bir savunma sağlayabilmek, milli yazılımların üretilmesi hatta siber saldırı yapabilen bir ülke konumuna gelmek amaçlanmaktadır (STM, 01.12.2022). Ayrıca MSB'nin Muhabere ve Bilgi Sistem Dairesi Başkanlığına bağlı Siber Güvenlik Daire Başkanlığı da vardır (MSB, 2023).

Diğer devletler de benzer şekilde askeri birimlerindeki siber savunma unsurlarını ve sivil siber savunma birimlerini ayrı oluşturmaktadır. Örneğin Çin Halk Kurtuluş Ordusu'nun Ünite 61398 olarak ortaya çıkan siber ordusu ilk etapta gizli olmuştur (Shen, 2019). Daha sonra bazı saldırıların arkasındaki devlet destekli birim olarak keşfedilmiştir (Sanger vd. 2013). Hatta Çin Halk Kurtuluş Ordusu'ndaki bu birim çalışanları ABD tarafından ABD ve Çin arasındaki siber savaştan sorumlu olarak görülmüştür (Hvistendahl, 2016). İsrail'in Birim 8200 oluşumu buna benzer askeri kuvvetlere bağlı radyo dalgası, GPS veya dijital iletişim konulu güvenlik birimidir. Askeri İstihbarat Başkanlığı'nın alt birimlerinde yer alan en büyük askeri siber

birimdir. Birim 8200 ana bilgi toplama birimidir. Bölgesel bir komutanlığa değil, doğrudan Genelkurmay Başkanı'na bağlıdır (Israel Defense Forces, 29.12.202).

Askeri birimlerdeki siber ordular genel olarak gizli tutulmaya çalışılmış ya da faaliyetler kamuoyu ile paylaşılmamıştır. Diğer yandan askeri alan dışı siber güvenlik konuları için kurumsallaşmalar da olmuştur. Güç mesajı vermek ve şeffaflık algısı için bu alanda oluşturulan siber güvenlik birimleri ise aksine tanıtılmıştır. Askeri birimler dışındaki devlet kurumlarında kurulan siber güvenlik birimleri yine de ordu sıfatı ile tanıtılmıştır. Böylelikle askeri birimlere bağlı olmayan resmi bir ordu anlayışını ilk kez siber alanda görmekteyiz. Örneğin Türkiye'nin siber ordu sıfatı ile kurulan ilk birimi 2017'de Ulaştırma ve Alt Yapı Bakanlığına bağlı oluşturulmuştur (BTK, 15 Mart 2017). Gerçek bir ordu niteliğinde olmayan bu birim; kurumlara yönelik siber saldırılara acil karşılık vermek, kritik altyapıların korunmasını sağlamak gibi amaçlar taşımaktadır.

Türkiye'de siber güvenlikle ilgili eylem planlarının hazırlanması ve uygulaması da Ulaştırma ve Alt Yapı Bakanlığınca yapılmıştır. 2013'te ilk ulusal siber güvenlik stratejisi ve eylem planı yayımlanmıştır. İkincisi 2016'da ve üçüncüsü 2020'de yayımlanmıştır (2013-2014 Eylem Planı; 2016-2019 Ulusal Siber Güvenlik Stratejisi; Ulusal Siber Güvenlik Stratejisi 2020-2023). Bu belgelerle Türkiye siber güvenliği ulusal güvenliğinin bir boyutu olarak görmektedir. Diğer yandan askeri birimlerin siber güvenliğinin sivil bir bakanlığın sorumluluğunda olması yeterli bir ulusal güvenlik hamlesi olmayacaktır. Bundan dolayı Türkiye, kurumlar arası iş birliği stratejisini uygulamaktadır.

Türkiye'nin siber güvenlik konusundaki karma kurumsallaşma çabası siber güvenlik meselesinin sorumluluğunun tek bir kurum üzerine bırakılamayacak kadar kapsamlı olmasından kaynaklanmaktadır. 2018 yılından itibaren uygulamaya koymaya çalıştığı sivil ve askeri kurumlar ile yerli firmalar iş birliğinden oluşan bir strateji yürütmektedir. Böylesi bir yaklaşım 2021'de ise Cumhurbaşkanlığı Savunma Sanayii Başkanlığı ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi arasında protokol imzalanarak resmiyete dökülmüştür (Dijital Dönüşüm Ofisi, 26 Temmuz 2023). Siber güvenlik tek bir alana ait güvenlik mesele olmamasından dolayı disiplinler arası bir konuyu oluşturmaktadır. 2021'de protokolü imzalanan Siber Güvenlik Kümelenmesi oluşumu böylesine bir iş birliği sonucunda ortaya çıkmıştır. Savunma Sanayii Başkanlığı ve Dijital Dönüşüm Ofisi Başkanlığı tarafından desteklenen ve SSTEK A.Ş. (Savunma Sanayi Teknolojileri A.Ş.) tarafından yürütülen bir projedir (Dijital Dönüşüm Ofisi, 2023). Böylelikle savunma sanayii ile iletişim teknolojileri kurumları birada görülmektedir. Aselsan, Havelsan gibi savunma sanayi şirketlerinin yanı sıra

siber güvenlik şirketleri de bu kümelenmenin içindedir. Bu oluşumların hepsi siber güvenliğe yerlileşme ile karşılık vermektedir. Örneğin Aselsan'ın son yıllardaki verilerine bakıldığında silah üretiminde millileşen ürün sayısının arttığı görülecektir (SavunmaSanayiST, 2022).

Siber Güvenlik Kümelenmesi projesinde yerli firmalar yurt içi siber güvenlikte kullanım bakımından desteklenirken yurt dışı rekabeti de desteklenmektedir. Siber Güvenlik Kümelenmesi projesinde pazara erişim, inovasyon, yeteneğe erişim, etkileşim ve teknolojik üstünlük gibi ana faaliyetler vardır (Dijital Dönüşüm Ofisi, 26.07.2023). Proje ile yerli firmaları ihraç edilebilir bir kapasiteye getirmek ve rekabet edebilir bir seviyede tutmak hedeflenmektedir. Bu yüzden ithalat odaklı değil ihracat odaklı bir eğilim yani yerlileşme görülmektedir.

Türkiye yerli ürünlere verdiği önemi diğer projelere de yansıtmaktadır. Yerli ve Millî Siber Güvenlik Ürünlerinin Kullanımının Yaygınlaştırılması Koordinasyon Grubu bunlardandır. Bu platform Dijital Dönüşüm Ofisi Başkanlığı, Sanayi ve Teknoloji Bakanlığı, Savunma Sanayi Başkanlığı, Strateji ve Bütçe Başkanlığı, Devlet Malzeme Ofisi ve Kamu İhale Kurumu öncülüğünde 2021 yılında oluşturulmuştur (Dijital Dönüşüm Ofisi, 02.04.2023). Böylelikle siber güvenlik için yerli ürünlere güvenilebileceği ve onların teknolojik olarak gelişimleri devlet tarafından desteklenmesi gerektiği düşünülmektedir.

Türkiye siber güvenliği ulusal güvenlik meselesi olarak görmektedir ve bu konudaki iş birliğini uluslararası aktörler arasında değil Türkiye içerisinde yerli firmalar ve kurumlar arasında gerçekleştirmektedir. Amaçlardan biri de Türkiye'deki siber güvenlik firmalarının sayısını arttırmaktadır. Yerli ve milli siber güvenlik ürünlerinin geliştirilmesi ve kullanımının yaygınlaştırılması Türkiye'nin siber güvenlikte ana hedefidir. İş birliği yerli ve milli firmalar arasında arttırılmak istenmektedir. Ayrıca Türkiye'de kurumların siber güvenliğinde yerli yazılım ürünlerinin kullanımı arttırılmak istenmektedir. Siber güvenlik alanı, ulusal güvenliğin dış tehditlere karşı güvence altına alınabilmesi için uluslararası iş birliklerinden yerlileşmeye doğru gidilen önemli alanlardan olduğunu göstermektedir.

Askeri Haberleşme Sistemi ve Yerlileşme

Askeri haberleşme kara, hava ve deniz alanına yönelik tasarlanmış haberleşme sistemleri ile bunların arasında kesintisiz ve güvenli haberleşmedir. Askeri komuta ve kontrolün sağlanabilmesi için gerekmektedir. Bunlar için etkin personel, donanım ve belirli protokoller gerekmektedir. İletişimin güvenliği için korunaklı-gizli ve sağlıklı olması gerekmektedir. Bunun için geliştirilen sivil ortama kapalı iletişim ağları mevcuttur (Havelsan, 2023).

Günümüzde, örneğin, savaş yönetim sistemleri önemli askeri teknoloji gelişmelerindendir. Savaş yönetim sistemleri ile senkronize savunma, saldırı ve kontrol gibi fonksiyonlar dijital ortamda gerçekleştirilebilir. Hızlı karar alıcılık güvenli ve sağlıklı bir iletişim ortamında hızlı müdahaleye dönüşebilecektir. Siber güvenliğin önemli bir savunma konusu olmasıyla buradaki iletişim verilerinin sağlıklı aktarılabilmesi, bilginin korunması veya gizlenmesi önemli olmaktadır. Bu süreçte savaş yönetimi sağlanırken bu veri akışının sağlandığı askeri iletişimde güvenlik istikrarı esastır. Bu alanda da yeni teknoloji uygulamalarına geçilmiştir. Böylelikle tarihte istihbarat açısından en riskli konulardan olan savaş alanlarındaki iletişim konusu radyo ve dijital iletişim tabanı ile kolaylaşırken diğer yandan da karmaşıklaşmıştır. Çünkü dijital iletişim teknikleri güvenliğinin sağlanması gereken yeni tehditleri de doğurmaktadır.

Askeri birimlerde çok sayıda farklı platformun haberleşmesi gerekmektedir. Bunun için özel korumalı ağlar mevcuttur. Taktik Data Link sistemleri askeri haberleşme için garanti koşulları olan iletişim servisleridir. Birlikte çalışılabilirlik bakımından örneğin NATO üyelerinin iş birliklerindeki askeri iletişimde kullanılmaktadır. Ayrıca bunlar ulusal askeri iletişimde özel protokoller ile dönüştürülmektedir (Havelsan, 2023). Örneğin yerli üretim bir askeri sistem geliştirilirse, bu sistemin diğer platformlarla iletişimini sağlayacak ağ yerli olmayabilir. Bu NATO ağları ile birlikte çalışabilir olduğunu göstermektedir. Burada NATO müttefikleri arasında kullanılan ağlar dönüştürülerek kullanılacaktır. Bu ağların kullanabiliyor olması NATO müttefikleri için bir anlam ifadede ederken yine de, üretilebilen yerli sistemlerin ağlarının da yerli olması devletlerin ana hedeflerindendir. Dolayısıyla haberleşmedeki riskler bakımından ülkeler başarabildikleri takdirde milli Taktik Data Link sistemlerine yönelmektedir.

Artık kriptolanmış ve elektronik savaş konusunda dayanıklı ağlara ihtiyaç duyulmuştur. Zira bilginin anlık paylaşılması yeni çatışma alanlarında üstünlük için önemlidir. Link-16 bu sistemlerden biridir. Tespiti ve hasara uğraması zorlaşan iletişim ağlarındandır. Bunun için Link-16 hem kriz hem barış hem de savaş ortamlarında kullanılabilmektedir (Tuğcu & Gürel, 2012).

Taktik Data Linklerin işleyişini daha açık aktarmak gerekirse radarlar üzerinden örnek verilebilir. Genel itibariyle bir devletin radarların erişemediği noktada radara erişen diğer NATO üyesi devletin bu radar verilerini, radar verilerine erişemeyene göndermesi ile sağlanır. Verileri alan devlet sanki kendi radar tespiti yapmış gibi işlem yapar ve orada bir düşman

unsur varsa gerekli tedbiri alır. Bu Link-16'nın örnek işleyiş biçimidir (Asenstorfer vd., 2004).

Önceden kullanılan Link-1'in ardından kullanılan Link-11 deniz bağlantılı dost unsurlar arası iletişimi sağlayan ağ bağlantısıdır. Link-1, Link-11, Link-22 ve ardından geliştirilen Link-16 NATO'nun ortak veri paylaşım linkleridir (Göken & Atak, 2022, s. 170). Link-16, bilgisayarlar arası bilgi paylaşımı için kullanılmaktadır. ABD merkezli ve NATO için geliştirilen bir ağdır (Thinktech STM, Aralık 2015). Link-16, NATO'nun askeri teçhizat bakımından Standardizasyon Anlaşması STANAG'ın da dijital parçasıdır. 2016 yılından itibaren NATO'nın asli linki olarak kullanılmaktadır (NATO Standardization Agency, 2023).

Saldırı konumu, savunma konumu, birlik mühimmat miktarları, birliklerin GPS konumları, saldırının veya savunmanın şekli, zamanı gibi oldukça önemli bilgiler bu ağ üzerinden komuta edilip ve personel arasındaki irtibatta aktarılmaktadır. Savaş şekli, güvenlik konusu veya bu konularda alınan kararların eyleme dökülebilmesindeki koordine buradan yürütülmektedir. Bu bilgilerin güvenliği ise elbette ki gizlilik bakımından gerekli ve önceliklidir.

Savaş yönetimi için gözetleme, tespit, otomatik yönlendirme ve komuta kontrol gibi faaliyetler yapılırken, buradan elde edilen verilerin diğer birimlere ve yabancı ülke dost birliklere aktarılması da gerekli olacaktır. Bunun için ise platformlar arası ağ bağlantı kabiliyeti olmalıdır. Entegre Çoklu Veri Link sistemleri bu noktada önemlidir. Örneğin, Türk Savaş Yönetim Sistemi ADVENT ağ destekli kabiliyetle tüm konsollardan erişilebilen tam bütünleşik Link-11, Link-16, Link-22 ağ kapasitesine sahiptir (Havelsan, 2023).

Günümüzde güvenlik risklerinin bertaraf edilmesi için askeri iletişimi daha korunaklı yapabilme çalışmaları yoğunlaşmıştır. Askeri iletişimin güvenli ve dijital tabanlı olması için neler yapılabileceğine dair mühendislik çalışmaları yapılmaktadır. Örneğin Taktik Data Linklerin web hizmetlerinde kullanılabilirliğini güvenli sağlama yolları aranmaktadır. Hatta NATO, ağ destekli yetenek konusunda dönüşüm projesi benimsemiştir (Lund vd., 2010). Bu da artık disiplinler arası çalışmaların artışında bir itici unsur olmuştur. Askeri personellerin mühendislik yeteneği geliştirmesi bu açıdan artan bir ihtiyaçtır. Askeri personel saha yönetimine ek olarak dijital kabiliyet konusunda da yetenek geliştirmeye başlamıştır.

Siber savaş artık kabul görmüş bir savaş boyutu olduğundan milli ağ iletişim bağlantılarının NATO linklerine ek olarak tasarlanması bu savaş ortamında savunmacı bir güvenlik tedbiridir. NATO dışındaki bazı ülkeler zaten bu konuda milli Data Link Sistemlerine yer

vermektedir. Güney Afrika'nın Link-Za, İsrail'in Smart Data Link (SDL), Japonya'nın Milli Data Link, Brezilya'nın Link-BR2, Çin'in JSIDLS (Joint Service Integrated Data Link System), Hindistan'ın Link-II ağları bunlardandır (Smith & Venter, 8-10 Kasım 2011; Doğru, Mayıs 2019). Bu açıdan Türk Silahlı Kuvvetlerinin de harekât yapma kabiliyetini ve etkinliğini artırması için teknoloji bakımından dışa bağımlılığı azaltması kritik bir öneme sahiptir. Türkiye ilk etapta NATO ortak Taktik Data Link üzerinden savaş yönetim sistemlerinde millileşmeye gitmiş ardından buna ek olarak Taktik Data Link konusunda da bir milli ağa yönelmiştir.

2019 yılı sonrası Havelsan'ın GENESİS savaş yönetim sistemi uzantısı olan milli Advent savaş yönetim sistemi ile tam bütünleşik Taktik Data Linkleri Link-11, Link-16 ve Link-22 üzerinden iletişim sağlanmaktadır (Havelsan, 2023). Böylelikle, NATO ortak Taktik Data Linklerine uyarlanabilir milli savaş yönetim sistemleri tasarlanmıştır. NATO Taktik Data Linki olan Link-16 üzerinden iletişim çalışmaları Türk savunma sanayi aktörlerince ele alınmıştır. Hatta, Havelsan savaş yönetim sistemi ile GENESİS; Milsoft, Çavlist; Meteksan Taktik Data Link ile KEMENT projeleri yapılmıştır (Havelsan, 2023; Meteksan, 2023; Eldem, 2015). KEMENT projesi Meteksan yükleniciliğinde Tübitak, Roketsan, Milsoft ve Hava Komutanlığı desteği ile sağlanmıştır. Hava-hava ve hava-kara sistemlerinde bir milli link projesidir. Milli donanım/yazılım kripto fonksiyonu ile Türkiye'nin ilk Milli Taktik Data Linkidir (Meteksan, 2023).

Yine 2019 yılında askeri komuta merkezleri arasındaki bu Taktik Data Linklerinde yaptığı çalışmalar ile MİLSOFT NATO Taktik Data Linkleri olan Link-11, Link-22, Link-16'nın yerlileştirme çalışması yapmıştır. Milli olan ve Link-M olarak isimlendirilen bu link Türkiye'de üretilen milli telsiz, modem ve kripto sistemleriyle görev yapabilecektir. Yani Link-M, askeri platformlar arasında milli linkle oluşturulan bir ağın kullanılmasına imkân verecektir. Bu linkin taşıdığı ilk test mesajı ise "Merhaba tarihi an" olmuştur (TRT, 10.01.2019). Yine de NATO üzerinden bahsi geçen linklerin kullanımı devam etmekte; kara, hava ve deniz/ denizaltı gibi alanlardaki iletişim için farklı ağlar kullanılmaktadır.

NATO üyesi ülkelerin savunma sanayi şirketleri Taktik Data Link geliştirmeleri yaparken bunları NATO ülkeleri arasında birlikte çalışabilirliğini tescillenmesi gerekmektedir. NATO tatbikatlarının amacı özellikle bu tür yenilikçi projelerin birlikte çalışabilirliğinin test edildiği eylemler de olmaktadır. Örneğin Türkiye MİLSOFT'un Mil-DLP NATO Link-11, Link-22, Link-16'nın yeteneklerine sahip olurken NATO üyesi olmayanlar için de Link-M üzerinden ve Mil-NET yerli linki üzerinden çözümleme sağlanmaktadır (MİLSOFT, 2023).

Taktik Data Linklerde dışa bağımlılığı azaltma girişimleri yine bilimsel çalışmalarla güvenli bir askeri iletişim hedefi ile desteklenmektedir. Mevcut kullanılan Link-1, Link-11, Link-22, Link-16 mesaj formatı veya menzil uzatma gibi analiz ihtiyaçları doğmuştur (Direskeneli vd., 2016). Bu süreçte hem dışa bağımlılığı azaltmak hem de siber saldırılarda korunaklı olmak için milli geliştiricilere duyulan ihtiyaç arttırmıştır.

Dijital tabanlı ürün ve hizmetlerde siber güvenilirlik uluslararası risk konusu olmaktadır. Bilindiği üzere Türkiye S-400 krizinin nedenlerinden biri buna benzer bir sorundur. S-400 konusunun tartışma konularından birisi F-35'ler ile birlikte çalışabilirlik sağlamasıdır. NATO cihazları ile Rus cihazlarının birlikte çalışabilirliği veri güvenliği bakımından tartışmaya açılmıştır. NATO üyesi olan Türkiye'nin Rus yapımı S-400 alımı Türkiye'ye hava savunma planlamasında bir katkı sunabilirken tam bir kalkan rolü de sunmayabilecektir. Çünkü S-400 NATO'nun yeteneklerine entegre edilemeyecek ve NATO'nun kullandığı Taktik Data Linklerden yararlanmayacaktır. Bu da F-35'ler ile S-400'lerin aynı Taktik Data Linki kullanmayacağı anlamına gelmektedir (Kasapoğlu, 2017, ss.1-4).

Askeri haberleşme konusunda Taktik Data Linklerin güvenliği bir savaş konusudur. Güvenlik, elektronik savaş koruma teknikleriyle sağlanmaktadır. Bilgi güvenliği ise çoğunlukla veri kriptolaması ile yapılmaktadır. Taktik Data Linklere karıştırma denilen saldırılar olabilir. Saldırıya uğrayan platformun işlevi engellenebilir. Yanlış bilgilerle aldatılma veya tasarlanmış ağ operasyonunun başarısızlığa uğrama durumları söz konusu olabilecektir. Örneğin keylogger denilen virüsler bu tür saldırılarda riskli siber saldırılardır. Saldırısı yapılan cihazın eylemlerini gizlice takip eden yazılımlardır. Aslında bu gizli bir gözetleme olup dijitalleşmiş askeri sistemlerin platform komutalarını etkileyebilir (Direskeneli, vd., 2016).

Askeri haberleşmede iş birliği NATO bünyesinde olduğu gibi farklı siber konuları da ortaya çıkarmıştır. Örneğin, NATO Link-16 gibi ortak kullanım alanları veri alışverişindeki stratejik alışverişte kullanılmaktadır. Diğer yandan devletler tekil olarak güvenlik tedbirlerini en üst seviyede tutmak zorundadırlar. Her ne kadar NATO'nun kuruluş felsefesi birlik ve ortak hareket olması ve bunun anlaşmalarla teyit edilmesi olsa da elbette ki devletler askeri güvenliklerini doğrudan uluslararası organizasyonlara bırakmamaktadır. Her devlet uluslararası arenada bir güç unsuru olabilmek için olası riskleri hesaplamak ve kurumlarının güvenliğini dış bağımlılık olmadan sağlayabilir kapasiteye getirmek durumundadır. Siber savaştaki savunma riskleri de bunlar arasındadır. Dolayısıyla NATO dışında milli linklerin sağlanması güç mücadelesinin bir parçasıdır. Bu konuda da Türkiye'nin askeri dijitalleşmede

uluslararası sistemde denge sağlayıcı aktör olma eğiliminde olduğu görülmektedir. Yazılımda ve iletişim ağlarında millileşme projeleri bunun göstergesidir. Askeri siber güvenlik konusunda Türkiye'nin tavrı, teoriden pratiğe bakıldığında, anarşik uluslararası ilişkiler doğasında liberal bir uluslararası karşılıklı bağımlılıktan ziyade saldırı ve savunma ikileminde yapısal anlamda düşünülmesi gereken milli bir savunma alanı oluşturan bir reflekstir. Bu refleks yerlileşme yönelimindedir.

Sonuç ve Tartışma

Siber savaşta saldırı kaynağının belirlenmesi geleneksel savaşlar kadar net değildir. Bu durum devletlerin çatışmacı ortamında uluslararası iş birliğinin sorun çözücü rolünü etkileyebilir. Siber saldırıların tek başına bir saldırı kuvveti olarak kullanılmasından ziyade geleneksel yöntemleri destekleyici unsurlar olarak kullanıldığında toplam tahrip gücü daha yüksek olmaya başlamıştır.

İletişim ağında veri alışverişi bir iş birliği ortamını zorunlu kılmıştır. Örneğin NATO üyesi ülkelerin kullanmış oldukları Taktik Data Linklerin oluşumu iş birliğine dayalıdır. Bunlar belirli güvenlik garantilerine sahiptirler. Bu bağlantılar arası işlev imkânı belirli protokole tabidir. Yine de siber savaşta bu ağlar üzerinden çalma, yönlendirme, dinleme gibi dijital bir casusluk durumunun olmama garantisi yoktur. Çünkü saldırı kaynağının tespit edilmesindeki zorluk diğer savaş alanlarına göre siber savaşta yüksektir.

Ağ destekli savaş Türkiye açısından şimdiye kadar NATO üyeliği ile birlikte yürütülen bir alan olmuştur. NATO bünyesindeki ağ tabanı halen kullanılmaktadır. Diğer yandan Türkiye, siber savaşta ilk etapta savunma bakımından bir alan oluşturmak için askeri birimlerinin güvenliğini millileşmeye giderek sağlamak istemiştir. Bu savaş yönetim sistemlerindeki millileşme ve yerlileşme projelerinden ve askeri iletişim ağındaki milli ağ bağlantıları projelerinden anlaşılmaktadır. Ayrıca bu sistem tasarımlarında işlevsellik sağlandıktan sonra öncelik kriptolama gibi dış tehditlere karşı korumaya odaklanmaktır.

Siber alanda askeri anlamdaki iş birlikleri olabildiğince sınırlı tutulmaya çalışılmaktadır. Örneğin milli sistemlerin değeri, keşfedilmemiş saldırılara en azından hazırlanabilmek adına daha hâkim olunabilecek bir savunma mekanizması olabilmesindedir. Yerli ve milli sistemler bu tür saldırılarda karşı müdahale için daha fazla hâkimiyet sağlayacaktır. Dijital askeri sistemlerin dış kaynaklı tedarikinde en önemli sorun yazılım güvenliğidir. Bu da veri gizliliği olan alanlarda etik sorununu doğurmakta, uluslararası güç rekabeti düşünüldüğünde karşılıklı bağımlılığı pek de mümkün yapmamaktadır.

Siber saldırıların yeni bir savaş boyutunu tanımlaması ve bu savaşta yetersiz kalanların denge kurmakta zorlanacağı bir ortamda siber savunma diğer ülkelerinin teknolojilerine bırakılamayacak kadar belirleyicidir. Uluslararası anlamda güç dengesinin sağlanabilmesi için siber savaş açısından askeri haberleşme sistemleri gibi askeri teknolojilerin millileşmesi gerekmektedir. Bu perspektifte siber güvenlik konusunda iş birliklerinin ve devletlerin siber silah konusunda kabiliyetlerinin birbirine benzer hale getirilmesinin ana nedeni bir denge yaratma gayesidir. Örneğin, NATO'nun askeri haberleşme sistemi üzerinden STANAG'a uyumlu dijital sistemler geliştirmesi ve üyelerin bunlardan ortak yararlanma girişimleri NATO dışı devletleri dengeleyebilmektedir. NATO üyesi olmayan devletlerin de kendine has milli askeri haberleşme sistemleri geliştirdikleri görülmektedir. Türkiye'nin hem NATO ile hem de NATO dışında ayrı bir askeri haberleşme sistemi geliştirebiliyor olması iç dengesini sağlamayı rasyonel bir seçim olarak gördüğü ve güç dengesinin gerekli olduğuna inandığı anlamına gelmektedir.

Askeri siber güvenlik konusunda Türkiye uluslararası firmalarla iş birliğini azaltma eğilimindedir. Askeri alandaki siber güvenliğin önemi arttıkça Türkiye'nin yerli firmalara ve kurumlar arası iş birliğine yönelimi de artmaktadır. Bu açıdan askeri haberleşme teknolojilerinde yerli firmaların desteklenmesinde artış vardır. Askeri teknolojilerin siber güvenliğinde uluslararası iş birliğinden ziyade devlet içi kurumlar arası iş birliği stratejisi izlenmektedir. Dolayısıyla siber güvenliğin askeri teknolojilerde yerlileşmeyi tetiklediği söylenebilir.

Kaynakça

Anadolu Ajans (2021, 22 Kasım). *Milli siber güvenlik zirvesi başladı*. https://www.aa.com.tr/tr/bilim-teknoloji/milli-siber-guvenlik-zirvesi-basladi/2427205

Asenstorfer, J., Cox, T. &Wilksch, D. (2004). *Tactical data link systems and the Australian Defence Force (ADF): Technology developments and interoperability issues*. Australia: DSTO Information Sciences Laboratory

Bilgi Teknolojileri ve İletişim Kurumu (2017, 15 Mart). *Türkiye'nin ilk siber ordusu hazır*. https://www.btk.gov.tr/haberler/turkiye-nin-ilk-siber-ordusu-hazir

Bilgi Teknolojileri ve İletişim Kurumu. (2013). *Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı*. https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf.

Cornish, Paul (2017). Deterrence and the ethics of cyber conflict, Ed. Marriarosaria Taddeo and Ludovica Glorioso. Ethics and policies for cyber operations: A NATO cooperative cyber defence center of excellence ınitiative, Springer, Swetzerland.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023). *Türkiye siber güvenlik kümelenmesi* https://siberkume.org.tr/hakkimizda.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023, 2 Nisan). *Yerli Siber Güvenlik Ürünlerinin Yaygınlaştırılması Platformu.* https://cbddo.gov.tr/projeler/siber-platform/

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023, 26 Temmuz). *Siber kümelenme projesi.* https://cbddo.gov.tr/projeler/siber-kumelenme/

Direskeneli, A., İnci, A. & Başkuş, B. (2016). *Taktik Data Link analizine yönelik simülasyon ihtiyacı ve sağlaması gereken işlevleri*, SAVTEK 2016 Conference, Ankara.

Doğru, S. (Mayıs 2019). NATO ve koalisyon dışı ülkelere ait milli taktik data link sistemleri. *Trendanalizi STM*, 5-9.

Eldem, M. Oktay (2015). Askeri aviyonik sistemler ve modernizasyon (6). *TMMOB EMO Ankara Şubesi Haber Bülteni,* 2015/3, https://www.emo.org.tr/ekler/3e26879d0b269e8_ek.pdf?dergi=999

European Defence Agency (2023). Cyber, https://eda.europa.eu/what-we-do/capability-development/cyber.

Göken, Ç. & Atak, O. (2022). Veri linkleri, *Aselsan Dergi*, 111 (1), 170.

Greenberg, L. T, Goodman, S. E. & Soo Hoo, K. J. (1998). *Information warfare and international law*. National Defense University Press. http://www.dodccrp.org/files/Greenberg_Law.pdf.

Haggman, A. (2018). Cyber Deterrence Theory and Practise. In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security: Power and Technology. Intelligent Systems, Control and Automation: Science and Engineering, vol 93. Springer, Cham. https://doi.org/10.1007/978-3-319-75307-2_5

Havelsan (2023). *ADVENT ağ destekli veri entegre savaş yönetim sistemi*. https://www.havelsan.com.tr/sektorler/savunma-ve-guvenlik/deniz/su-ustu-savas-yonetim-sistemleri/havelsan-advent

Havelsan (2023). *Ağ destekli veri entegre savaş yönetim sistemi*, https://www.havelsan.com.tr/sektorler/savunma-ve-guvenlik/deniz/su-ustu-savas-yonetim-sistemleri/havelsan-advent

Havelsan (2023). *GENESİS savaş yönetim sistemi*. https://www.havelsan.com.tr/sektorler/savunma-ve-guvenlik/deniz/su-ustu-savas-yonetim-sistemleri/havelsan-genesis

Hunker, Jeffrey (November 2010). Cyber war and cyber power: Issues for NATO doctrine, *NATO Defense College*, (62), 1-13

Hvistendahl, Mara (25 Ekim 2016). The Decline in Chinese Cyberattacks: The Story Behind the Numbers, https://www.technologyreview.com/2016/10/25/156465/the-decline-in-chinese-cyberattacks-the-story-behind-the-numbers/

Indian Space Research Organisation (23.08.2023). *Chandrayaan-3*, https://www.isro.gov.in/Chandrayaan3.html.

Israel Defense Forces (29.12.2021). *The military intelligence directorate*. https://www.idf.il/en/mini-sites/directorates/military-intelligence-directorate/military-intelligence-directorate/

Kasapoğlu, C. (2017). Türkiye'nin S-400 ikilemi, *EDAM Dış Politika ve Güvenlik Kâğıtları Serisi*. 5: 1-4.

Köker, A. E. (2021). Çatışma ve Savaş İkileminde Siber Savaş: Siber Dünya, İstanbul: Urzeni Yayınevi.

Lund, K., Skjervold, E., Johnsen, F. T. ,Hafsøe T. and A. Eggen A. (2010, Ekim). Robust web services in heterogeneous military networks, *IEEE Communications Magazine*, 48(10). 78-83, doi: 10.1109/MCOM.2010.5594680.

Meteksan (2023). *KEMENT projesi tamamlandı*, https://www.meteksan.com/tr/haberler/kement-projesi-tamamlandi

Meteksan (2023). *KEMENT TDL taktik veri bağı sistemi.* https://www.meteksan.com/tr/urunler/haberlesme-sistemleri/ms-tdl-taktik-veri-bagi-sistemi

Milli Savunma Bakanlığı (2023). *Muhabere ve bilgi sistem dairesi başkanlığı.* https://www.msb.gov.tr/BakanYardimciBirimler/icerik/bakan-yardimcisi-mebs-baskanligi

MilSOFT (2023). *Taktik veri link sistemleri*. https://www.milsoft.com.tr/index.php/portfolio/taktik-veri-link-sistemleri/

NATO Standardization Agency. (2023). Standardization Agreement (STANAG) No. 5516 (Edition 6), Chapter 3, 28

Robinson, N. (2017, 06 Nisan). *Başarılı bir siber savunma için harcama yapmak.* https://www.nato.int/docu/review/tr/articles/2017/04/06/basarili-bir-siber-savunma-icin-harcama-yapmak/index.html.

Sanger, D. E., Barboza, D. & Perlroth, N. (2013, 18 Şubat). *Chinese army unit ıs seen as tied to hacking against U.S. the New York Times*. https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

SavunmaSanayiST (2023, Şubat). *Aselsan'ın 2022 yılı finansal sonuçları açıklandı*. https://www.savunmasanayist.com/aselsanin-2022-yili-finansal-sonuclari-aciklandi/.

Shen, M-S. (2019, Haziran). China's cyber warfare strategy and approaches toward Taiwan. *Taiwan Strategists*, (2), 1-18.

Smith, C.J. & Venter, J.P. (2011, 8-10 Kasım). *Case study: development of a SANDF tactical data link network enabling capability*. Military Communications and Information Systems Conference (MilCIS 2011), Canberra, Australia.

STM (2022 1 Aralık). *STM milli siber güvenlik fuarında bilişim çözümlerini paylaştı*. https://www.stm.com.tr/tr/medya/haberler/stm-milli-siber-guvenlik-fuarinda-bilisim-cozumlerini-paylasti

The Council on Foreign Relations. (2023). *PLA Unit 61398.* https://www.cfr.org/cyber-operations/pla-unit-61398

Thinktech STM (2015, Aralık). muharebe sahasının dijitalleşmesi. *Sektör Değerlendirme Raporu*.

TRT. (2019, 10 Ocak). *Milli veri linki yazılımının taşıdığı ilk mesaj: Merhaba tarihi an*. https://www.trthaber.com/haber/bilim-teknoloji/milli-veri-linki-yaziliminin-tasidigi-ilk-mesaj-merhaba-tarihi-an-400679.html

Tuğcu, M. & Gürel, O. (2012, Mayıs). Taktik data link teknolojilerinde birlikte çalışabilirlik ve kritik simülasyon bileşenleri, *Savunma Bilimleri Dergisi*, 11 (1), 239-250.

Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016). *Ulusal siber güvenlik stratejisi 2016-2019*. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2020). *Ulusal siber güvenlik stratejisi 2020-2023*. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf

U. S. (2023). Cyber command, https://www.arcyber.army.mil/About/About-Army-Cyber/; https://www.cybercom.mil/

OPINIONS / YORUMLAR

CYBER-AI TECHNOLOGY AND INTERNATIONAL RELATIONS

Yavuz AKDAĞ*

ORCID:0009-0009-5368-3937

In this commentary, I will address some of the major issues affecting International Relations (IR) scholars to fully engage in and comprehend how rapid advancements in cyber and artificial intelligence (AI) technologies influence and shift state-to-state strategic cybersecurity interactions. In particular, I will focus on two overarching but interrelated problems in the study of the intersection between cyberpolitics and IR theory. The first issue concerns analytical bareness due to conceptual infertility or ambiguity surrounding cybersecurity-AI studies in IR literature. Second relates to epistemological problems slowing or hindering intellectual progress towards refining or modifying existing IR concepts and theories or building new ones to meet emerging challenges of the 21st century technologies. Both problems arise mainly, if not exclusively, as a function of the swiftly evolving, novel, and confidential nature of cyber-AI technologies.

First, there exists a conceptual turmoil regarding fundamental concepts of the digital terrain such as "cyberspace", "cyberwar", and "cyber conflict", as many of these notions are erroneously used interchangeably particularly by policy circles, media reporters, and commentators. Indeed, this conceptual ambiguity persists also due to scholarly works. For instance, there are several approaches to defining the term "cyberspace". One of the structural approaches divides cyberspace into four layers— "physical", "logical" or "platform", "information", and "people" or "users" layers (Choucri & Clark, 2018, pp.36-38). The other approach splits the domain into three layers— "semantic, "syntactic", and "physical" (Libicki, 2009, p.12). Adding a "sociopolitical" dimension to the definition, some argue that the structural approach merely captures the "sociotechnical" aspects and overlooks the domain`s political saliency (Choucri & Clark, 2018, pp.37-52; Akdağ, 2023).

A more acute definitional disagreement in the relevant literature revolves around what constitutes cyberwar. Some contend that the word "war" in "cyberwar" is misleading, as cyber battlefield lacks characteristics of conventional war—political, violent, and lethal (Rid,

* Ph.D. in Politics and International Affairs/University of South Florida

2012). Others disagree and point to the case of Stuxnet as conclusive evidence to call it cyberwar given the nature of the cyber weapon. The latter argument warrants acknowledgment. The political aspect of Stuxnet rests with US-Israel collective effort to prevent Iran from ending Israeli nuclear power preponderance in the Middle East. Stuxnet is also known to cause physical destruction in Iranian nuclear plant. While no casualty was reported from the incident, one can induce that masses could have tragically suffered if the aim had been to cause more destruction or destroy the entire nuclear facility via cyber conduits. Despite the case of Stuxnet, some scholars are still hesitant to use the concept "cyberwar", but the existing literature seems to have achieved some conceptual clarity and accord around the notion "cyber conflict" as a more encompassing, ambarella term (Valeriano, Jensen, Maness, 2018; Akdağ, 2023).

Similar conceptual challenges exist in defining the key notions and boundaries of IA. Just as cyber technology, AI technologies (e.g., machine learning and quantum computing) evolve rapidly. Therefore, conceptual parameters of "artificial intelligence" and cyberspace are extremely blurry. While some believe that AI and cyberspace are not necessarily overlapping, others consider AI as a "subset of cyber" (Demchak, 2019, p.99 Whyte, 2023, p.309). Neither argument may be wrong. AI co-evolves and intersects with cyberspace. For instance, AI technology is already integral to cybersecurity, as it helps enhance the ability of states to conduct offensive cyber operations and counter and prevent cyber threats (e.g., detecting intrusion) (Doran & Britton, 2018; Whyte, 2023, pp.308-310; Akdağ, 2023, p.250). Yet interwoven AI-cyber technologies—along with the nascency and interdisciplinary features of cybersecurity and AI studies- make it challenging to establish precise and universally agreed conceptualizations. As a result, IR scholars are having difficulties of fully understanding how AI systems affect the nature of cyber operations and states` cybersecurity strategic calculations such as offense-defense balance, deterrence, and decision-making (Whyte, 2023, pp.308-310; Akdağ, 2023).

The second major problem facing the study of cybersecurity and AI within IR literature concerns epistemological challenges. Scholars overwhelmingly draw on "open sources" to obtain empirical data or information about interstate cyber relations, which is inadequate (Buchanan, 2016, p.12). The lack of robust empirical data can be ascribed to the novelty and nature of cyber conflict (e.g., clandestine characteristics of cyber operations and cyber capabilities and anonymity of cyber perpetrators), rendering most cyber actions concealable

and, therefore, empirical data acquisition and collection intractably difficult. As an illustration, notwithstanding the widespread agreement among scholars and experts, Washington`s role in the development and employment of Stuxnet has not been conclusively proven yet. As a result of this epistemological challenge, the link between actors` behavior and their motive or intent in the digital domain becomes ambiguous, and the conceptualization and measurement or operationalization of fundamental cyber-related concepts becomes a rather challenging task (Cavelty, 2018, p.305; Whyte, 2018, pp.55-56; Bergman & Mazzetti, 2019; Akdağ, 2023).

In conclusion, the novel, secret, and ever-changing nature of cyber-AI technologies makes it very challenging to create precise and fixed conceptual parameters and obtain robust empirical data to test key concepts and theories against new realties. Thus, it is not surprising to see conceptual turmoil and infertility and analytical bareness in scholarly works focusing on the intersection between cybersecurity-AI and IR theory. When concepts lack clarity, theories` explanatory power remains poor, which is internally corrosive to theory, thereby risking theoretical stagnation. This may, in turn, impede intellectual progress.

However, theoretical stagnation can be avoided. Normally, theory-building studies tend to increase in volume when new technologies or realities arise. This was the case with the advent of nuclear technology, which spurred tremendous scholarly interests to develop deterrence theories during the Cold War. Similar picture also emerges within IR literature studying the intersection or co-evolution of cyber-AI technology with international politics (e.g., cyber deterrence studies). Yet due to cursory and superficial theoretical and conceptual analyses in the existing literature, some may consider IR theory unfit for explaining state behavior in rapidly evolving landscape of cyber-AI worlds, but it will be an error to divert attention from IR theory to elsewhere without first adequately testing how IR concepts perform in the face of new actualities. Despite epistemological challenges that make theory-testing difficult, the latest developments such as increasing investigations over cyber conflict and leaked classified cyber operations (e.g., Snowden revelations) have offered significant source of data for scholarly inquiry, potentially enabling more empirically robust and theoretically rigorous studies (Kello, 2013, p.12; Buchanan, 2016, p.12; Akdağ, 2023).

References

Akdağ, Y. (2023). *Great Power Cyberpolitics: Re-Interpreting Offensive Realism and Power Transition Theory for Cyber Deterrence* [Doctoral Dissertation, University of South Florida]. ProQuest Dissertations Publishing.

Bergman, R. & Mazzetti, M. (2019, September 4). The Secret History of the Push to Strike Iran: Feature. *New York Times (Online)*. https://www.nytimes.com/2019/09/04/magazine/iran-strike-israel-america.html

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press

Cavelty, M., D. (2018). Europe`s cyber-power. *European Politics and Society*, *19*(3), 304-320. https://doi.org/10.1080/23745118.2018.1430718

Choucri, N. & Clark, D.D. (2018). *International Relations in the Cyber Age: The Co-Evolution Dilemma.* MIT Press.

Demchak, C. C. (2019). China: Determined to dominate cyberspace and AI. *Bulletin of the Atomic Scientists*, *75*(3), 99-104. https://doi.org/10.1080/00963402.2019.1604857

Doran, T. & Britton, B. (2018, February 6). How a company founded by ex-spies uses AI to fight hackers. CNN. https://www.cnn.com/2018/02/05/tech/darktrace-cybersecurity-immune-system/index.html

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7-40. doi:10.1162/ISEC_a_00138

Libicki, M. C. (2009). *Cyber Deterrence and Cyberwar*. Santa Monica, CA: RAND Corporation.

Rid, T. (2012). Cyber war will not take place. *The Journal of Strategic Studies*, *35*(1), 5-32. http://dx.doi.org/10.1080/01402390.2011.608939

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.

Whyte, C. (2018). Dissecting the digital world: A review of the construction and constitution of cyber conflict research. *International Studies Review*, *20*(3), 520-532. https://doi.org/10.1093/isr/viw013

Whyte, C. (2023). Learning to trust Skynet: Interfacing with artificial intelligence in cyberspace. *Contemporary Security Policy*, *44*(2), 308-344. https://doi.org/10.1080/13523260.2023.2180882

DİJİTAL VATANDAŞLIK VE SİBER DÜNYANIN SORUNLARI

E. Dilara KILINÇ*

ORDIC: 0009-0008-7316-2269

Öz

Günlük hayatımızın ayrılmaz bir parçası olan internet, 1990 yıllardan sonra tüm dünyaya yayılmış milyonlarca resmi, özel ve ticari ağların birbirine bağlanmasıyla oluşan yeni bir ortamdır. İnternet ve internet üzerindeki dijital yapıların ve uygulamaların, sundukları hizmetler, ürünler ve iletişim imkânları bireylere yeni fırsatlar sunarken, yeni sorunları da beraberinde getirmektedir. 2023 yılı başı itibariyle tüm dünya nüfusunun %63,5'i interneti (yaklaşık 5,07 milyar kişi) kullanmaktadır. Oluşan bu yeni dünyanın en önemli parçası olan bireyin, dijital vatandaş olarak hak ve sorumluluklarının ele alınması hayati önem arz etmektedir. Bu bağlamda, dijital vatandaşlık kavramı ve dijital vatandaşlığın dokuz boyutu (dijital erişim, dijital ticaret, dijital iletişim, dijital okur-yazarlık, dijital etik, dijital kanunlara riayet, dijital hak ve sorumluluklar, dijital sağlık ve dijital güvenlik) ortaya konulmaktadır. Bu çalışmada, dijital vatandaşlığın boyutları da göz önünde tutularak, bireylerin siber dünyada karşılaştığı veya karşılaşabileceği temel sorunlar ve başta eğitim olmak üzere muhtemel çözüm önerileri üzerinde durulmaktadır.

Anahtar kelimeler: Siber dünya, dijital vatandaşlık, dijital vatandaşlığın boyutları, dijital vatandaşların karşılaştığı sorunlar ve çözüm önerileri.

DIGITAL CITIZENSHIP AND PROBLEMS OF CYBER WORLD

Abstract

The internet, which is an integral part of daily life, is a new environment appeared in result of the interconnection of millions of official, private and commercial networks spread all over the world after the 1990s. While the internet, digital structures and applications on it, offering services, products and communication opportunities to individuals, they also bring new problems. As of the beginning of 2023, 63.5% of the world's population (approximately 5.07 billion people) uses the internet. It is vital to address the rights and responsibilities of the individual, who is the most important part of this new world, as a digital citizen. In this context, the concept of digital citizenship and nine elements of digital citizenship (digital access, digital commerce, digital communication, digital literacy, digital ethics, compliance with digital laws, digital rights and responsibilities, digital health and digital security) are

* MA Student, Department of International Relations, Selçuk Universisity-Konya.

elaborated. In this study, taking into account the elements of digital citizenship, the main problems that individuals face or may face in the cyber world, and possible solution suggestions, especially education, are emphasized.
Key Words: Cyber world, digital citizenship, elements of digital citizenship, problems of digital citizens and proposals of possible solutions.

Giriş

Dünyanın gündemine wolrd wide web (www)'in geliştirilmesiyle1990'lı yıllarda giren ve artık günlük yaşamımızın ayrılmaz parçası haline gelen internet, birbirine bağlı bilgisayar ağlarının tümü olarak da tanımlanabilir. Milyonlarca ticari ağ ile devlet ve özel bilgisayar ağlarının birbirine bağlanmasıyla oluşmuştur.

"Siber uzay" veya "siber âlem" kavramı ise, internet üzerindeki dijital alanların tamamını ifade etmek için kullanılan bir terimdir. Bu alanlar, web siteleri, sosyal medya platformları, bulut depolama servisleri, çevrimiçi forumlar, e-posta hesapları ve benzeri birçok dijital varlığı kapsar. Hayatımızın her alanını etkileyen siber uzay, vatandaş-devlet ilişkilerini derinden etkilemiş ve bu çerçevede insan hakları alanında da yeni fırsatlar ve yeni tehditleri beraberinde getirmiştir (Demirer, 2023).

İnternet kullanımının artması ve internet tabanlı hizmetlerin genişlemesi ile birlikte, bu alanda güvenlik tehditleri de artmaktadır. Siber saldırılar, çevrimiçi kimlik avı, veri hırsızlığı ve diğer siber suçlar, suçların unsurlarını yeniden şekillendirmiş, bireyler, kuruluşlar ve devletler için ciddi riskler oluşturmaya başlamıştır (Demirer,2023 ; Cengiz, 2021:407-424). Siber gelişmeler ulusal ve uluslararası sistemi teori ve uygulamada derinden etkilerken, bu alanda egemen güçlerin evrensel düzenlemelerden kaçındığı görülmektedir. Kapsam ve üyeler açısından oldukça sınırlı olan Avrupa Konseyi'nin Siber Suçlarla Mücadele Sözleşmesi ve ikili bazı anlaşmalar dışında henüz bir siber uzay rejimi oluşturulamamıştır (Akyeşilmen, 2018: 185-186). Siber âlemdeki her şey gibi siber güvenlik kavramları da sürekli gelişim ve değişim içindedir.

Hız, güvenlik, teknoloji okuryazarlığı ve büyük veri tehditleri gibi çok yönlü çözüm gerektiren meseleler bir kenara bırakıldığında, internetin hayatın her alanına geri dönülmez şekilde girmesi nedeniyle, yavaş yavaş demokrasiyi e-demokrasiye, vatandaşlığı dijital vatandaşlığa, yönetimi e-yönetişime dönüştürdüğü söylenebilir (Işıklı, 2015 : 22).

Dijital Vatandaşlık Kavramı

Bilişim ve iletişim teknolojilerinin gün geçtikçe gelişmesine paralel olarak bilgiye her yerden ulaşılabilmekte ve her birey dünyanın farklı bir coğrafyasındaki ülke vatandaşı ile iletişim kurabilmektedir. Dijital vatandaşlık kavramı bu gelişmelerin sonucu olarak ortaya çıkan kavramlardan birisidir. Diğer bir ifade ile internetin iletişim ve haberleşme noktasında ülke sınırlarını ortadan kaldırması, dünyayı küreselleştirmesi bu kavramın ortaya çıkmasına sebep olmuştur (Çubukçu ve Bayzan, 2013).

Teknolojiyi ve teknolojiyle beraber hayatımıza giren dijital araçları doğru kullanmasını bilen, etik kurallara ve kişi haklarına dijital platformda da saygı duyan ve bu araçları güvenlik ve sorumluluk bilinciyle kullanmasını bilen kişiye dijital vatandaş denmektedir. Dijital vatandaşlık ise kısaca, teknoloji kullanımı ile ilgili dijital vatandaşların sorumluluk sahibi davranış normları olarak tanımlanmaktadır (Mossberger, Tolbert ve S. McNeal, 2007: 140). Başka bir deyişle dijital vatandaşlık; temelde dijital ortamda pozitif, eleştirel ve yetkin bir şekilde etkileşime girme, etkili iletişim ve yaratma becerilerini kullanarak, teknolojinin sorumlu kullanımı ile insan haklarına ve onuruna saygılı sosyal katılım biçimlerini uygulama becerisi anlamına gelir (Mediatrend:2023). Bununla birlikte, dijital vatandaşlık kavramının henüz ulusal ve uluslararası alanda herkesin üzerinde hemfikir olduğu bir kavram olduğu söylenemez.

We are social isimli anket şirketinin 2022 raporu verilerine göre, 2022 yılı sonu itibariyle, tüm dünya nüfusunun %63,5'i internet (yaklaşık 5,07 milyar kişi) kullanmaktadır. Aynı zamanda dünya nüfusunun %59,3'ü (yaklaşık 4,72 milyar kişi) aktif olarak sosyal medya araçları kullanmaktadır. İnternet kullanıcı sayısı bir önceki yıla göre %3,5, sosyal medya kullanıcı sayısı ise %4,2 oranında artmıştır (Terzibaş, 2023 : 39-57).

Dünyanın birçok noktasından dijital teknolojilerin kullanılabiliyor olması, bütün dünya vatandaşlarının eşit hak ve sorumluluklara sahip birer dijital vatandaş olabileceğini göstermektedir. Coğrafi sınırlara bağlı bir vatandaşlık algısının küreselleşmeyle aşınması, aynı dijital platformların tüm dünya vatandaşları tarafından kullanılabilir hale gelmesi gibi sebepler, dijital vatandaşlık kavramının ortaya çıkmasını neden olmuştur (Çubukçu ve Bayzan, 2013).

Dijital Vatandaşlığın Boyutları

Dijital vatandaşlığın her açıdan anlamlarını ortaya koymaya çalışan ve bu alandaki pek çok makalede atıf yapılan Mike Ribble, dijital vatandaşlığı 9 boyutta incelemektedir:

1-Dijital Erişim: Bireylerin teknoloji okuryazarlığı doğrultusunda dijital hizmetlere erişebilmesi ve bunu sağlayan teknolojik araçlarını kullanma becerisidir.

2-Dijital Ticaret: Bireylerin alışveriş, para transferi yapmak, banka işlemleri gibi işlemleri bilinçli ve doğru bir şekilde gerçekleştirebilmesi, dolandırıcılık, fidye gibi kötü niyetli tuzaklardan kendilerini ve malvarlıklarını koruyabilmesidir.

3-Dijital İletişim: Bireylerin başta dijital kamu hizmetleri, sosyal medya platformları, çevrimiçi faaliyetler olmak üzere, tüm dijital iletişim kanallarında tıpkı gerçek ortamlarda olduğu gibi özenli ve etik kurallara uygun davranmasıdır.

4-Dijital Okur-yazarlık: Siber uzayda edinilen bilgileri doğru analiz etme ve güvenilir kaynak süzgecinden geçirme sorumluluğudur. Denetimin minimal seviyede olduğu siber dünyada, bilgi kirliliğinin yüksek olabileceği bilinciyle hareket edilmesidir.

5-Dijital Etik: Toplumsal ve bireysel etik değerler çerçevesinde, saygılı ve sorumlu internet kullanımıdır.

6-Dijital Kanunlara Riayet: İnternet kullanımının gerektirdiği ulusal ve uluslararası düzenlemelere uyma, suç oluşturabilecek internet ihlallerinin bilinmesine ilişkin dijital vatandaşlık bileşenidir. Bu anlamda, siber suçlar gibi suçların yanı sıra sosyal medya ortamlarında, zorbalık, ifade özgürlüğü ihlali, şantaj veya tehdit suçlarının cezai yaptırımlarının bulunduğunun bilinmesi ve bu konuda üçüncü kişilerin de bilinçlendirilmesidir.

7-Dijital Hak ve Sorumluluklar: Dijital ortamlardaki hakların bilinmesi ve hukuki yükümlülüklerin yerine getirilmesi sorumluluğudur.

8-Dijital Sağlık: Bilgisayar, akıllı telefon ve tablet gibi cihazların kullanımından kaynaklanabilecek sağlık problemlerini bilme ve kaçınma sorumluluğudur.

9-Dijital Güvenlik: Güvenlik konusunun aslında dijital vatandaşlığın boyutlarını aşkın pek çok yönü bulunmaktadır. Ancak bireysel düzeyde, internetten güvenli araçlarla ve doğru yöntemlerle faydalanılması, kişisel bilgilerin çalınmasına neden olabilecek hatalara karşı uyanık olunmasıdır (Ribble, 2011: 15-43).

Teknolojinin her gün biraz daha gelişmesi, farklı dijital araç ve gereçlerinin kullanımına fırsat tanımaya başlamış ve dijital vatandaşlığın daha fazla boyutlarda ele alınabileceğini göstermiştir. Ribble'ın dijital vatandaşlık için önerdiği 9 boyuta bulut bilişim, akıllı telefonlar,

dizüstü bilgisayarlar ve tabletler gibi dijital araçların da eklenmesiyle dijital vatandaşlığın, 11 boyutta incelendiği de görülmektedir (Çubukçu ve Bayzan: 2013).

Dijital Vatandaşlığın Boyutlarıyla İlgili Siber Sorunlar

İnternetin ve siber dünyanın riskleri çok çeşitli ve gerçek vakalardan örneklerle bireysel, kurumsal, ulusal ve uluslararası seviyelerde incelenmiştir (Akyeşilmen, 2018 : 173-189, 288-305). Türkiye'de bilişim ve iletişim sektörünü düzenleyen ve denetleyen üst kurul Bilgi Teknolojileri ve İletişim Kurumu'na bağlı çalışan Telekomünikasyon İletişim Başkanlığı (TİB) internetin bilinçli ve güvenli kullanımına yönelik yapmış olduğu bilinçlendirme faaliyetlerinde internetin risklerini dokuz başlıkta incelemiştir: Yanlış ve/veya zararlı bilgiye erişim, siber zorbalık, sanal dolandırıcılık, kişisel bilgilerin paylaşımı, zararlı yazılımlar, pornografi/çocuk istismarı, oyun ve internet bağımlılığı, yabancılarla çevrimiçi ve çevrimdışı iletişim ve şiddet/nefret/ırkçılık faaliyetleri (Çubukçu – Bayzan, 2013).

Bu çalışmada ise, internette bir dijital vatandaşın karşı karşıya kalabileceği riskler ele alınmaya çalışılacaktır. Ribble'ın belirlediği 9 dijital vatandaşlık boyutunun hangi siber sorunlarla ilişkili olabileceğini inceleyelim:

a-Dijital Erişim Boyutu

Öncelikle her bireyin çevrimiçi ortama erişme hakkı vardır. Bazı konularda devletle iletişimin, haberleşmenin ve bazı kamu hizmetlerine ulaşmanın tek yolu olan internete erişimin temel bir hak olup olmadığı tartışılmaktadır. İnternete erişim, herhangi bir hukuki belgede olmamasına ve insan hakları yazınında henüz böyle bir kabul olmamasına rağmen, Birleşmiş Milletler (UN) raporlarında bir insan hakkı olarak tanımlanmaktadır (Akyeşilmen, 2018: 285).

Otoriter rejimlerde internetin yasaklanması veya kısıtlanması, internetin etkisi konusunda açık bir fikir vermektedir. Bununla birlikte, internete giren bireylerin kişisel bilgilerinin, ticari ve mali varlıklarının korunması devletin, kurumların ve servis sağlayıcı şirketlerin görevidir. Çünkü, kişisel bilgilerin çalınması, sosyal medya hesaplarının ele geçirilmesi ve dolandırıcılık günümüzde rastlanan en yaygın rastlanan güvenlik sorunları arasındadır.

b-Dijital Ticaret Boyutu

2015 - 2021 döneminde internet üzerinden yapılan ticaret hacminde, yıllık ortalama %20'nin üzerinde artış gerçekleşmiştir. 2015 yılında küresel e-ticaret hacmi 1,5 trilyon dolar olarak gerçekleşirken, 2021'de 4,9 trilyon doları aşmış ve 6 yılda 3 kattan fazla artmıştır (Terzibaş, 2023). Günümüzde ise, dünya çapındaki e-ticaret hacminin 10 trilyon doları geçtiği tahmin edilmektedir.

İnternet üzerinden alışveriş, mali işlemler ve bankacılık işlemlerinin yapılması ciddi yazılım ve donanım alt yapısını gerektirdiği gibi, bireylerin de bu alt yapıyı kullanacak bilgi birikimine sahip olmaları gerekir. Ayrıca, bireyler yaptıkları işlemlerin dolandırıcılığa, virüslere ve üçüncü kişilerin müdahalelerine karşı korunması gerekmektedir.

c-Dijital İletişim Boyutu

İletişimin 2024 yılında geldiği noktaya bakılacak olursa, bütün geleneksel iletişim yöntemlerinin (telefon, mektup, faks, başvuru, dilekçe, kısa mesaj, görüntülü iletişim vb.) ya aynısı ya da alternatifi internette ve dijital dünyada mümkündür. Hatta sosyal medya, görüntülü konuşma, e-posta, bulut teknolojisi ve anlık mesajlaşma gibi bazı iletişim yöntemleri sadece dijital alanda mümkündür.

Bu denli yoğun ve kaçınılmaz etkileşim içinde bireylerin her türlü bilgisi ve iletişimi, kurumların ve üçüncü kişilerin müdahale riski altındadır. Bu anlamda, bireylerin haberleşmesinin mahremiyeti ve gizliliğinin korunması en önemli sorun olarak karşımıza çıkmaktadır. Aynı şekilde, sosyal medyada bireylerin paylaştığı her şeyin sınırı belli olmayacak şekilde yayılması ve anonimleşmesi diğer bir risktir.

d-Dijital Okur-Yazarlık Boyutu:

İnternet okur-yazarlığı ve dijital okur-yazarlık günümüzde her bireyin zorunlu vasıfları arasında yer almaktadır. Bu bağlamda, dijital kitap ve medyanın geleneksel okuma ve yazma alışkanlıklarını değiştireceğinin ilk işareti, NTV Haber sitesinin 20.7.2010 tarihli haberine göre; dünyadaki dijital kitapların satışının ilk olarak 2010 yılında kağıt kitap satışlarını geçmesiydi.

Aynı şekilde, 244 yıldır basılan *Britannica* Ansiklopedisi'nin basımı ücretsiz hizmet veren dijital ansiklopedilerin yaygınlaşması nedeniyle 2012 yılında durdurulmuştur. Londra'da 1734 yılında kurulan dünyanın en köklü gazetelerinden birisi olan *Lloyd's List,* 2013'ün

Aralık ayında kâğıt baskıyı bırakıp, tamamen dijitale geçmiştir (LLoyd's List,2024). 1933 yılında New York şehrinde basımına başlanan ve 12 ülkede dağıtımı yapılan *Newsweek* dergisi, Ocak 2013 tarihinden itibaren tamamen dijital yayına geçti (Newsweek, 2024).

Matbaanın bulunmasından sonra, dünya dijitalleşmeyle yeni bir döneme girmiştir. Matbaa herkesin okur olmasını kolaylaştırırken, dijital kitaplar okurluğun yanısıra herkese yazar olma şansı da sunmaktadır (Soydan, 2012: 395-397).

Günümüzde bilgisayar, akıllı telefon, tablet ve benzeri araçları kullanma kamu hizmetlerine, ürün ve içeriklere ulaşım için neredeyse zorunlu hale gelmiştir. Bu nedenle bireylerin, dijital araçları ve interneti kullanmayı öğrenmesi ve yeni gelişmelere uyum sağlamaları en temel gereklilik olarak ortaya çıkmaktadır (CoE, 2017). Bu temel yetilere sahip olmama veya "yanlış bir düğmeye basma korkusu" toplumdan ve günlük hayattan dışlanmaya varabilecek bir izolasyonun başlangıcı olabilmektedir.

e-Dijital Etik Boyutu:

Bireylerin dijital araçları ve interneti kullanırken, güvenilir kaynakları kullanmaları, başkalarının haklarına saygılı olmaları ve gereken ahlaki sorumlulukla hareket etmeleri de önemlidir.

Kabul edilebilir çevrimiçi davranışların tümü İngilizce'den esinlenerek *"netiquette"* (netteki görgü kuralları) adı altında ele alınmaktadır. Bu kavram temelde, dijital vatandaşların uymak zorunda olduğu davranış kurallarını, siber zorbalık yapmamayı, mahremiyete saygı göstermeyi ve dürüst davranmayı ifade etmektedir (OECD, 2019).

f-Dijital Kanunlara Riayet:

Gerçek dünyada olduğu gibi siber dünyada da yapılması hukuki, cezai veya idari yaptırıma bağlanmış olan eylemleri düzenleyen yasalar ve kurallar mevcuttur. Her bireyin ve kurumun bu kurallara uygun davranması zorunludur. Kuralların uluslararası ve ulusal planda olmak üzere iki seviyesi bulunmaktadır. Bir de, siber dünyanın esas aktörleri konumunda olan hizmet, ürün ve içerik sağlayıcı şirketlerin sözleşmelerle koydukları kurallar vardır. Siber dünyaya giren her bireyin bu kurallara uyması gerekmektedir.

Siber dünyadaki hukuka aykırı hareketleri engelleme ve suç teşkil eden eylemlerin faillerini cezalandırma konusunda, uluslararası planda çok ciddi bir gelişme olmamıştır. Bu kapsamda, 2001 tarihli Avrupa Konseyi Siber Suçlarla Mücadele Sözleşmesi dışında kapsamlı bir uluslararası sözleşme bulunmamaktadır.

Bu bağlamda, internetin sağladığı anonimliğe veya dijital maskelere güvenerek hakaret, tehdit veya aşağılama, normal hayatta yapmadığı şeyleri yapma ve suç işleme konusunda rahatlık hissetme en sık karşılaşılan olgulardan birisidir. Halbuki, dijital ortamdaki hareket ve eylemlerin çoğu iz bırakmaktadır. İstendiği ve detaylı araştırma yapıldığı takdirde, siber dünyadaki her suçun failinin büyük oranda tespit edilebileceği bilinmektedir. Bireylerin, bu gerçeğin farkında olarak siber ortamda hareket etmeleri gerekmektedir.

g-Dijital Hak ve Sorumluluklar:

İnternete erişim, henüz anlamı ve kapsamı üzerinde evrensel bir uzlaşma olmasa da, ulusal ve uluslararası alanda bir genelde bir hak olarak kabul edildiği söylenebilir. İnternete girildiği andan itibaren, tıpkı gerçek dünyada olduğu gibi başkalarının özgürlüklerinin başladığı yerde kendi özgürlüklerimizin sonlanması veya sınırlandırılması söz konusudur.

Başka bir anlatımla, özgürlüklerin yarışması, üstünlük veya önceliğin belirlenmesi söz konusudur. Siber dünyada henüz küresel düzenleyici bir sistem kurulmadığı veya kurulamadığı için, özgürlüklerin ve varsa sınırlamalarının nasıl gerçekleştirilebileceği konusundaki tartışmalar devam etmektedir. İnternette hiç bir kural ve sınırlamanın kabul edilmemesi gerektiğini savunan anarşist ve kaotik görüşlerden, dijital dünyanın tıpkı gerçek dünya gibi tamamen kontrol altında tutulması gerektiğini savunan otoriter görüşlere kadar sayısız görüş ileri sürülmektedir.

Bu konuda akla gelen ilk çözüm, gerçek dünyadaki durumun siber dünyaya yansıtılmasıdır. Yani gerçek dünyadaki hak ve sorumlulukların, dijital dünyada da uygulanmasıdır. Gerçek dünyada ifade özgürlüğü ne oranda kullanılıyor ve korunuyorsa, siber alemde de o oranda kullanılabilmesi ve korunmasıdır. Ancak siber dünyanın sınırlarının belirsizliği, yer, zaman, kişi ve eylem kavramlarının tüm siber aleme yayılabilecek nitelikte olması, sadece siber dünyaya has kavramların varlığı (avatar kullanımı, yapay zeka, otobot hareketleri, *meta verse* ve benzeri sanal dünyalar) bu çözümlerin yetersiz olduğunu göstermektedir. Örneğin, Hindistan'dan internete bağlanan bir kişinin, Fransa merkezli bir şirketin sosyal medya

uygulamasında, Kanada'da yaşayan bir ABD vatandaşına hakaret etmesi durumunda hukuki ve cezai sorumluluğun hangi ülkenin kanununa göre, hangi mahkeme tarafından, ne zaman ve hangi usule göre belirleneceği gibi sorular, imkansız olmasa da, cevaplanması zor sorulardır. Ancak dijital vatandaşlar, siber dünyada hareket ederken "en az" gerçek dünyadaki kadar, haklarını bilme ve kullanma, sorumluluklarını da yerine getirme yükümlülükleri olduğunu fark etmek zorundadırlar.

h-Dijital Sağlık:

Bireylerin dijital dünya ile etkileşimlerinin sağlıklarına etkisi genelde olumsuz sonuçlarla bilinmektedir. Siber dünyada gerçek dünyada bulunan pek çok mesleğin, hobinin, sanatsal aktivitenin veya yasadışı faaliyetlerin aynısının veya benzerinin bulunması, insanların hayatlarının önemli bir bölümünü bilgisayar, telefon ve ekran başında geçirmelerine neden olmaktadır.

Globalwebindex'in 2021 yılı raporuna göre tüm dünyada günde ortalama 6 saat 54 dakika internette geçiriliyor. Buna sosyal medya, haber kanalları, TV ve alışveriş de dahildir. Türkiye'de oran biraz daha artıyor. Bizde günlük olarak internette geçirilen zaman 7 saat 57 dakikadır (Linkedin, 2021). Bu rakamlar, insanların günün ortalama üçte birini internet başında geçirdiklerini göstermektedir. Bu kadar uzun süreyi siber dünyada geçiren bireylerin, göz, kas-iskelet sistemi rahatsızlıkları, gastro intestinal, nörolojik veya ortopedik rahatsızlıklar geçirmeleri olasıdır.

Fiziksel rahatsızlıklar yanında, internet bağımlılığı, çevrimiçi kumar bağımlılığı ve dijital oyun bağımlılığı gibi pek çok yeni psikolojik rahatsızlıklar ortaya çıkmıştır. Bu nedenle, dijital bireylerin internetten faydalanırken de, her şeyde olduğu gibi "azı karar, çoğu zarar" ilkesiyle hareket etmeleri, çok uzun süre ekran karşısında hareketsiz kalmamaları, gerçek dünyayla sanal dünyayı birbirine karıştırmamaları, hatta gerçek dünyadan kopup sanal dünyada yaşama yanılsamasına girmemeleri gerekmektedir.

ı-Dijital Güvenlik Boyutu:

Yukarıda değinilen hususlar dikkate alındığında, siber dünyadaki güvenliğin en az gerçek hayattaki güvenlik kadar önemli hale geldiği söylenebilir. Çünkü, gelişmiş ve gelişmekte olan ülkelerdeki siber dünyanın aktörleri konumunda olan bireylerin, şirketlerin, kurumların, devletlerin ve uluslararası kuruluşların hayati faaliyetlerinin büyük çoğunluğu dijital araçlarla

internet, intranet ya da benzeri yerel, ulusal ve küresel ağlar üzerinden gerçekleştirilmektedir. Siber güvenliğin ana noktalarına değinilmesi bile bu makalenin kapsamını aşmaktadır. Bu nedenle, siber güvenliğin dijital vatandaşlığa ilişkin yönlerine sadece göz atmakla yetiniyoruz. Son yıllarda bireyler yanında şirketlerin ve devletlerin bilgilerinin bilgisayar korsanlarınca çalınması, şirketlerin veya devletlerin hizmetlerinin siber saldırılarla aksatılması, bireyden devlete kadar tüm seviyelerde siber güvenlik önlemlerinin alınmasını zorunlu kılmıştır. Hatta bu durum o kadar önemli hale gelmiştir ki, devletlerde siber güvenlik birimleri kurulurken, bilgi güvenliği konusunda şirketler için ISO 27001 gibi bazı uluslararası standartlar konulmuştur.

Global araştırma şirketi *Statista* verilerine göre, 2021'de 139 milyar dolar olan siber güvenlik pazarındaki gelirin 2022'de 159,8 milyar dolar civarında gerçekleştiği düşünülüyor. Pazarın yüzde 13,33'lük bir yıllık büyüme oranı göstermesi ve bunun 2027 yılına kadar devam etmesi halinde 298,7 milyar dolarlık pazar hacmiyle sonuçlanacağı tahmin ediliyor. Türkiye'de ise 2020 yılında 247,4 milyon dolar olan siber güvenlik çözümleri pazarının 2025 yılında 344,9 milyon dolara ulaşması beklenmektedir (Yeniova, 2022).

Dijital güvenlik pek çok alanda olduğu gibi, en küçük halka olan bireyden başlamaktadır. Bireylerin kullandıkları her türlü dijital aracın dış etkilere karşı güvenliğini sağlamaları (Anti-virüs programı kullanmaları, güvenli internet hizmeti sunan şirketlerden hizmet almaları, güvenlik duvarı kullanmaları, güvenli sayfalarda gezinmeleri, dijital hizmetlerde ve cihazlarda parola, parmak izi, yüz tanıma vb. güvenlik araçları kullanmaları) ilk adımdır. Devletin ve hizmet sunan şirketlerin kendi alanlarında siber güvenliği sağlamaları ikinci adımdır. Siber saldırılara ve güvenlik açıklarına karşı bireylerin, şirketlerin, kurumların ve devletlerin işbirliği yapması ise üçüncü adım olarak gözükmektedir.

Sonuç ve Değerlendirme

Dünyanın dijitalleşmesi ve internetin yaygınlaşması sonucu olarak, dünyanın dört bir tarafındaki bireylerin ve kurumların birbiriyle gerçek zamanlı iletişim kurmaları ve etkileşime geçmeleri mümkün hale gelmiştir.

Dijital dünyada dijital vatandaşlık, dijital araçların kullanıldığı her durumda geçerli olan davranış normlarını tanımlamakla beraber günümüz dijital platformların kullanımının büyük bir çoğunluğu çevrimiçi teknolojiler yani internet aracılığıyla gerçekleşmektedir. Bu yüzden,

dijital vatandaşlık algısını, artık çevrimiçi ya da daha geniş anlamda internet teknolojilerini kullanım alışkanlıkları çerçevesinde değerlendirmek gerekmektedir (Çubukçu ve Bayzan). Dijital araçları kullanım yaşının oldukça düşmesi nedeniyle dijital vatandaşlık algısının çocuk yaşlarda başlaması gerektiğini ve bu çağdaki çocuklara dijital araçların kullanımının öğretilmesi gerektiği ifade edilmiştir (Ribble, 2011). Ülkemizde ilköğretimde bilişim dersinin konması önemli bir adımdır. Aslında çocukların okuma yazma öğrenmeden telefon ve tablet kullanmayı öğrendikleri dikkate alınırsa, okuldan önce başlayan bu dijital etkileşime ilişkin eğitimin ilk önce ailede başlaması gerektiğini göstermektedir.

Okuldaki hayata hazırlama eğitiminin yanında, hem bu şansı kaçıranlar hem de bilgilerini güncellemek isteyen yetişkinler için, devletin hem örgün hem de uzaktan eğitim yöntemiyle eğitimler ve kurslar düzenlemesi gerekmektedir. Aksi takdirde pek çok yetişkinin, özellikle de yaşlıların, dijital dünyadan soyutlanması sosyal bir problem olarak ortaya çıkacaktır. Her ilçede bulunan halk eğitim merkezleri, dijital vatandaşlık eğitimlerin ve kursların düzenlenmesinde önemli bir çözüm noktasıdır. Yine belediyelerin ve diğer kamu kurumlarının verdiği eğitimler yardımcı olabilecek niteliktedir. Ayrıca televizyondan veya akıllı telefonlardan yayınlanabilecek çevrimiçi veya çevrimdışı dersler, kurslar, podcast'ler, işitsel ve görsel eğitim materyalleri şahsen kursa katılma olanağı olamayanlara çözüm olabilecektir.

K aynakça

AKYEŞİLMEN, Nezir (2018). Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik. Ankara: Orion Kitabevi.

CENGİZ, Gönül (2021). Siber Suçlar, Sosyal Medya ve Siber Etik. İletişim Çalışmaları Dergisi, Cilt 7, Sayı 3, s.407-424.

Council of Europe (2017). Digital Citizenship Education, Strasbourg: CoE Publishing.

ÇUBUKÇU, Ahmet – BAYZAN, Şahin (2013). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. https://www.guvenliweb.org.tr/dosya/73bDc.pdf İET:22.12.2023.

DEMİRER, Egemen (2023). Siber Uzay ve Siber Güvenlik?. Hukuk ve Bilişim Dergisi, 12, https://www.hukukvebilisimdergisi.com/siber-uzay-ve-siber-guvenlik/ İET: 22.12.2023.

IŞIKLI, Şevki (2015). Digital Citizenship: An Actual Contribution to Theory of Participatory Democracy. AJIT-E: Academic Journal of Information Technology, 6(18). https://doi.org/10.5824/1309-1581.2015.1.002.x İET:22.12.2023.

Linkedin https://tr.linkedin.com/pulse/ İET:10.01.2024

Lloyd's List (http://www.lloydslist.com) İET:09.01.2024.

Mediatrend https://mediatrend.mediamarkt.com.tr/dijital-vatandaslik-nedir/ İET:22.12.2023.

Mossberger, Karen ve Tolbert, Caroline ve McNeal, S.Ramona (2007). Digital Citizenship, the Internet, Society and Participation, London: The MIT Press.

Newsweek http://www.newsweek.com İET:09.01.2024

OECD (2019). Educating 21st Century Children : Emotional Well-being in the Digital Age.

RIBBLE, Mike (2011). Digital Citizenship in Schools, Second Edition, Washington: International Society for Technology.

TARHAN, Ufuk (2021). Dijital Vatandaşlık ve 9 Elementi. https://www.platinonline.com/yazarlar/ufuk-tarhan/dijital-vatandaslik-ve-9-elementi-1084756 İET:23.12.2023.

SOYDAN, Ersoy (2012). E-kitap Teknolojisi ve Kitabın Geleceği. Batman Üniversitesi Yaşam Bilimleri Dergisi, Cilt 1, Sayı 1, s.389-399.

TERZİBAŞ, Ayhan (2023): E-girişimciliğin Dünya ve Türkiye e-ticaret verileri ışığında değerlendirilmesi: Covid-19 ve öncesi dönemin analizi, Güncel Pazarlama Yaklaşımları ve Araştırmaları Dergisi, 4(1), 39-57. s.40 https://doi.org/10.54439/gupayad.1309682 İET:04.01.2024.

YENİOVA, Gözde (2022, 6 Eylül). Siber Güvenlik Pazarı Büyüyor: Beklenti Nedir?. Ekonomist. https://www.ekonomist.com.tr/makale/siber-guvenlik-pazari-buyuyor-34569 İET:11.01.2024.

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

TECHNOLOGY ETHICS: A PHILOSOPHICAL INTRODUCTION AND READINGS

By Gregory J. Robson and Jonathan Y. Tsou, New York: Routledge, 2023, pp.306, DOI: 10.4324/ 9781003189466

Kamil Tarhan

ORCID: 0000-0003-4668-7920

Technology Ethics a Philosophical Introduction and Readings was edited by Gregory J. Robson and Jonathan Y. Tsou and it was published by Routledge in 2023. The book consisted of five parts and 32 articles. Each article was written by different authors. The first part of book focuses on Perspectives on Technology and Its Value. The second part of book analyses the Technology and the Good Life. The third part of book looks into Computer and Information Technology. The fourth part examines Technology in Business. The final part of book is tried to evolute Biotechnology and the Ethics of Enhancement.

The editors introduce the study by highlighting a world without the internet and technology is now deemed unacceptable. They succinctly outline the unique aspects of their work, emphasizing its significance in the literature. Ethics has become a crucial consideration not confined to specific domains but permeating every facet of social and human life. This study stands out by addressing the ethical dimensions of business and medicine, often overlooked in previous research. The editors aim to contribute with anthological articles, both analytic and continental philosophy, to bridge the existing gap in the literature on the evolving field of technology ethics.

The first part of the work consists of seven different articles as Perspectives and Values of Technology. The articles in this part generally discuss philosophical investigations into the nature of technology and its impact on society. It explores important questions about the definition of technology, its relationship to science, and whether it is value-neutral or value-laden. Two opposing views are presented: instrumentalists argue that technology is a neutral tool shaped by human use, while technological determinists argue that technology influences and even determines social changes.

Technology is defined very succinctly and clearly as "humanity at work" in part one (C. Pitt, 2023, p.14). The focus shifts from the lens of technological infrastructures to the value-laden

nature of technology, emphasizing that assessing the goodness or badness of technology often depends on the context of use. It shows that the value of technology is not innate, but emerges from how individuals use it.

It is a fact that today, an important goal of many cybersecurity policies and government policies is the circulation of information and the dissemination of false information. This study critically examines the role of technology, especially social media, in spreading misinformation and its impact on user behaviour. It challenges the notion of value neutrality of technology, arguing that technology can lead morally decent individuals to contribute to negative outcomes. The overall theme highlights the importance of considering the broader societal impact of technology and recommends a predictable system for technology designers to reduce negative outcomes.

In the first part, the permanence of "technological determinism" is particularly discussed. Technological determinism is defined as the belief that technologies operate independently of society and direct cultural, political and social forms (Wyatt, 2023, p.26). The text highlights alternatives to this view, such as the idea that technology is neutral and its social consequences result from human choices. Essentially, it acknowledges the complex relationship between technology and society, emphasizing that technologies are socially constructed and shaped by human practices.

The first part continues by providing an overview of Martin Heidegger's contributions to the philosophy of technology. It aims to explain Heidegger's philosophy of technology, highlighting its historical, ethical and existential dimensions, as well as its potential for establishing a transformative relationship with technology. Then it explores the ethical significance of technology with a postphenomenological approach and underlines the interconnectedness between humans and technologies. One author challenges the idea that technology is ethically neutral, arguing that technologies play a crucial role in shaping human practices, perceptions, and interpretations, thereby influencing ethical questions such as how to act and how to live (Verbeek, 2023, p. 44).

The second part of the book begins with an exploration of the ethical dimensions of technology, specifically focusing on what constitutes a good life and how technology influences its pursuit. The part delves into historical philosophical debates on the good life,

discussing various theories and questioning the positive or negative effects of technology, particularly the internet and mobile phones. Ethical theories like Aristotelianism, Confucianism, Kantian ethics, and Utilitarianism are applied to topics such as online honesty, the impact of technology on life enjoyment, and broader ethical dilemmas. The goal is to help readers assess how wisely using technology aligns with the pursuit of a fulfilling life.

The articles in this part cover challenges in regulating technology firms, honesty in the technological landscape, Confucian perspectives on technology aligning with societal values, and a critical examination of technology within capitalism from a Marxist viewpoint. In this part, it is also explored the Kantian concept of trust in navigating the complexities of modern technological societies, emphasizing the shared responsibility of technology proponents, regulators, and users in fostering ethically sound trust.

The third part of the book delves into the impact of the Computer and Information Technology revolution on human life, examining both its positive and negative effects. The exploration spans various facets, including artificial intelligence (AI), social media, internet censorship, gender issues, and misinformation in cyberspace.

The following part starts to explore the ethical dimensions of AI systems, arguing that they are not value-free. It emphasizes the importance of considering societal values during AI development, particularly in problem identification, framing, and design phases. The article in this part advocates for a Kantian approach to ensure morally right autonomous machine behaviour, emphasizing the need for a course correction in machine ethics (Wright, 2023, p145-146).

Another article discusses ethical issues with AI technologies in mental health, focusing on Chat_Bots offering Cognitive Behavioral Therapy (CBT) (Tekin, 2023, p.152). It evaluates promises and concerns, emphasizing the need for ethical guidelines in implementing AI for mental health interventions. There is also an article in which privacy rights are highlighted in the trade-off between privacy and security. The author argues that privacy is a fundamental aspect of human flourishing and questions common justifications for extensive surveillance.
It was not overlooked in the study that people today live their lives through social media and screens. Living through screens, suggests screens are fundamentally changing our perceptions and way of being social. The prevalence of screens may be leading to a different kind of

subjectivity and social existence. The dynamics of visibility on social media, particularly TikTok, are explored in a chapter discussing the #BlackTikTokStrike. It underscores issues of visibility, labour, and inequalities for Black creators, emphasizing the need for critical examination of power structures on social media (Rim, 2023, p.175-176).

The gendered and racialized dynamics of visibility in influencer culture on platforms like TikTok are examined in another article. It critically addresses the racialized and gendered labour involved in achieving visibility on social media platforms. Lastly, the concept of fake news examines its characteristics and discusses its impact on public trust, political polarization, and democracy. Approaches to addressing fake news are considered, highlighting the need for a nuanced understanding.

The fourth part addresses critical ethical issues at the intersection of technology, business, and economics, an area often overlooked in discussions of computer ethics. Unlike standard articles that focus primarily on technical aspects, they delve deeply into business ethics, an important but often overlooked area. The discussion begins with Adam Smith applying his insight into the formation of moral sentiments to the contemporary use of technology, especially social media (Otteson, 2023, p.197). The author of the article, also argues that by highlighting enduring psychological similarities between individuals despite technological advances, Smith's principles offer valuable insight into assessing the evolving dynamics of human interaction in the digital age.

On the other hand, the impact of social media platforms such as Twitter, Google, Facebook and YouTube on individuals' access to various information is evaluated. The unprecedented level of information sharing facilitated by these platforms is being investigated and the value of such access is being questioned. Its main focus is on the concept of echo chambers, where users isolate themselves from alternative views by creating personalized information streams. The problem arising in the context of social media and its potential impact on public discourse and civic thought are emphasized. It discusses the ethical implications of individuals actively filtering and blocking alternative viewpoints, leading to the reinforcement of their views and the rejection of competing views. The three main problems that contribute to the exacerbation of echo chambers are the problem of influence of firms, the problem of impersonation and the problem of manipulation (Robson, 2023, p.207-208). These issues contribute to the polarization of political discourse and prevent meaningful interaction with

different perspectives. The echo chamber phenomenon is seen as a threat to democratic discourse and civic virtue. In conclusion, the significance of understanding and addressing the echo chamber issue in social media to ensure a healthier democratic discourse and the development of civic virtues is occurred.

The part continued with an exploration of diversity within technology firms, specifically the relationship between ideological diversity and business performance. It begins by highlighting examples of perceived political bias in select technology firms, highlighting the potential impact of internal cultural biases on decision-making processes. It is argued that due to the significant influence of these technology firms on various aspects of society, they have a social responsibility to ensure that their policies are not distorted by internal biases that discourage different ideological perspectives. It has also been stated that promoting ideological diversity is not only a social responsibility but also a strategic business move. It is argued that technology firms such as Twitter can benefit from cognitive diversity even without significant interactions between individuals who think differently.

Another article delves into the evolving role of Big Tech in corporate activism and highlights its impact on political equality. It introduces the divisive moral goods arising from activism on controversial issues and raises concerns about the influence of these tech giants in shaping democratic processes. The central argument revolves around how Big Tech decided to raise questions about political equality and democratic legitimacy. Finally, in this part, the debate underscores the need for a nuanced legal framework that balances openness, incentives and fairness. The inadequacies of existing models and innovative approaches tailored to algorithms encourage careful thinking and creative legal solutions to address the complex intersection of artificial intelligence, corporate responsibility, and laws.

The fifth part discusses the growing significance of bioethical considerations due to the widespread adoption of biotechnologies in various fields such as medicine, sports, agriculture, and food production. Specifically, it highlights bioethical and biomedical issues related to the use of biotechnologies in medicine and sports, covering topics like genetic enhancement, the role of biomedical technologies, reprogenetic technologies, and doping in sports.

This part also explores the ethical implications of using biomedical technologies for human betterment. It delves into the arguments against enhancement, focusing on the irrational anti-

enhancement perspective. This perspective questions the morality of all or particular forms of biomedical enhancements. This section critically evaluates these arguments, questions their empirical basis, and highlights the potential value in some improvements. It concludes by assessing whether the concerns expressed against the development need a solid justification. Overall, it addresses the complex ethical landscape surrounding biomedical technology and development and sheds light on different perspectives in ongoing debates.

An interesting article examined the intersection of feminism and ethical considerations surrounding reprogenetic technologies. The author discusses the historical development and widespread use of these technologies, highlighting their impact on reprogenetic choices and the disproportionate role of women undergoing relevant procedures. The concerns of feminist scholars are highlighted; It focuses on issues such as the rhetoric of expanding reproductive options, health risks to women, and the values inherent in these technologies. Ethical considerations include questions about autonomy, reinforcement of social norms, and potential injustices regarding access and outcomes.

It challenges the traditional bioethical perspective, especially in the context of biomedical treatment of HIV risk. It has been argued that traditional bioethics, influenced by principles such as respect for autonomy, non-maleficence, beneficence, and justice, has failed to adequately address the complexities introduced by biomedical technologies, particularly in the area of HIV prevention and treatment.

As a result, each article in the book is designed to expand the reader's horizons. Almost all topics have been carefully selected and conveyed to the reader as a summary of today's people's relationship with technology. Each article is very impressive because it reflects a problem in our lives or a situation we are discussing. It is intended to convey to the reader that many of us benefit from technological developments in our lives, but also how these technological developments affect our entire social life without being aware of them. The philosophical discussions within the study are associated with technology in a very appropriate and consistent way.

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.