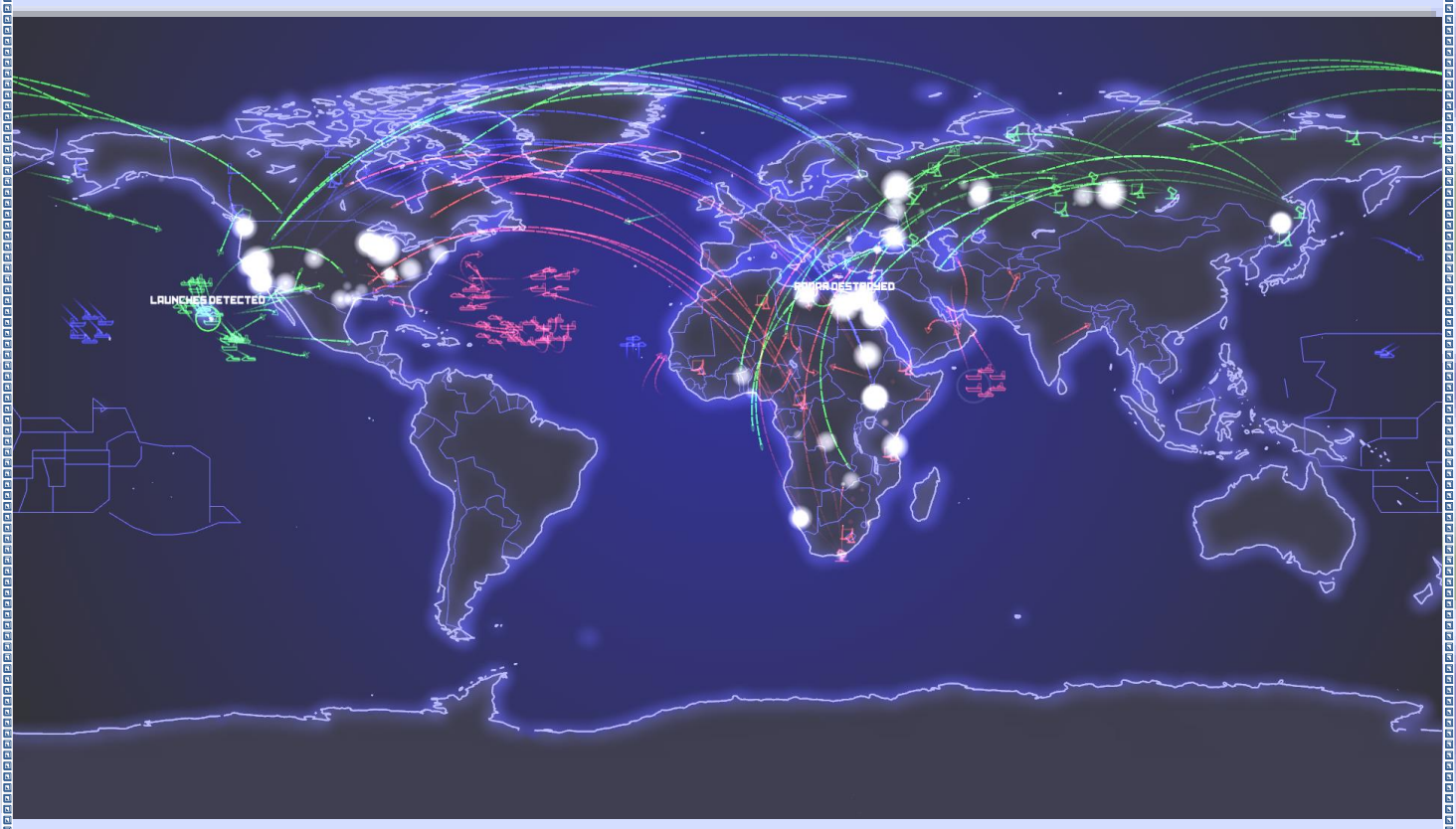
ISSN: 2587-1218

CYBERPOLITIK JOURNAL

Siber Politikalar Dergisi

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

Volume 3 Number 5, 2018



Resource/Kaynak: http://cimsec.org/real-time-strategy-rts-pilot-episode/19439

ISSN: 2587-1218

CYBERPOLITIK JOURNAL
Siber Politikalar Dergisi

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

www.cyberpolitikjournal.org

Summer 2018

ISSN: 2587-1218

ABOUT THE JOURNAL

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.

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 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

Dear Readers,

We are proud to present to you the fifth issue of the *Cyberpolitik* Journal. It is a great honor for all of us to continue our journey that we started three 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 area within our limitations.

This volume deals with a number of topics ranging from cyber conflicts, securitization of cyberspace, cyber warfare, humanitarian law, cyber threats to human rights, music in cyberspace and future industries. There are also rich content in this issue and research that will increase the question marks in our minds. But in this brief discussion, I want to focus on human rights, especially privacy, in cyberspace because of its urgency and importance.

Internet is the most important and most effective tool of the cyber era. It is a simple tool like all other technological developments and products. It is not good or bad in its essence. We get good outcomes if used for good, bad results if used for bad. The Internet is a great blessing for mankind, but at the same time a great threat. There are about 7 billion GB of information flow that enriches human memory every day, and millions of cyber attacks can happen every day again. For this reason, it is an important issue how and why the internet is used?

In terms of human rights, the internet is not necessarily good or absolute bad. There are some of its positive as much as negative impacts in the promotion and protection of human rights. On the one hand, there is the National Security Agency(NSA) that oversights millions of people while on the other side there are people like Edward Snowden who decipher hese activities that violate rights. While governments and global corporations are conducting a series of activities that violate human rights, Wikileaks, which decrypts, is trying to prevent them.

While some human rights are positively affected by cyber technology, some have faced serious risks. Freedom of expression, freedom of assembly and association, the right to participate in social and democratic life, social, economic and cultural rights are positively

affected. Again, freedom of expression (in terms of internet blocking and electronic surveillance) and privacy right are the most negatively affected rights. The most sensitive and the most risky in this regard is the right to privacy. Since without it, it is difficult for man to protect his true humanity and to preserve his honor.

The Universal Declaration of Human Rights, Article 12 defines the right to privacy 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. "* The elements in these article are personal and family privacy, such as private life, family, home, correspondence, honor, fame and name. They are all under the protection of international law and national legislation. But this right and its elements are unfortunately facing the greatest risks on the internet. Everyone we use computers and smartphones as well as social media platforms, from which we face with a number of threats such as electronic surveillance and cyber intelligence.

The phenomenon known as the Snowden incident and the fact that the NSA took the citizens of the United States as well as the entire world under the electronic surveillance is a very big scandal. It turned out that NSA has followed all the subscriptions of Verizon Telekom company and the main servers of global social media companies like yahoo, google, twitter and faceboook (importantly by the consent and permission of these companies). The Snowden documentary shows that a US agent who testified in Germany in this case clearly says that all the intelligence agencies in the world use these programs. In other words, humanity is being watched with local and national eyes beside NSA which is the biggest eye of the world. Besides these, electronic surveillance operated by individual hackers and private companies increase the level of the threats that human rights face.

I want to explain with a simple example how intense people are being watched. In the global cyber surveillance, only about 11% of surveillance is done by companies for advertising. So, you experienced many times that when you talk about something a little later, her ad falls on your phone or computer,. If you search for a hotel or airline tickets or any other product, for a little while then its ads come to your computer or even your mobile phone for days. All this constitutes only 11% of the total electronic surveillance. Intelligence organizations, or state surveillance, are 85%. In other words, this is almost 8 times of the pursuit for advertising purposes. This shows how great threats the human rights and privacy rights are faced with.

Some would argue that if you do not commit a crime, you might not try to avoid it or afraid of surveillance. But, privacy is not for crime, but for the protection of human dignity. There is no continuous crime in the houses, but the curtain is always kept in the house windows, for privacy and human honor.

In short, internet is a useful tool, but there are also serious risks. We can be partly safe as long as we have succeeded in keeping our overseers within the limits of law and human rights, or we will say good-bye to the human rights in the next few years. In this case, the Internet can serve to enslave people in the long run. If there is no consciousness and struggle in this matter, there will be darkness. Keep reading and learning.

Nezir Akyesilmen, Ph.D

Editor-in-Chief

ISSN: 2587-1218

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ

ISSN: 2587-1218

THE IMPLICATIONS OF THE LACK OF A CYBER-CONFLICT DEFINITION

Luis Carlos AVELLA HUERFANO[♣]

Abstract

This article aims in the first place, to answer why a general definition of cyber-conflicts is needed. To do so, it explores the reasons why it has not been possible to create a general definition for this term and what have been the implications of this lack. Among the causes of not having a general definition for the term of "cyber-conflict" it can be found the lack of clarity and rigor in the use of this term and the definition of other terms related to cyber-space that might be confused with each other. In order to better understand the closest approaches to the meaning and definition of what cyber-conflict is, the first part of this paper exposes several definitions of key terms surrounding the concept of "cyber". The second part of the article shows the relationship between the lack of international organizations that regulate or give guidelines regarding cyber-space and the lack of a universal definition of cyber-conflict. The third and last part presents three relevant cases that demonstrate the recent importance of the cyber-space at the state level, its relationship with cyber-conflicts and how the lack of a universal framework prevents a solution to these type of conflicts. After the analysis, the main conclusion of the study is that a universal definition of the term cyber-conflict is required in order to set a framework that allows the development of regulation measurements towards this new threat that the cyber-space has brought.

Key Words: Cyber-conflict, lack of definition, cyber-space, threat, state level, diplomatic crises, lack of regulation.

INTRODUCTION

Technology has become a fundamental part of the human being, is present in everyone's daily life. The use of internet on different platforms such as computers, tablets and smartphones is becoming more common and this has also produced changes in different dynamics, from the simplest and most daily ones such as social relationships to the most complex ones, such as the way international businesses are carried out, the storage of information, banking transactions, political campaigns and even diplomatic relations. Despite

♣ Master Student of Peace and Conflict Studies Master Program, Ankara Social Sciences University, Department of International Relations. E-mail: luis.carlos.avella@gmail.com

their advantages, new technologies also represent a risk to the safety of people, companies and states through different threats.

These threats have different levels: personal, such as hacking of personal email accounts or social networks and different informatic viruses that affect computers or mobile devices; Corporate level, such as attacks between companies to steal information and / or sabotage the competition; And at the state level, such as the theft and leaking of information between different states to generate diplomatic crises, attacks to damage government websites, hacking and black propaganda to sabotage democratic elections, and even virus attacks capable of causing physical damage on state infrastructures. This last approach will be the focus on the present article.

These new threats the states have been facing in recent years have generated tensions within and between states. Some scholars have called this phenomenon as "cyber-conflicts". However, there is no general definition of this term and often changes the meaning depending on the perspective that is used to analyze the phenomenon. There is also a problem in the use of terminology, since many times academics, researchers and journalists use terms such as cyber-space, cyber-attacks, among others, without rigor and consequently, causing confusion. The lack of a general definition of cyber-conflicts leads to the absence of a general path or policy for all states to end or control these conflicts. For this reason, this paper will attempt to answer why a general definition of cyber-conflicts is needed.

To answer the question, this research work will be of a descriptive nature and a literature review of primary and secondary sources, such as official documents and academic texts, will be carried out. The work will be divided in the following way: first, due to the problem in the use of terminology (cyber-, cyber-space, cyber-attacks), some definitions will be presented that will help to better understand what cyber-conflicts are; then, a summary of the institutions that are working on the definition of the term cyber-conflict will be presented; after that, some cases will be presented to expose the phenomena of cyber-conflicts and finally the conclusions.

1. BASIC DEFINITIONS TO UNDERSTAND WHAT CYBER-CONFLICT IS

These days, when reading the press or listening to the news, terms such as cyber-, cyber-space or cyber-attacks are used without any distinction; although they are related, do not have the same meaning. To have more clarity about their meaning and understand better these terms, some of the most complete definitions of these concepts will be presented and compared.

The term “cyber” according to the Oxford dictionary (2018) is defined as "Relating to the characteristics of the culture of computers, information technology, and virtual reality". For Kleinsteuber (2002) cyber- is a prefix taken from an older word although recent, “cyber-netic”, which has a Greek etymological root; comes from "kybernetike", whose meaning is “the art of navigation”. In Tallinn Manual (2013) it is said that "Connotes a relationship with information technology". As it can be seen in the Strategy on Cyber-Security of Montenegro to 2017 (2013), the term cyber- is referred as "anything related to, or involving, computers or computer networks (such as Internet)". Finally, one of the definitions that explains best what the term “cyber-” is can be found in Finland's Cyber-Security Strategy Government (2013):

> The word ‘cyber-’ is almost invariably the prefix for a term or the modifier of a compound word, rather than a stand-alone word. Its inference usually relates to electronic information (data) processing, information technology, electronic communications (data transfer) or information and computer systems. Only the complete term of the compound word (modifier + head) itself can be considered to possess actual meaning. The word cyber- is generally believed to originate from the Ancient Greek verb κυβερεω (kybereo) to steer, to guide, to control”.

As seen, these definitions have something in common: they consider that the term "cyber" on its own does not have a specific definition, or give any full meaning.

Despite the first impression, the term cyber-space is not a univocal term. Cyber-space, as cyber-culture or globalization, is a term used in different ways, in different contexts and with different purposes. Brunner (2018) describes cyber-space, based on its structure, as "the virtual geography created by computers and networks". Following this, it has been equated to information highways, understood as the common space created in telematic networks. Cyber-space has also been defined as the field of communications constituted by a computer network (El Mundo, 2018).

Hans Kleinsteuber (2002, p.47) presents a more restricted concept of cyber-space to differentiate it from information superhighways. Based on the so-called Magna Carta of the Information Age, of 1994, he characterizes those, among other features, because they are limited in their content by the power of State's Control and the tendency towards centralization and bureaucratization. Cyber-space, on the other hand, would have exactly the opposite characteristics.

In the Tallin Manual (2013) cyber-space is defined as "The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks". The United Kingdom Cabinet Office (2011) defines it as "An interactive domain made of digital networks that is used to store, modify and communicate information. It includes the internet but also other information systems that support our businesses, infrastructure and services". The Prime Minister Office of Israel (2011) defines this term as "the physical and non-physical domain that is created or part of all of the following components: mechanized and computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data ".

According to the previous definitions of cyber-space, the following can be said: there is no universal or general definition about the term, each country or author includes or excludes factors within definitions. The most complete definition is the one made by Prime Minister Office of Israel (2011), since it links the physical part of cyber-space (hardware), the virtual part (software, internet) and the human part (the user) within the definition.

In terms of cyber-attacks, the Tallinn Manual (2013) defines this term as "a cyber- operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects". The UK Cabinet Office (2011) defines it as "anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated goals such as: gaining unauthorized access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems)". NATO (2014) defines cyber-attacks as an "action taken to disrupt, deny, degrade or destroy

information resident in a computer and / or computer network, or the computer and / or computer network itself".

As for cyber-conflicts, there is really very little that has been researched and written about it, although there are several academic texts and researches that mention the topic, these are not enough and often do not receive the importance they deserve. One of the most complete definitions of this term, given by Henry J Sienkiewicz in his book "The Art of Cyber-Conflict" defines the term cyber-conflict as "the use of computational means, via microprocessors and other associated technologies, in cyber-space for malevolent and / or destructive purposes in order to affect, change or modify diplomatic and military interactions between entities "(2017, p 90). This definition limits cyber-conflicts to the relationship between states, meaning that an attempt to hack a personal email of a student or any worker for the purpose of generating personal tensions cannot be defined as a cyber-conflict, but if the hacking attempt aims to generate diplomatic or military tensions between two states, and it succeeds, it is a cyber-conflict.

Brandon Valeriano and Ryan C. Maness in their book "Cyber-War Versus Cyber-Realities" (2015) wrote about the importance of terminology and the importance of researching and theorizing more on the subject of cyber-conflicts. They also made a summary of cyber-disputes among rival states, like China, the United States, India, Japan, North Korea and Russia from 2001 to 2011, in which it is explained that the attacks between states do not necessarily end in a cyber-conflict: "Only 16 percent of all rivals have engaged in cyber-conflict. In, total, we recorded 111 cyber-incidents and 45 disputes over the period of relations among the 20 rivals "(p, 88). This shows that many times the states allow "small attacks" that they do not consider so dangerous for political and military stability and do not see the need to start a cyber-conflict.

Despite the existence of these definitions and the attempts of several academics to give an universal definition of cyber-conflicts, there is not yet one that is accepted globally and there is, so far, no international organization or authority that covers the majority of countries that are working on this problem.

2. INTERNATIONAL ORGANIZATIONS AND CYBER-CONFLICTS

One of the reasons why there are currently no standardized definitions of terms such as cyber- conflict, cyber-war, cyber-attacks, etc. is the lack of an international authority or organization of a global nature that can set the guidelines, principles, rules and norms on the topics related to cyber-space. In the last 20 years the concern for the ethical, legal, political and anthropological problems of cyber-space has been accentuated throughout the world and worldwide examples are proof of it: the celebration of the Round Table on Cyber-culture, held in the city of Hannover in 2000; the 2000 Infoethics Seminar of governmental experts from Latin America and the Caribbean on "The Right to Universal Access to Information in the XXI Century: The Ethical, Legal and Sociocultural Challenges of the Information Society for Latin America and the Caribbean "; and the celebration of the III International Congress of UNESCO on the Ethical, Legal and Social Challenges of Cyber-space, which took place in Paris on November 15, 2000. However, it was not until the attacks of Estonia in 2007 that the international community realized the real importance of cyber-space and how it could be a risk for the development of relations between states and could represent a danger to the security of every country.

Internally, the states have begun to create measures to face the new problems that cyber-space brings; One of those measures is the creation and implementation of guidelines and / or cyber-security strategies. Many countries so far have their own document regarding this topic; however, the definitions and scope of the strategies are often different. Likewise, the measures and punishments of offenders vary from country to country: these measures are frequently insufficient, since cyber-space has no borders and cyber-criminals often do not reside within the country they affect, revealing the need for establishing international binding strategies and standards on cyber-space.

At a supranational level, the United Nations (UN) created the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GEG). However, as Orcutt (2017) describes, this group that was created to define how the current international legislation should be applied to cyber-space, failed in reaching a consensus in the terminological use. Despite this, they made some progress in the development of some non-binding rules, such as the one that claims that one state should not attack the critical civil infrastructure of another in times of peace. At the

beginning of 2017, the GEG did not reach a consensus and did not submit a report to the UN General Assembly. This failure of the UN led to the creation of a new commission that includes both public and private representative as well as academicians that aims to develop a guide of good practices and clarify how to apply international law to new cyber-conflicts. This commission is called Global Commission on the Stability of Cyber-space.

On the other hand, NATO, after a proposal from Estonia, created in 2007 the "NATO Cooperative Cyber- Defense Center of Excellence" (CCDCOE) in Tallinn. The majority of the member countries of NATO participate in this commission and hold regular meetings to discuss progress and problems and to provide solutions. Representatives from different states and academics participate in these meetings. This has been the only international commission that has so far discussed the problem in the definition of cyber-conflict, being a recurring theme in its meetings and publications. One of the problems that have been identified thanks to this commission is that there is very little academic information about cyber-conflict, also a problem in the use of the terms (the use of the term cyber-war instead of cyber-conflict), as well as the lack of researchers working on these issues. Despite the efforts of the CCDCOE, a globally accepted definition of cyber-conflicts has not yet been reached (Herzog, 2011, p.55).

3. RELEVANT CASES

Below there are three cases that demonstrate the importance of terminology and a definition of cyber-conflict and the consequences of not having an international authority that can regulate the cyber-space through the statement of a universal framework. The first case is the attacks in Estonia in 2007, this case shows, among many other things, that the states were not prepared to respond to the threats of cyber-space, and it is from this moment that terms such as cyber-attacks, cyber-war or cyber-conflict begin to become popular in the international arena. Then we have the case of Stuxnet; this case is also relevant since it showed that cyber-attacks not only put at risk information but also can affect the physical infrastructure of the states. Finally, there is the case of cyber-attacks from China to the United States that resulted in major diplomatic crises.

3.1. The Estonia Attacks: On April 27th, 2007, a series of cyber-attacks began, that affected several websites of organizations in Estonia, in the context of a conflict between Estonia and Russia over the relocation of the Tallinn Bronze Soldier, a Soviet monument of the II World War (McGuinness, 2017). The main objectives were the websites of the Estonian Presidency and Parliament, most of the ministries, political parties, three of the most important media corporations in the country and two important banks. The crisis unchained a wave of denial of service (DDoS) attacks; where websites are flooded with thousands of visits that "jam" them and clog the bandwidth of servers. Another type of attack identified was the use of "botnets" for the massive distribution of spam.

The first reaction of the Estonian Foreign Affairs' Minister Urmas Paet was to accuse the Kremlin of being directly involved in the attacks. However, the Minister of Defense accepted that they lacked evidence to make such an accusation (Traynor, 2007). So far, neither NATO nor the European Commission has found any evidence of any involvement from the Russian government. Only an Estonian citizen with Russian origins has been convicted, who ended up admitting his guilt for attacking the site of the Estonian Reform Party.

The attacks triggered the importance of the issue of cyber-security in the modern militia. NATO undertook political actions after a meeting and a communiqué issued from Brussels in June 2007, which ultimately resulted in the creation of the Cooperative Cyber-Defense Center of Excellence. It has been operating since 2008 and its mission is to become the main source of information regarding cyber-defense (Tamkin, 2017).

What can be seen in this case is that, first, the states were not prepared for cyber-attacks; the efforts of the states have historically focused on strengthening their security and defense, however these efforts only focused on the physical aspect and forgot to reinforce security and defense in the cyber-space. Second, thanks to this case, organizations such as NATO have tried to respond to threats and have begun to investigate and try to define this new problem that states face. Finally, it shows that the lack of an authority or organization to regulate the cyber-space and the difficulty of demonstrating the guilt of an individual, organization or state are the causes that make impossible to punish or implement sanctions against the real responsible of the cyber-attacks.

3.2. Stuxnet, the first "cyber-weapon": On January 2010, inspectors from the International Atomic Energy Agency visiting a nuclear plant in Natanz, Iran, noted that the centrifuges used for uranium enrichment were failing. Interestingly, the Iranian technicians who replaced the machines also seemed amazed (Holloway, 2015). The phenomenon was repeated five months later in the country, but this time the experts could detect the cause: a malicious computer virus. The "worm" - now known as Stuxnet - took control of 1,000 machines involved in the production of nuclear materials and instructed them to self-destruct. It was the first time that a cyber-attack succeeded in damaging the infrastructure of the "real world" (Kelley, 2013).

3.3.

After the attack in Iran, Stuxnet has infected more than 100 thousand computer systems around the world (Zetter, 2014). At first, the worm seemed to be one of the bunch, created to steal information. However, the experts soon determined that it contained code specifically designed to attack Siemens Simatic WinCC SCADA systems that are responsible for controlling the handling of pipelines, nuclear plants and other industrial equipment (Pazulka, 2016).

According to Nakashima and Warrik (2012), the United States and Israel would be behind the creation of this "Worm" and the subsequent attack on Iran. However, there is insufficient evidence to blame a specific agency or individual, and consequently, to generate sanctions.

This case shows that cyber-attacks can also affect the tangible world, and like the case of Estonia, shows the difficulty of punishing the guilty, because although there are many signs of the culprits behind the Stuxnet virus, there is not enough evidence to be able to apply sanctions to the states behind this attack.

3.4. China vs. USA: In early 2010, Google reported that it had detected a cyber-attack from China that had breached the company's security wall and had accessed to its servers. At first, it was reported that the attackers wanted to have access to the email accounts (Gmail) of prominent Chinese opponents, such as Ai Weiwei. Google did not facilitate the investigation launched by the FBI at its headquarters in Mountain View and began a legal dispute with the US security agency to prevent its agents from accessing sensitive company information

related to its technical operation (Nakashima, 2013). Time later, it was known that the cyber-attacks against Google and other US companies, in addition of having a nature of industrial espionage and anti-opposition, could have had the main purpose of counterintelligence (Markoff, 2011). Apparently, as described by Zetter (2010), hackers in the service of Chinese state agencies would have launched Operation Aurora to control the information held by US agencies about Chinese intelligence agents operating within the territory of the United States.

3.5.

A few years before this attack, another assault from China managed to violate the defenses of the US military computer system by staying active for almost two years, between 2003 and 2005. That attack, known as Titan Rain, infiltrated mainly private contractors of defense, although it also penetrated the systems of NASA (Thornburgh, 2005).

In June 2015, China hacked the U.S. Office of Personal Management's systems, leaking more than 4 million sensitive records. The U.S. government's only viable response was economic sanctions against companies and individuals (Hirschfeld, 2015).

This final case demonstrates that every state is vulnerable to cyber-attacks, including the United States. It also shows the scope that this type of attacks can have, generating diplomatic instability even in two countries as powerful as China and the United States. Like the two previous cases, this case also demonstrates the impossibility of generating sanctions or demonstrating the guilt of a government, in this case the Chinese government, in the cyber-attacks on the United States.

CONCLUSION

As seen in this paper, there are several factors that have hindered the definition of the term cyber-space and its related issues, such as cyber-conflicts, cyber-attacks, etc., from happening. First, the use of these terms without the necessary academic rigor from states, researchers, journalists, among many others that lead to misinformation and confusion; Second, the lack of research creates an important hole in the field, although there are several investigations regarding this topic, they are not enough to build a strong base of knowledge and some of the existing ones, are not as well appreciated as they deserve to be. Finally,

there is a lack of an international organization or authority that regulates cyber-space issues through a universal framework, that can set guidelines, definitions and even sanctions.

While it is important to have a generally accepted definition of several terms related to cyber-space, is the term cyber-conflict which has the greater importance because it directly affects states, as seen with the given examples. Unfortunately, as long as the term does not have a globally accepted definition, it will not be possible to generate guidelines and rules to regulate this phenomenon. Simultaneously, there is a need for an international organization acting as the authority on this matter, responsible of the creation of these guidelines and rules under a global framework and capable of managing and controlling every issue regarding cyber-conflicts. Without the definition and the organization, it will not be possible to regulate and mitigate properly a cyber-conflict and its consequences. This is why it is necessary that the debates about the definition matter and the researches of the cases continue, in order to generate an academic base on which international organizations can support themselves to generate the regulations needed by the cyber-space and eventually, create the authority that is required.

Bibliography

Brunner, J. 2018. Cibercultura: la aldea global dividida. Retrieved from: https://www.researchgate.net/publication/265287580_cibercultura_la_aldea_global_dividida

El Mundo. 2018. Diccionario el Mundo. Retrieved from: http://diccionarios.elmundo.es/diccionarios/cgi/lee_diccionario.html?busca=Ciberespacio&diccionario=1

Finland. 2013. Finland's Cyber-Security Strategy Government Resolution 24 Jan 2013. Retrieved from: http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber--security-strategy.

Herzog, S. 2011, Revisiting the Estonian Cyber- Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, Vol. 4, No. 2: 49-60, 2011. Retrieved from: https://ssrn.com/abstract=2807582

Holloway, M. 2015. Stuxnet Worm Attack on Iranian Nuclear Facilities. Retrieved from: http://large.stanford.edu/courses/2015/ph241/holloway1/

Hirschfeld, J. 2015. Hacking of Government Computers Exposed 21.5 Million People. Retrieved from: https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

Kelley, M. 2013. The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. Retrieved from: http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

Kleinsteuber, H. 2002. El surgimiento del ciberespacio: la palabra y la realidad en Vidal Beneyto, J. (Editor): La ventana global, Taurus, Madrid, 2002, pp. 47.

University of Oxford. 2018. Oxford Dictionary. Retrieved from: https://en.oxforddictionaries.com/?utm_source=od-panel&utm_campaign=en

McGuinness, D. 2017. How a cyber- attack transformed Estonia. Retrieved from: http://www.bbc.com/news/39655415.

Montenegro. 2013. Strategy on Cyber- Security of Montenegro to 2017 (2013). Retrieved from: https://ccdcoe.org/strategies-policies.html.

Nakashima, E. 2013. Chinese hackers who breached Google gained access to sensitive data, U.S. officials say. Retrieved from: https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html?utm_term=.d72ebcb4c83e.

Nakashima, E & Warrick, J. 2010. Stuxnet was work of U.S. and Israeli experts, officials say. Retrieved from: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.25cd42acad75

NATO. 2014. NATO AAP-06 Edition 2014. Retrieved from: http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf

Orcutt, M. 2017. El nuevo vigilante privado de la geopolítica y el ciberconflicto internacional. Retrieved from: https://www.technologyreview.es/s/8812/el-nuevo-vigilante-privado-de-la-geopolitica-y-el-ciberconflicto-internacional

Pasulka, N. 2016. A Virus Altered the Face of Security in Iran. Retrieved from: http://www.takepart.com/article/2016/07/25/zero-days-stuxnet-iran.

Prime Minister Office of Israel. 2011. Advancing National Cyber-space Capabilities, Resolution No. 3611 of the Government of august 7, 2011 – 2011. Retrieved from:

http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber-/Documents/Advancing%20National%20Cyber-space%20Capabilities.pdf

Sienkiewicz, H. 2017. The Art of Cyber- Conflict. Dog Ear Publishing, (pp. 5-180).

Tallinn Manual. 2013. Tallinn Manual on the International Law Applicable to Cyber-Warfare – 2013. Retrieved from: https://ccdcoe.org/tallinn-manual.html

Tamkin, E. 2017. 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber- Threats?. Retrieved from: http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber--threats/

Thornburgh, N. 2005. Inside the Chinese Hack Attack. Retrieved from: http://content.time.com/time/nation/article/0,8599,1098371,00.html

Traynor, I. 2007. Russia accused of unleashing cyber-war to disable Estonia. Retrieved from: https://www.theguardian.com/world/2007/may/17/topstories3.russia

United Kingdom Cabinet Office. 2011. UK Cyber- Security Strategy (2011). Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber--security-strategy-final.pdf

Valeriano, B & Maness, R. 2015. CYBER- WAR VERSUS CYBER- REALITIES: CYBER-CONFLICT IN THE INTERNATIONAL SYSTEM New York, NY: Oxford University Press, 2015, 288 pages. ISBN: 9780190204792

Zetter, K. 2014. AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON. Retrieved from: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zetter, K. 2010. GOOGLE HACK ATTACK WAS ULTRA SOPHISTICATED, NEW DETAILS SHOW. Retrieved from: https://www.wired.com/2010/01/operation-aurora/

ISSN: 2587-1218

SİBER ÇATIŞMALARIN TANIMLAMA SORUNU

Gül Nazik ÜNVER[♣]

"Bir Tanım Seçmek Bir Nedeni Savunmaktır."
Charles Leslie Stevenson (1908-1979)

Özet

Son yirmi yılda yaşanan gelişmeler, insan yapımı yeni bir çatışma alanı ortaya çıkarmıştır. Kara, deniz, hava ve uzay alanlarında silahlı çatışmaların yanı sıra, farklı siyasal aktörler arasındaki çatışmalar, artık siber uzayda yer almaya başlamıştır. Siber çatışmalar, çeşitli değişkenlerin -teknolojik, sosyal ve entelektüel- değişen ilişkilerinden dolayı ortaya çıkmaktadır. Belirli bir kuvvet, eğilim, hareket veya politikadaki değişim, siber çatışmayı oluşturabilir. Siber çatışmalar farklı nedenlere bağlı olarak zaman zaman artışlar ya da azalmalar göstermektedir. Siber çatışmaların tanımlanmasındaki sorunlar hakkında kesin bir değerlendirme yapmak zor olsa da, siber operasyonların daha önemli hale gelmesi sadece bir zaman meselesi olmaktadır. Yapılacak her tanımlama, siber çatışmaların bir boyutunu dışarıda bırakacaktır.

Bu çalışmanın ana amacı, dijitalleşen dünyada siber çatışmaların tanımlama sorunları hakkında "NATO Uluslararası Siber Çatışma Konferanslarını" incelemekte ve siber çatışmaların hem teknik hem de toplumsal bakış açılarındaki unsurlarının kapsamlı bir analizine dayanmaktadır. Son olarak çalışma, en ciddi tehdidi getiren ve etkisi kitle imha silahları ile karşılaştırılabilir olabilen, modern savaşın en gelişmiş biçimi olarak siber çatışmayı değerlendirmek için bir fırsat sunmaktadır.

Anahtar Kelimeler: Siber Uzay, Siber Çatışma, İnternet, Siber Terörizm, Dijitalleşme.

♣ Doktora Adayı, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler ABD, gulunver@outlook.com.

Abstract

The developments in the last two decades have revealed a new area of human-made conflict. Armed conflicts in land, sea, air and space areas, as well as conflicts between different political actors, are now beginning to take place in cyberspace. The cyber conflicts arise due to the changing relations of various variables - technological, social and intellectual. Any change in a particular force, tendency, movement, or policy can create a cyber conflict which occasionally increase or decrease depending on different reasons. While it is difficult to make a definitive assessment of the problems with identifying cyber conflicts, it is only a matter of time before cyber operations become more important. Every definition to be made will exclude a size of cyber conflicts.

The main aim of this work is to examine the "NATO International Conference on Cyber Conflicts" on the identification problems of cyber conflicts in the digitalizing world and to rely on a comprehensive analysis of the elements of both cyber space and cyber conflicts. Finally, the study presents an opportunity to evaluate cyber conflict as the most advanced form of modern warfare, which brings the most serious threat and can be comparable to weapons of mass destruction.

Keywords: Cyber Space, Cyber Conflict, Internet, Cyber Terrorizm, Digitization.

1. Giriş

Uluslararası ilişkiler teknolojiden genellikle derin bir şekilde etkilenmiştir. Okyanustan geçen yelkenli gemiler, 16-18. yüzyıllarda Avrupa'nın genişlemesini sağlamıştır. Telgraf 19. yüzyıl imparatorlukların gelişmesinde katkıda bulunmuştur. Uçak, radyo ve televizyon 20. yüzyılda uluslararası ilişkilerin etki alanını değiştirmiştir. İnternet ise dünya için yeni bir dizi fırsat ve risk ortaya çıkarmaktadır. Bilgi (IT) sistemleri, insanların hem birebir hem de birden çok iletişim kurma yeteneğinde bir kuantum sıçraması oluşturmaktadır. İnternetin diğerlerinden temel farkı, değişikliklerin daha hızlı gerçekleşmesidir. İnternet eylemcilerin bilgileri toplamasına ve yayınlamasına, diyaloga girmesine, eylemlerini koordine etmesine ve gücü elinde bulunduranlara lobi yapmasına izin vermektedir.

Siber çatışma, siber bilgi savaşı, suç faaliyetleri (terörizm dahil), gizli operasyonlar ve önleyici askeri güç kullanma kabiliyetleri, uluslararası toplumun bunları yönetmek için kararlaştırılmış kurallar oluşturma kapasitesinden daha hızlı yayılmaktadır. Siber yetenekler daha hızlı ortaya çıkabilir ve gelişebilir; nükleer santraller ve silahlar, hava taşımacılığı, radyo vb. gibi öncekilere göre daha kapsamlı ve hızlı bir şekilde yayılabilir. Siber yetenekler, önceki teknolojilere göre coğrafi olarak daha az sınırlıdır. Bununla birlikte, devletlerin ve toplumların doğal çıkarları, bu yeni kabiliyetleri yönetmeye yönelik normların ve kuralların, uygulamalarının kusurlu olmasına rağmen, teklif edilmesi, müzakere edilmesi ve nihayetinde üzerinde anlaşmaya varılması gerektiğini dikte etmektedir. Zira, çoğu devlet ve toplum için tehdit edici faaliyetlerin tehlikeleri ve maliyetleri çok ağır olacaktır. Son on yıl boyunca, küresel sosyal ve politik manzaralar, Bilgi ve İletişim Teknolojilerinin (BİT) devrimci gelişimi tarafından değişime uğramaktadır. Yeni Bilgi ve İletişim Teknolojileri, ağ merkezli savaş doktrini ve alışılmamış, bilgi ve asimetrik savaşın ortaya çıkmasıyla diğer yolların yanı sıra savaşları da önemli ölçüde etkilemiştir. Siber savaş, askeri düzeyde bilgiye dayalı çatışmayı ifade ederken, ağ bağlantılı savaş çoğunlukla düşük yoğunluklu çatışmalarla ilişkilendirilen toplumsal mücadeleler için geçerlidir (Brose, 2015: 26).

Uluslar, gelecek çatışmaları daha fazla kontrol altına almak için tıpkı daha geleneksel savaşların anlaşmalar, sözleşmeler ve normlar yoluyla sınırlandırıldığı gibi giderek daha fazla çatışmaya yönelmektedir (Cycon, 2011: 21). Ancak, eski anlaşmaların ne kadar iyi tutacağı, siber uzayın ve siber çatışmaların doğası gereği ne icat edilmesi gerektiği hala bilinmemektedir. Günümüzde gelişmiş ulusların karşılaştığı siber çatışmaların çoğunda, bir aktörün siber uzayda düşmanca müdahaleleri seçmeyi tercih etmesini engellememekte, ancak çok başarılı olan müdahaleleri durdurmaya zorlamaktan alıkoymaktadır (Cycon, 2012: 126).

1999 Kosova operasyonu, NATO'nun siber çatışma ile ilgili ilk deneyimi olarak etkili olmuştur. NATO'nun Kosova Savaşı esnasında mail sunucuları hedef alınmıştır. Bu çatışma sırasında, her taraftaki eylemciler ve saldırganlar örgütü yaymak ve / veya propaganda yapmak için kullanılmasının yansıra temel hedef NATO'nun hava saldırısını durdurmak olmuştur. Ayrıca, dikkate değer bir dizi web sitesi protesto ve propaganda amaçları için hırsızlıklar ve bozulmalar yaşanmıştır. Bazı durumlarda, hacktivistler virüs yüklü ekler göndermiştir. Çatışmanın hemen önündeki partilerin ötesinde, Belgrad'daki Çin

Büyükelçiliği'nin kazara ABD'yi bombalaması sonrasında Çin'den hackerlar dâhil olmuştur (Denning, 2001: 239-240).

Estonya'ya yönelik 2007'deki siber saldırı, siber çatışmada NATO'nun en bilinen olayı olmuştur. Sovyet savaş anıtının taşınma kararının alınması ile birlikte saldırılar başlamış, Estonya'daki etnik Ruslar protestolar için sokaklara çıkmışlardır. Protestolar çevrimiçi olarak yayılmıştır (Erendor, 2017:114-133). Tallinn'deki NATO Kooperatifi Siber Savunma Merkezi'nin (CCDCOE) Rain Ottis (2010: 72) raporuna göre; "Siber saldırıların Estonya'daki insanlara doğrudan etkileri minimal olmuş ve çoğu durumda var olmamıştır. Altyapı hizmetleri kalıcı olarak etkilenmiştir." Bununla birlikte, saldırılar hem Estonya hem de NATO için "uyandırma çağrısı" olmuş ve her ikisi için de politikadaki değişikliklere yol açmıştır (Lawson, 2012: 3). 2013 yılında gerçekleşen Uluslararası Siber Çatışma Konferansı'nda, Kalm; siber çatışmanın ve siber suçun tanımları üzerine tartışma çok fazla olduğundan, aralarında ayrım yapmamıştır. Aksine, herhangi bir siber çatışmanın teknoloji tarafından sağlanan suç eylemlerinden oluştuğunu varsaymıştır. Farklı suç eylemleri farklı örgütsel yapılar gerektirdiğinden siber uzayda gizli ağlar çeşitli biçimlerde olabilir (Kalm, 2013: 218). Devlet destekli siber suç örgütleri siber çatışma bağlamında en ağır tehditleri uyguladıkları için diğer türden gizli ağlara maruz kalan pek çok özellikten yoksun kalmışlardır. Devlet destekli siber suçlar çoğunlukla casusluk ve teknik operasyonları içerdiğinden, önemli miktarda kaynak gereklidir (Kalm, 2013: 224).

Çatışma, çok boyutlu ve çok kapsamlı bir kavram olarak disiplinden disipline farklı tanımlara sahiptir. Yapılacak her tanımlama, çatışmanın bir boyutunu dışarıda bırakacaktır (Akyeşilmen, 2013: 449). Genel itibariyle çatışma terimi ifade, görüş, menfaat, gaye veya değerler arasındaki karşıtlık veya uyumsuzluktur. Çatışmaların iki yönü vardır. Bunların birincisi taraflar arasındaki menfaat ya da fikir uyuşmazlığıdır. Diğeri ise bu anlaşmazlıkların fiziki müdahaleye başvurma ya da tartışmalar yoluyla gözlemlenebilir "çatışma davranışı" olarak ortaya konmalarıdır. Çatışma davranışı sergilemek, iletişim aracılığıyla veya güç kullanarak tarafların ihtilaflarını dile getirmeleri anlamına gelmektedir (Tekin, 2013: 87). Çatışma terimi ile ilgili yapılan tanımlamaların ortak noktası, aslında mücadele eden en az iki tarafın varlığı, bu iki taraf arasında bir tür karşılıklı bağımlılığın bulunması ve tarafların amaçlarına ulaşmasında diğer tarafın önleyici bir unsur olduğu algısının oluşmasıdır (Akyeşilmen, 2015: 42-43). Siber uzayda bireyler ve aktörler giderek yaygınlaşırken,

yaşanan her çatışma sorun haline gelmiştir. Bu nedenle konu ile ilgili literatür taraması yapılmakta ve çalışmanın yanıt aradığı temel sorular şu şekilde sıralanmaktadır:

Siber alanda sayısız çatışma varken ve giderek farklı türde çatışmalar ortaya çıkarken bu disiplinin tanımlanamaması sorun teşkil eder mi? Ya da genel bir tanım yapılması, giderek genişleyen siber uzayda yeterli kalabilir mi? Çatışma ne zaman başlamıştır? Şu an çatışmanın durumu nedir?- hangi safhadadır? United Nations Development Programme (UNDP)'ye göre çatışma çok boyutlu bir fenomen olduğundan tek bir faktörle açıklanamamaktadır. Siber çatışmayı etkileyen ve zorlaştıran en önemli unsur aslında sayılamayacak kadar çok olan, herkese göre değişebilen ve aysberg misali büyük bir kısmı görünmez olan nedenlerdir (Akyeşilmen, 2013: 9-10).

"NATO Uluslararası Siber Çatışmalar Konferansında" siber çatışmaları önlemek ve barışçıl bir çözüm bulmak adına ne gibi çalışmalar yapmaktadır? Peki devlet egemenliğinin ve hukuki yaptırımın oldukça güçlü olduğu iç meselelerde/sorunlarda siber çatışmalar tanımlanamaz olması nasıl açıklanabilir? Siber çatışmalar devletlerarasındaki çatışmalar seviyesini artırıyor mu?, yoksa *siber olayın ya da anlaşmazlığın türü ve şiddeti temelinde farklı çatışma ya da işbirliği dinamikleri var mıdır?* Siber kötülük, (DDoS) saldırılarının yalnızca devletlerarasındaki çatışma-işbirliği dinamiklerini etkilediği görülmüştür (Maness and Valeriano, 2015: 2). Her ne kadar bazı teorisyenler siber çatışma ve siber savaşı epistemolojik farklılıklarına bakılmaksızın birçok kez beraber aynı cümlede, hatta çoğu kez birbirinin yerine dahi kullanmaktadır. *Bu kadar geniş yelpazeye sahip bir alanı kapsayan çatışma yönetimine göre siber çatışma nedir? Çatışmanın çeşitleri var mı? Siber Çatışma sınıflandırılabilir mi? Siber çatışma, ulus-devletlerde ne gibi zararlara sebep olmaktadır?* Bu sorular gibi daha fazla pek çok soruya cevaplar verilmeye çalışılacaktır.

Siber uzayda şiddet içerikli kafa karışıklıklarının değerlendirilmesinin üzerinde durulduğu "Conflict Barometer"'de iddia edilen taraflar arasındaki somut eylemler ve iletişim, araçların nitel ve nicel göstergelerini ve şiddetin sonuçlarını birleştirerek değerlendirmektedir. Bu yaklaşım, özellikle şiddetlerle ilgili olarak, daha geniş ve daha ayrıntılı bir ampirik temele ilişkin politik karışıklıkların analizini vermektedir. Bu, sunulan söz konusu bilginin doğruluğunu, güvenilirliğini ve tekrarlanabilirliğini daha da geliştirmeyi amaçlamaktadır. Bu nedenle siber çatışmayı incelerken, 2017 yılına kadar Heilderberg Enstitüsü'nde yapılan

(Conflict Barometer 1992'den bu yana, çatışma süreçlerine odaklanarak örneğin savaşın zayiatının tamamen nicel eşiklerinden ziyade siyasi anlaşmazlıkları analiz etmiştir.) uluslararası çatışmaları ele almak gerekmektedir (https://hiik.de/conflict-barometer/, er.tar.: 22.04.2018). Çalışma siber çatışmada devletlerin karşılaşabileceği ve siber operasyonların rol oynayabileceği bir dizi yüzleşme ve karmaşıklık ihtimallerine anlam çıkarmak için geniş bir tarih yelpazesinden analojileri araştırmaktadır. Dahası siber çatışma olaylarını, bunlara dâhil olan aktörleri ve araştırmacılar tarafından yararlı olacak şekilde tanımlamaların ötesinde yaşanan sorunlara ilişkin inceleme yapmaktadır. Bu çalışmanın amacı, siber çatışmanın NATO'nun ele almaya çalıştığı güçlüklere karşı genel bir bakış sağlamaktır. Çatışma tanımlanabilir mi / tanımlanamaz mı, çatışmanın çeşitleri ve sınıflandırılması üzerine kısaca değinilmektedir. Ardından ilgili kuruluşlar, ilkeler ve faaliyetler dâhil olmak üzere, NATO'nun mevcut siber çatışmayla ilgili duruşunun kısa bir özetini sunmaktadır. Son olarak, NATO'nun siber çatışmanın ortaya çıkmasına tepki verme girişimlerinde karşılaştığı zorlukların sadece bir kısmını vurgulamaya çalışmaktadır.

Çatışma Nedir? (Siyasi, Ekonomik, Kültürel Açıdan Siber Çatışma)

İnternetin gelişiminin ilk zamanlarında siber saldırılar çoğunlukla nispeten küçük bilgisayar korsanlarına prestij kazandırmak amacıyla gerçekleştirilmiştir. Ancak son 20 yılda siber saldırılar hızla gelişmiştir. Suçlular giderek finansal kazanımlar elde etmek için siber saldırılardan yararlanmışlardır. Hacktivistler siyasi hedeflerini ilerletmek için dijital grevlere güvenmişlerdir. Devletler güvenlik politikalarını gerçekleştirmek için siber saldırıları kullanmaya başlamışlardır. Ama siber çatışmalar neden bu kadar çekici olmaktadır? Siber uzay, onu özellikle saldırganlar için çekici bir alan haline getiren benzersiz özellikler sunmaktadır. Bu tartışmanın üç yönü öne çıkmaktadır: ilişkilendirme sorunu, coğrafi mesafenin ilgisizliği ve nispeten düşük maliyetler. Temel internet protokolleri kurulduğunda, kullanıcı topluluğu çok kısıtlı olduğundan güvenlik endişe vermemiştir. İnternetin geliştirilmesinin amacı, ağın parçaları çalışmadığı zamanlarda bile varış noktasına bilgi verebilecek esnek bir iletişim ağı kurmak olmuştur. Dolayısıyla, bir mesajın göndericisini güvenilir bir şekilde doğrulamaya veya alınan yol verisini takip etmeye gerek yoktu. Bu nedenle, özellikle bir saldırının nereden geldiğini belirlemek teknik olarak zor olmaktadır. Ayrıca, bir saldırının belirli bir konumdan / ülkeden geldiğine dair makul bir kanıt olsa bile,

onu kimin yaptığını bilmenin neredeyse hiçbir yolu yoktur (bireysel bir hacker, suçlular veya bir devlet ajanı). Siber saldırıların teknik olarak nerden geldiği ve kimin/kimlerin yaptığı belirsiz olduğundan, çoğu zaman teknik olmayan akıl yürütme (örneğin saldırının gerçekleştiği ve kimin bundan yararlanacağı) ile desteklenmektedir (Conflict Barometer, 2017: 36-38).

Çatışma kavramsal açıdan genelde uzun süren bir anlaşmazlık veya tartışma olarak tanımlanmaktadır. İki ya da daha fazla aktör çatışıyorsa, ciddi bir anlaşmazlık ya da tartışma konusu olabilir. Bu tür çatışma süreçleri henüz anlaşmaya varılmazsa kanlı çatışmaya / savaşa dönüşebilmektedir. Siber çatışmalar için ortak bir tanım yoktur. Giderek yaygınlaşmasına rağmen farklı uluslar / kuruluşlar tarafından farklı şeyler anlamına geldiği anlaşılmaktadır. Bu durum göz önüne alındığında, ulusların / devletlerin ve farklı kurumların siber çatışma terimini nasıl yorumlayacağını ve siber çatışmalara nasıl yaklaştığını gösteren tek bir tanım bulunmamaktadır. Amerika ve Rusya'da ortak ifade edilen siber çatışma tanımı; karşılıksız siber saldırıların yeniden meydana geldiği ulus devletler ve / veya örgütlü gruplar arasında ve / veya aralarında gergin bir durum olarak tanımlanmaktadır (Godwin vd., 2014: 38). Rusya ve Amerika Birleşik Devletleri gibi iki ülke tarafından siber çatışmanın kritik terminoloji tanımları üzerinde anlaşmalar yapmak, Doğu-Batı köprüsü daha önce bulunmadığı bir atılımdır. Aynı zamanda, kültürel ve politik bakış açılarının eşitsizliği ile anlaşma sağlanabiliyorsa, o zaman tanımların farklı kültürler ve politik görüşlere sahip başka ülkeler tarafından kullanılabileceği de ileri sürülebilir (Godwin vd., 2014: 64). Nicholson'a göre çatışma, çarpışma rotası anlamına gelir; aynı zamanda mevcut görüşe, duruşa veya pozisyona muhalefet anlamına da gelir (Nicholson, 1992).

Aşırı ve dinsel bir perspektiften bakıldığında, çatışma insanın iki doğasından birini temsil eder: "kötülük". İşbirliği, tam tersi, insanın "iyi" doğası olan ikincisini temsil eder. Çatışma böylece anlaşmazlık, öfke, kavga, nefret, yıkım, ölüm veya savaşta kendini gösterir. Siyasi veya sosyal ortamı şekillendirme kapasitesine sahip, herhangi bir tavizsiz tavır çatışmasıyla sonuçlanacaktır. Açgözlülük, öz-merkezlilik, hoşnutsuzluk, kıskançlık, kibir, kabalık, dokunulmazlık, diğer eylemlerin yanı sıra, insan ilişkilerinin bir kopuşunu üretme yeteneğine sahiptir. Bir bakıma, bu ahlaksızlık, insanın "çatışma doğasının" doğuştan gelen nitelikleridir. Çatışma, çoğu zaman sona eren farklı ya da benzer siyasi grupların çapraz amaçlarının bir gösterisidir (Folarin, 2013:3).

Siber suçun doğası hakkında konuşamayız, ancak devletler ve bağlı kuruluşlar arasındaki uluslararası etkileşimlerin doğasıyla ilgili olarak, uluslararası rakipler arasındaki siber ihtilafın doğasına doğrudan beslenen bu olayları analiz etmek için bir tarih, kaynak ve yöntem vardır. Siber çatışma devletler veya bireyler tarafından devletlere karşı kullanılan bir dış politika aracıdır (Maness and Valeriano, 2015: 3). 2011'de ABD hükümeti, geleneksel askeri araçlarla cezalandırılabilen bir savaş eylemine benzer bir siber olayı ilan etmişti. Bu önemli bir adım oldu. Çünkü siber uzayda, kinetik bir formda fiziksel olmayan bir olaya karşı tepkiye izin vermektedir. Çatışma daha sonra siber uzaydan geleneksel formlara geçmiştir (Maness and Valeriano, 2015: 4). Siber operasyonlar, siber suçlar ve bir devletin diğerine karşı yönelttiği diğer siber faaliyetler, artık normal ilişkilerde çatışma ve çatışmanın bir parçası olarak kabul edilmektedir. Clarke ve Knake'nin (2012: 1) iddia ettiği gibi, "siber savaş, patlayıcılar, mermiler ve füzelerle daha geleneksel mücadelenin gerçekleşme olasılığını artırabilir." Clarke ve Knake, siber tartışmayı dönüşümsel olarak şekillendiğini belirterek; "böyle bir çatışma dünya askeri dengesini değiştirir. Böylece politik ve ekonomik ilişkileri temelde değiştirme potansiyeline sahip olabileceği güvenilir bir olasılık var olur", demiştir (Clarke and Knake, 2012: 32). Kello, siber alanın, politik bozukluk ve stratejik istikrarsızlık için mükemmel bir üreme alanı olduğunu belirtmiştir. Bir başka tanım ise siber çatışma terimini, bilgisayar aracılı ortamlarda siyasal çatışma olarak ifade etmiştir. İki biçim alır: etnik (dini hayatta olduğu gibi siber uzayda savaşan iki etnik veya dini grup) ve sosyopolitik (düşmanca kurumlara karşı toplumsal hareketler) (Karatzogianni, 2005: 7-8). "Gerçek" politik çatışmaları analiz etmek için, siyaset bilimcileri "Çatışma Kuramı" ve "Uluslararası Çatışma Analizi"ni geliştirmişlerdir. Çatışma teorisini kullanma sorunu, siber çatışmanın iki önemli parametresini tam olarak açıklayamamasından kaynaklanmaktadır: sosyopolitik boyutu (interneti düşman kurumlara karşı kullanan sosyal hareketler ya da muhalifler) ve çatışmanın bir ortamın (internet) içinde ya da internet aracılığıyla gerçekleşmesidir. Toplumsal hareketlerin siber kavgalara nasıl karıştığını, Bilgi ve İletişim Teknolojilerinin kullanımından nasıl etkilendiğini anlamak için, teorisyenlerinden halihazırda var olan teorik araçları kullanmaları mantıklı olacaktır (Karatzogianni, 2005: 196- 197).

İnternetin yapısı ağ grupları için idealdir (merkezi otoritesi olmayan küresel bir ağ olduğundan) ve yönetişim (yönetim yok), zaman ve mekân (kısaltma), ideoloji (bilgi ve

erişim özgürlüğü), kimlik (çokluk) ve temel olarak gözetim ve kontrol, sınırlar ve aygıtlara karşı bir muhalefet deneyimi sunmuştur. Bununla birlikte, grupların inanç ve örgüt sistemlerinin hiyerarşik aygıtlara (ulus, din, partiler ve liderlerle özdeşleşme) yöneldiği etno-dini siber kavgalarda, bu ağ formu her zaman açık değildir. Sosyo-Politik Siber Çatışma'da bilgi ve iletişim teknolojilerinin etkisi; a. Yapıları harekete geçirme (internet, katılım, işe alım, taktik, hedefleri kullanarak ağ hareket tarzı), b. Çerçeveleme Süreçleri (sorunlar, strateji, kimlik, internetin bu süreçler üzerindeki etkisi), c. Siyasi fırsat yapısı (internetin bu yapının bir bileşeni olarak), d. bilginin özgür dolaşımını sağlamak amacıyla hackerler tarafından gerçekleştirilen siyasal internet saldırılarıdır. Etno-dini siber çatışmalar: a. Etnik / dini bağlantı, şovenizm, ulusal kimlik, b. Dâhil etme ve dışlama söylemleri, c. Bilgi savaşı, internetin bir silah, propaganda ve mobilizasyon kaynağı olarak kullanılması d. Çatışma çözümü, yasal ve örgütsel çerçeveye, tarafların ve sorunların sayısına, iktidarın dağıtılmasına ve değer ve inançların içeriğine bağlıdır (Karatzogianni, 2005: 198- 201).

Son yirmi yıl içinde yapılan sayısız olay, kötü niyetli kodun, her türlü amaç için, her türden sayısal sistemi tahrip eden ve bozan bir araç olarak büyük bir potansiyele sahip olduğunu göstermiştir. Suçluların ve ülkelerin benzer şekilde, kötü amaçlı yazılım kampanyası için gerekli tüm araçları satın alabilecekleri çevrimiçi pazarlar vardır. Kötü amaçlı yazılımlara erişim artık her zamankinden daha kolay olduğundan, aktif savunma veya doğrudan suç için kötü amaçlı kod kullanımı, ulus devletler için büyük bir hayranlık uyandırmaktadır. Ancak, siber tartışma literatürü, kötü niyetli kodların ulus devletler tarafından dağıtımının sorunlu olduğunu belirtmektedir (Cycon, 2014: 72). Eskiden, devletlerarasında çeşitli biçimlerde karışıklıklar olsa da, örgütlü organlar öncü roldeyken, bireyler artık sınırlı bir boyutta bile, uzak ve güvenli konumlardan daha güçlü, daha büyük yapılara karşı çalışabilirler. Resmi veya gayri resmi gruplar, suç ya da siyasi etkinlik tarafından harekete geçirilen plan belirleme, hedeflerine ulaşma ya bazı finansal ya da politik kârlar elde etme konusunda iyi bir fırsat bulmak için siber boyutta hareket etmektedirler (Cycon, 2014: 142). Siber çatışmalar, gerçek hayat çatışmaları ile paralel (aynı amaçlar, aynı hedefler doğrultusunda) olarak hareket edebilir ve katılımcı grupların doğasını ve çatışmalarını açığa çıkarabilir (Karatzogianni, 2009: 3). Siber savaşın çizgileri bulanık olabilir. ABD eski Ulusal İstihbarat Başkanı Joel Brenner; "ABD'de bizler savaşı ya tam ölçekli bir savaş ya da barış içinde bir açma-kapama düğmesi olarak düşünmeye eğilimliyiz." demiştir. "Gerçek farklıdır. Artık nadiren savaş açacak uluslararasında sürekli bir çatışma durumundayız... Alışmak zorunda

olduğumuz şey, Çin gibi, hatta savaşta olmadığımız ülkelerin bile bizimle yoğun bir şekilde iletişim halinde olmalarıdır." Bu, siber savaşın, sürekli çatışmanın aslında doğrudan açık şiddet ile sonuçlanmadığı Soğuk Savaş gibi daha gayri resmi çatışma kavramlarıyla daha çok ortak noktası olabileceği yerler olabilir (Singer P. W. and Allan Friedman, 2014: 121). Uluslararası hukuk amaçları için "siber savaş", "siber düşmanlık" ve "siber çatışma" kavramları resmi olarak tanımlanmamıştır. Var olan tek antlaşma tanımı Şangay İşbirliği Örgütü'dür ve daha geniş bir "bilgi savaşı" kavramı ile ilgilidir. Bilgi sistemleri, süreçleri ve kaynaklarına zarar vermek; siyasi, ekonomik ve sosyal sistemleri zayıflatmak; kitlesel beyin yıkamayı, toplumu ve devleti yıkmak için bilgi alanında iki ya da daha fazla devlet arasında yüzleşme olarak ve de devleti, karşı tarafın çıkarları doğrultusunda karar almaya zorlamak gibi tanımlama mevcuttur (Melzer, 2012: 3).

Çatışma Çeşitleri

Çatışmayı, birçok alanda nasıl kullanıldığına bağlı olarak tanımlamanın farklı yolları vardır. Bu nedenle çatışma, farklı varlıkların karşıt fikirlerine ve eylemlerine aittir, dolayısıyla uzlaşmaz bir duruma yol açmaktadır. Çatışma hayatın kaçınılmaz bir parçasıdır. Her birimiz kendi görüşümüze, düşüncelere ve inanç gruplarına sahibiz. Bu nedenle, sıklıkla kendimizi farklı senaryolarda çatışıyor buluyoruz; Diğer bireyleri, insan gruplarını veya kendi içimizdeki mücadeleyi içerebilir. Dolayısıyla çatışma, eylem ve kararlarımızı bir şekilde etkilemektedir (Conflict Barometer, 2016: 6-8). Çatışma farklı nedenlerle ortaya çıkar ve insan toplumunda farklı çatışma çeşitleri vardır.

Kişilerarası çatışma, iki birey arasındaki çatışmayı ifade etmektedir. Bu, tipik olarak insanların birbirinden nasıl farklı olduğuyla ortaya çıkmaktadır. İnsanlar, uyumsuz seçimler ve görüşler ile sonuçlanan çeşitli kişiliklere sahipleridir. Görünüşe göre, kişisel gelişime yardımcı olabilecek veya başkalarıyla ilişkileri geliştirebilecek doğal bir durumdur. Ayrıca, bu tür çatışmaları yönetmek için ayarlamalar yapmak gerekmektedir. Ancak, kişilerarası çatışmanın çok yıkıcı hale gelmesi durumunda, bir arabulucuyu aramak, çözüme kavuşturmak için yardımcı olacaktır. *İçsel çatışma* bir bireyde gerçekleşir. Bu deneyim kişinin aklında gerçekleşir. Dolayısıyla, bireyin düşüncelerini, değerlerini, ilkelerini ve duygularını içeren psikolojik bir çatışma türüdür. İç mücadelelerinizi deşifre etmekte

zorlanırsanız, bu tür çatışmanın ele alınması oldukça zor olabilir. Huzursuzluğa ve tedirginliğe yol açmaktadır. Hatta depresyona bile neden olabilir. Depresyon geçiren kişi durumdan çıktığında, daha güçlü hale gelebilir. Böylece, deneyim kendi kişisel gelişiminde, bireye yardımcı olacak olumlu bir değişim ortaya çıkarmaktadır. *Grup içi çatışma*, bir takım bireyler arasında gerçekleşen bir çatışma türüdür. Bu bireyler arasındaki uyumsuzluklar ve yanlış anlaşılmalar gruplar arası bir çatışmaya yol açmaktadır. Kişilerarası anlaşmazlıklardan (örneğin, ekip üyelerinin gerilim yaratabilecek farklı kişilikleri vardır) ya da görüş ve fikirlerdeki farklılıklar ortaya çıkmaktadır (örneğin, bir sunumda, ekip üyeleri, bir başkan tarafından sunulan kavramların hatalı olduğu için görüş ayrılıkları). Bir takım içinde, çatışma olarak hedeflerine ulaşmalarına izin verecek olan kararların ortaya çıkmasında yardımcı olabilir. Ancak, çatışmanın derecesi üyeler arasındaki uyumu bozarsa, çözümlenebilmesi için farklı bir gruptan bazı ciddi rehberliğe ihtiyaç duyulacaktır (Folarin, 2013:5-7). Uyuşmazlık sorunları olacaktır. Çünkü çıkar farklılaşır ve çatışır, bu da anlaşmazlıklara veya çatışmalara yol açabilir. Bir grup içindeki farklı takımlar arasında bir yanlış anlaşılma ortaya çıktığında *gruplararası çatışma* yaşanır. Rekabet ayrıca gruplar arası çatışmanın ortaya çıkmasına da katkıda bulunmaktadır. Bir grup tarafından kendi kimliklerini oluşturan bir gruba karşı bir rekabet içerebilir. Ya da bir grup tarafından belirlenen sınırlara karşı bir rekabet içerebilir (Evans, 2013). Bilgi ve İletişim Teknolojilerinin artan önemi göz önüne alındığında, tarafların, siber uzayın belirli yönlerinden faydalanmak için çeşitli araçlar ve teknikler kullanarak rakiplerine karşı avantaj elde etmek isteyecekleri şaşırtıcı değildir. Mesela, hangi çatışma sorunlarının (bölgesel, ideolojik vb.) ya da çatışma şiddetlerinin (şiddet veya şiddet içermeyen) siber uzayda yankılanıp yankılanmadığını bilmiyoruz. Giderek artan siber olay sayısı göz önünde bulundurulduğunda, araştırmacıların, araştırmaları ve işbirlikleri yetersiz kalmaktadır (Conflict Barometer, 2017: 37). Çatışma bazıları için bir sorun gibi görünebilir. Ancak bu, çatışmanın nasıl algılanması gerektiği değildir. Öte yandan, büyüme için bir fırsattır ve gruplar veya bireyler arasında açılma için etkili bir araç olabilir. Bununla birlikte, çatışma üretkenliği geri çekmeye ve daha fazla anlaşmazlığa yol açmaya başladığında, bir çözüme ulaşmak için çatışma yönetimine ihtiyaç duyulacaktır (Conflict Barometer, 2015: 6).

Uluslararası İlişkilerde Siber Çatışmalar

Siber çatışma, ulus devletler için hızla değişen stratejik bir sorunu temsil etmekte ve onun etkilerini yönetmek için yeterli bir politika çerçevesinden yoksun kalmaktadır. Estonya,

Suudi Arabistan, İran ya da en son ABD başkanlık seçimleri gibi olaylar, siber saldırıların kritik hizmetleri tehlikeye atabileceğini, ekonomilere zarar verebileceğini, demokratik devletlerin temel sütunlarını zedeleyebileceğini ve resmi devlet çatışması düşüncesine ulaşabileceğini göstermiştir. Siber alan birden fazla ulusal, idari ve yargı sınırlarını aşar ve ticari kurumlardan bireylere, siber suçlulardan terörist gruplara kadar geniş bir yelpazede devlet dışı aktörleri bir araya getirmektedir. Devletler siber uzayda en güçlü ve aktif unsurlar olmaya devam etmektedir. Devletler uluslararası çatışma için yeni bir arena geliştirmişlerdir. Bu durum, ulus devletlerin siber suçluların kendi çıkarlarını daha da ileri götürmeleriyle açıklığa kavuşmaktadır. Siber alanın tekilliğini ve devletlerarası çatışmadaki rolünü anlamak için, onun yapısını değerlendirmek gerekir. Bunun nedeni, kaçınılmaz olarak siber saldırıların içine gömülmüş karmaşıklığın, mekânın kendisinin özelliklerinden kaynaklanmasıdır. Siber çatışmalar genellikle ticari işlemler için tasarlanan teknolojiler içinde gerçekleşir ve gelişir; bağımsız, anonim olarak ve dünya çapında bağlantıyı desteklemek için oluşturulmuşlardır. Bu alanın siber çatışmanın geliştiği bağlamda olması, çözüm üretmenin zorluğunu ya da sadece bu konuya standartlaştırılmış cevapları yansıtmaktadır.

Çatışmayı önlemek için bir dizi tanımlama girişimleri yapılmıştır. Çatışma önlemleri, politik bir itiraz bağlamında bir akıl yürütme aktörü tarafından gerçekleştirilen eylemler ve iletişimdir. Bunlar, belirlenmiş kurallara aykırı düzenlemelerin prosedürleri dışında ya da uluslararası düzeni veya devletin temel işlevini tehdit ederse, tanımlanabilir bir iddia için kurucu niteliktedir. Oluşturulan düzenleyici prosedürler, çatışma yönetimi aktörleri tarafından kabul edilen çatışma yönetimi mekanizmaları olarak tanımlanmaktadır. Örnekler arasında seçim ve muhakeme işlemleri bulunmaktadır. Düzenlenmiş tüzük prosedürleri, fiziksel şiddet kullanımı veya tehdidine başvurmadan gerçekleştirilmelidir. Devlet fonksiyonları, bir nüfusun güvenliğini, bir bölgenin bütünlüğünü ve belirli bir politik, sosyoekonomik veya kültürel düzenin güvenliğini sağlamayı içerir (Conflict Barometer, 2017: 6). Sınır ötesi siber olayların ve çatışmaların yönetimi, genellikle devlet kurumları ve özel olarak sahip olunan bilgi altyapısından sorumlu kuruluşlar arasında kapsamlı ve ayrıntılı bilgi paylaşımı gerektirmektedir. Siber olayların araştırılması ve yönetimi için verilerin sadece olayların seyri ve olayların arka planı hakkında detaylar değil, aynı zamanda hedefler üzerinde gerçek zamanlı raporlama ve sunucu günlüklerinin ayrıntılarından oluşmaktadır.

Bu, iyi trafiği kötülükten ayırt etmeyi mümkün kılmakta, düşman IP adreslerini engellemekte ve saldırıların kökenini izlemektedir (Tikk, 2010: 24).

İnternet altyapısının pratikte oldukça dayanıklı olduğu kanıtlanmıştır. İş dünyasında internetin bozulmasını ya da özel verilerin kaybolmasıyla yok olacak çok şey olduğu için, güvenlik çözümleri, hackerlar, sahtekarlar ve siber-sabotajcıların bir adım ötesine geçmektedir. Ancak bu, yalnızca büyük Bilişim Teknolojisi şirketlerinin (Microsoft, Cisco, Google, Yahoo v.d.) çoğu kez hükümetlerle yakın işbirliği içinde çalıştığı sürekli yenilik ve yatırımla elde edilir. Bununla birlikte, internetin bütünlüğüne yönelik gelecekteki tehdidin, düşman saldırıları gibi, giderek daha fazla sayıda ve daha geniş dosyaları dolaşarak, kapasite üzerindeki kısıtlamalardan gelmesi muhtemeldir (Wescott, 2008: 2).

Siber çatışmalar, teknik bilgi birikimine sahip siber savaşçılar tarafından bit ve bayt kullanan ağlar üzerinden de mücadele edilir. Siber çatışma, taktik düzeyde hızlıdır; Birler ve sıfırlar gerçekten ağ hızında seyahat ediyorlar. Siber çatışmalar düzensiz çatışmalar olma eğilimindedir. Bu tür bulanık ve belirsiz koşullarda siber çatışma kavramını tanımlamak, neredeyse her zaman bir sorun haline gelmektedir (Healey, 2016: 43-44). Mevcut belirsizlik, hükümetler arasında gerçek siber tehdit hakkında kafa karışıklığına yol açmaktadır. EastWest Enstitüsü tarafından "Siber Uzay için Cenevre ve Lahey Sözleşmelerinin Oluşturulması" başlıklı bir raporda, "İkili barışa karşı savaş paradigmasının İnternet Çağının karmaşıklıkları için çok basit olması mümkündür." Raporda, mevcut politika araçlarının nasıl kullanılacağı ve daha da önemlisi, uluslararası hukukun uygulanabilirliğinin açıklığa kavuşturulması için "üçüncü bir savaş dışı yöntem" geliştirilmesi önerilmektedir. Siber saldırıları kategorize etmek için iki basit kritere dayanan bir sistem önerilmektedir: etki ve niyet. Siber uzaydaki herhangi bir eylem, bu iki model aracılığıyla değerlendirilebilir. Kötü şöhrete sahip Stuxnet saldırıları gibi siber uzayda çeşitli yüksek profilli eylemleri değerlendirmek, savaş metaforunun bu olaylara uygulanamaz hale geldiği oldukça açıktır. Stuxnet'in niyeti politik bir unsura sahip olsa da (örneğin İran rejimini müzakere masasına dönmeye zorlamak), ölümcül bileşen eksiktir. Bu saldırılarda hayatlar kaybedilmiş olsa bile, temel amaç sabotaj, uluslararası alanda "kabul edilen" bir eylem ve kendi içinde çatışma, bir politik savaş biçimiydi (Gady, 2012). Birçok ülke için siber çatışmayla yüzleşmenin en önemli adımı, tercih edilen ulusal güvenlik sonuçları konusunda çok daha açık olmaktır. Bir hükümetin rekabet halindeki kamuoyu hedefleriyle karşı karşıya kaldığı durumlarda, kararları

netleştirmek için net bir ulusal siber stratejide bunlar öncelikli olmalıdır (Ünver, 2017: 110-111; Cycon, 2016: 45).

Uluslararası siber koruyucular ve olay ekipleri arasındaki etkileşimler çoğunlukla teknik, diplomatik ve politik ilişkilere dayanmaktadır. Özellikle kritik altyapılar, bilgisayar sistemlerinde meydana gelen olaylar ile ilgili ulusal güvenlik kaygısı alanıdır. Böyle bir olayın bir örneği, Ülke B hükümeti tarafından eylemleri protesto eden A Ülkesi bireylerinin "vatansever" çabaları olacaktır. Bu bireyler, B Ülkesinin hükümet veya kritik altyapı bilgisayar sistemlerine girebilir. Alternatif olarak protestocular, B ülkesinin hükümetini, finansal ve medya bilgisayar sistemlerini, o kadar fazla elektronik trafiğe maruz bırakacaklarını, sistemlerin kullanılamayacak kadar yavaşlatabilmeyi koordine edebilir. İlişkilerinin niteliğine bağlı olarak, A Ülkesi, B Ülkesine siyasi veya yasayı uygulama sağlama konusunda isteksiz olabilir. Ek bir karmaşık faktör, internetin yapısı ve doğası gereği, A Ülkesinden bir protestocunun kötü niyetli faaliyetinin, ani bir şekilde çatışmanın ötesinde telekomünikasyon sistemleri aracılığıyla gerçekleştirilebilmesidir (örneğin, sadece A ve B ülkelerinde değil, aynı zamanda X, Y ve Z ülkelerinde). Diğer ülkelerin B ülkesine yardım etmesini gerektiren ortak bir uluslararası yasa yoktur ve bu nedenle yardımda başarısızlığa dair hiçbir sorumluluk yoktur. Siber olaylar silahlı çatışma olarak tanımlanabilir ve belirli bir ülkeye atfedilebilirse, o zaman B Ülkesi uluslararası insancıl hukuk çerçevesinde eylemler başlatabilir. Özellikle NATO'nun hukuksal olarak almış olduğu kararlar bu noktada etkili olmaktadır. Ayrıca şu anda uluslararası anlamda oluşturulmaya çalışılan hukuk kuralları da bu anlamda önemlidir. Geleneksel çatışmaların siber bileşenleri içermesine rağmen, bugüne kadar hiçbir bağımsız siber olayın (fiziksel çatışmaya bağlı olmayan) silahlı çatışmalar olarak kabul edilmediği veya belirli ülkelerin desteğine yeterince atfedilmediği belirtilmelidir. Savaş paradigması dışında, uluslararası toplum, siber tehditleri veya ulusal güvenliği etkileyen olayları yönetmek için yaygın kabul görmüş bir çerçeveye sahip değildir. Dahası her bir ülke işbirliği sağlayabilsin diye, asgari siber olaylara müdahale yeteneğine sahip olan uluslararası bir anlaşma bulunmamaktadır. Çok uluslu siber olaylara müdahale çabalarını koordine eden tek bir örgüt yoktur (Dion, 2010: 71-73).

Çatışmanın Sınıflandırılmasında Hukuki Boyut

Modern savaşta "çatışmanın sınıflandırılması", yani belirli düşmanlıkların bir hukuk meselesi olduğu çatışma türünün tanımlanması olarak sorunlu olduğu şeklinde birkaç

uluslararası insancıl hukuk konusu görülmektedir. Söz konusu çatışmanın sınıflandırılması, her zaman uluslararası insancıl hukuk analizinde, çatışmanın niteliği geçerli yasal rejimi belirlediği için ilk adımdır (Schmitt, 2012: 245). Siber çatışma yeni olmayabilir, ancak eski de değildir. Diğer büyük, yıkıcı küresel eğilimlerde olduğu gibi, geleneksel uluslararası normların hala uygulandığı, ister geçerli olsun, isterse de değişiklikler olsun, ya da tamamen yeni normların icat edilmesinin gerekip gerekmediği konusunda sıkıntı veren sorular vardır. En önemli normlardan biri, devletlerin Lahey Sözleşmesi'nin güvence altına aldığı hak ve sorumluluklarla uluslararası yardıma cevap olarak tarafsız kalabilmeleri olmuştur. Siber gizliliğin doğası gereği, bu türden yasal norm, değiştirilmiş bir siyasi tarafsızlık normundan daha az yararlı olabilir. İnternet protokolleri siber saldırıları herhangi bir sayıdaki tarafsız ülke üzerinden yönlendirmektedirler. Siber anlaşmalar genellikle uluslararası hukuku tetikleyecek kadar yıkıcı değillerdir ve savaşanların kimliği veya uyruğu açık olmayabilir (Cycon, 2012: 22). Buna göre, uluslar, resmi bir anlaşma yükümlülüğü olup olmadığına bakılmaksızın, siber saldırıları durdurmak ve makul adımlar atmak için politik baskı altında olabilirler (Karatzogianni, 2009: 5-6).

"Uluslararası olmayan silahlı çatışma", bir devlet ile "örgütlü" silahlı grup arasındaki çatışmalar belirli bir yoğunluk seviyesine ulaştığında ortaya çıkar. Yoğunluk ayrıca şiddet seviyesinin ayaklanma veya sivil rahatsızlıklardan daha yüksek olmasını gerektirir (Cycon, 2017: 137-138). Yaralanma veya hasar tek başına yeterli değildir. Bireyler tarafından yürütülen siber operasyonlar, yetersiz bir şekilde örgütlenmedikleri için hak kazanamazlar. Çevrimiçi olarak organize edilen gruplar, duruma göre değerlendirilebilir, ancak geleneksel organizasyon kriterleri, onların hak kazanmalarını zorlaştırır. Buna göre sınıflandırma, önemli bir konudur. Örneğin, Eski Yugoslavya Uluslararası Ceza Mahkemesi (ICTY), ilk örneği olan Tadiç'te uluslararası olmayan çatışmanın uluslararasılaştırılmasına yönelik kriterler ile mücadele etmiştir. On yıldan kısa bir süre sonra, ulus ötesi terörizm sınıflandırma konuları dikkat çekmiştir. Bu uluslararası nitelikte terörizm olmuştur (Schmitt, 2012: 246). Sınırları aşmış ya da uluslararası olmadığından, bir devletin bir diğerine karşı düşmanlıklarla karşı karşıya gelen güçlerini içermediğinden mi (ya da hiç silahlı çatışma oldu mu)? Gürcistan 2008, Litvanya 2008, Radyosuz Avrupa / Radyo Özgürlük 2008 gibi siber olaylar, birbiriyle çelişen bakış açılarının, aynı ya da hatta benzer yasal sonuçları desteklemeyen farklı arka plan sistemlerinden ve deneyimlerinden ortaya çıkmaya eğilimli olduğu anlayışını pekiştirmiştir. Sonuç olarak, öykünün farklı yönlerini ve farklı türde siber faaliyetlerini

sistematik olarak kategorize etme yeteneğini göz önünde bulundurma yeteneği, yasal perspektiften çok büyük bir öneme sahiptir.

Gelecekte siber çatışma, sınıflandırmayı daha fazla karmaşıklaştıracaktır. Siber operasyonlar, tipik olarak silahlı çatışmalarla ilişkilendirilen fiziksel hasara neden olmadan, geniş toplumsal ve ekonomik zararı üretme potansiyeline sahiptir. Bunlar aynı zamanda doğal olarak sınır-ötesidir, dolayısıyla coğrafi faktörlere dayanan sınıflandırma yaklaşımlarını engellemektedirler. Dahası, kitlesel saldırılar tek bir kişi tarafından veya tamamen online olarak organize edilen bir grup tarafından başlatılabilir. Bu, bir devletin silahlı kuvvetlerinin veya tipik askeri operasyonları gerçekleştirebilecek bir grubun katılımına bağlı olan geleneksel çatışmaların tersi bir durumdur. Siber çatışmaların ortaya çıkışı, devam eden kinetik çatışmanın sınıflandırmasını hiçbir şekilde değiştirmemektedir. Paradigmatik örnek, Gürcistan ve Rusya arasındaki 2008 uluslararası silahlı çatışma sırasında "vatansever korsanların" yürüttüğü siber operasyonlardır (Schmitt, 2012: 250). Ülkelerin, ne hazırlığa ne de şansa sahip olamayacakları unutulmamalıdır. Zira ülkeler, siber olay yanıtları, yasaların uygulanması, gerekli olabilecek iç ve hükümetler arası koordinasyon için yeteneklerine göre değişmektedir (Dion, 2010: 71).

Bugüne kadar devletler, devam eden silahlı çatışma bağlamı dışında yürütülen herhangi bir siber operasyonu, uluslararası ya da uluslararası olmayan silahlı çatışma olarak nitelendirmekten kaçınmışlardır. Siber operasyonlar gelecekte, kaçınılmaz olarak devletler için zorlu çatışma sınıflandırma zorluklarını sunacaktır (Wingfield and Tikk, 2010: 22). Uluslararası silahlı çatışmayla ilgili olarak, devlet dışı aktörler tarafından gerçekleştirilen siber operasyonların atfedilmesi, geçmişte kinetik eylemlerin devletlere atfedilmesinden daha fazla sorun oluşturacaktır. Uluslararası olmayan silahlı çatışma bağlamında örgütlü bir silahlı grup olarak nitelendirme, sanal organizasyonun yapıları, araçları, yaygınlığı arttıkça ve geliştikçe, giderek karmaşıklaşacaktır. Devletlerin ve devlet dışı aktörlerin, siber altyapıya ve bağımlılık yaratan siber operasyonlara daha fazla bağımlı hale gelmesiyle, söz konusu devletin uygulamalarının mevcut eşiğin düşmesine neden olması beklenebilir. Siber silahlı çatışma yasası devam eden bir çalışmadır ve yakın gelecek için de öyle kalacaktır (Schmitt, 2012: 259-260).

Sonuç Yerine: Siber Çatışma Eğilimi

Siber çatışmayı etkileyen birçok sebep olabilir. Çoğu zaman bunları takip etmek zor olmaktadır. Siber çatışmanın izlenmesi siber alanın boyut, bant genişliği ve hacim bakımından artmasına paralel olarak günümüzde en büyük zorluklardan biri olmaya devam etmektedir. Buna ek olarak, siber aktörlerin eşiğin altında faaliyet göstermeye yönelik artan kararlılığı, yetkisi olmayan eylemlerin istenilen kesinlik ve gösterilebilirlik düzeyleriyle tanımlanmasını daha da zorlaştırmaktadır. Kalıcı ve yaygın izleme için bir olay olduğu kabul edilebilir. Bununla birlikte, ciddi sabotaj ve casusluk faaliyetlerinin tespiti, kısmen, mevcut tarih ve operasyonel kısıtlamaların biraz ötesinde, uzun bir zaman dilimi boyunca trafiğin akışına bağlıdır. Bu, siber alanın canlı ve modern ölçekte ele alınması, daha fazla araştırma için şüpheli faaliyetler algılaması ve tasarlanmış siber izleme altyapılarındaki araştırmalar için hayati önem taşımaktadır.

Pek çok araştırmacı, ağ izlerinden elde edilen bilgilere bağlı olarak tamamen internet altyapısının doğası gereği siber çatışma atfedilmesinde ve belirlenmesinde çok az şey yapılacağını iddia etmektedir. Bu nedenle, teknik çözüm verilerini bağlamsal analiz ve akıllı hizmetlerden elde edilen bilgilerle birleştiren yaklaşımlara ihtiyaç vardır. Siber çatışma atfedilmesi (özellikle yavaş faaliyetler) için etkili bir yöntemdir ve farklı koşullar altında etkinliğinin araştırılması sağlanmaktadır (Cycon, 2012: 407-408). Sadece siber alanda değil, suç ve hukuk bilimleri gibi diğer alanlarda da her tür aktör yetiştirmek için kullanılabilir. Mevcut bir yasal rejim veya çerçeve ile açıkça ilişkilendirilemeyen bir eylemden herhangi bir hukuki sonuca varmak siber çatışma için oldukça karmaşık olabilir. Bu nedenle pratik bir bakış açısı, ilgili yasal rejimin uygulanması açısından "neyin ne olduğunu" açık bir şekilde anlaşılması büyük önem taşımaktadır. Bilgisayar bilimleri ve bilişim teknolojileri, hukuk, stratejik, politik konular, sosyal ve ekonomik kaygılar ve insan davranışsal modellemelerini siber uzaya göre incelemektedir. Siber çatışmada çatışma aşamaları arasındaki etkileşimin dinamikleri, kinetik çatışmalarda bilinen aşamaları her zaman takip etmeyebilir. Tanım olarak, siber uzay, belirli bir atıfta başarısızlığa yol açan anonim saldırılara izin verir. Esasen, geleneksel yanıt yöntemleriyle çözülemeyecek kadar belirsizliği taşıyan eylemlerin olasılığını açmıştır. İlişkilendirme konusundaki belirsizlik, etkin devlet misillemesini felce uğratmış ve devlet çatışmasında ve uluslararası güvenlikte yeni bir paradigma ortaya çıkarmıştır. Bu belirsizlik, hem "saldırganlar" hem de "savunanlar" olarak adlandırılan güçlü siyasi etkilerin kaynağıdır. Çatışma ve orantılı tepki gibi birçok geleneksel çatışma kavramı,

siber savaşla başa çıkmak için yeniden uyarlanmalı ya da tamamen değiştirilmelidir. Saldırıların atfedilmesindeki yapısal belirsizlik, olası teminatların kapsamı ve devlet altyapısı ve kritik hizmetler üzerindeki olası etki, siber çatışmanın yönetilmesi ve yönlendirilmesi için özel ilkeler ve kurallara duyulan ihtiyacın yeni bir savaş türü olduğunu doğrulamaktadır. Siber çatışma hâlihazırda ele almaya hazır olmadığımız çok çeşitli olasılıklar sunmaktadır. Devletler arasındaki gelecekteki ilişkiler kuvvetli bir şekilde gelişmeli ve bu sayede siber çatışmaların varlığı azalmalıdır. Mevcut devlet uygulamaları, siber saldırıların ne ölçüde savaş eylemleri olarak tasarlanacağını ve hangi şiddetin diplomatik veya hatta askeri tepkiyi tetiklemeleri gerektiğini belirleyecektir. Bu nedenle, birbirine bağlı bir dünya gerçekliğinde, bu sınırlar yakında çatışma yönetiminde en hassas konulardan biri haline gelebilir. Siber çatışma artık sadece yükselen bir olay değil, yeni bir savaş alanı olmaktadır. Gelecekte siber çatışma devletlerin nasıl davrandığını, işbirliği yaptığını, yanıt verdiğini ve nihayetinde savaşı nasıl sürdürdüğünü yeniden tanımlayacaktır.

KAYNAKÇA

____ in Heidelberg, [https://hiik.de/conflict-barometer/bisherige-ausgaben/?lang=en].

____The EastWest Institute, [https://www.eastwest.ngo/issues/cyberspace].

Akyeşilmen Nezir ve Yılmaz Ensaroğlu, (2013). "Sonuç Yerine: Barış Sürecinde Yoldaki İşaretler", Nezir Akyeşilmen (ed.), *Barışı Konuşmak: Teori ve Pratikte Çatışma Yönetimi*, 1. Baskı, Ankara: ODTÜ Yayıncılık, ss. 444-460.

Akyeşilmen Nezir, (2015). "Çatışma Analizi: Hak-temelli Stratejik Barış Modeli", Ertan Efegil ve Esra Pakin Albayrakoğlu (ed.), *Türkiye'nin Yakın Havzasındaki Devlet İçi Çatışmaların Analizleri*, İstanbul: Gündoğan Yayınları, ss. 39-74.

Akyeşilmen Nezir (ed.), (2013). *Barışı Konuşmak: Teori ve Pratikte Çatışma Yönetimi*, 1. Baskı, Ankara: ODTÜ Yayıncılık.

Brangetto,P., M. Maybaum, J. Stinissen (Eds), (2014). *6th International Conference on Cyber Conflict*, Talinn: CCD COE Publications, http://www.ccdcoe.org/cycon/2014/proceedings/cyconBOOK2014.pdf.

Brose Robert, (2015). "Cyberwar, Netwar, and the Future of Cyberdefense", *7th International*

Conference on Cyber Conflict: Architectures in Cyberspace, M.Maybaum, A.-M.Osula, L.Lindström (Eds), Talinn: CCD COE.

Clarke,Richard and Robert Knake, (2012). *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco; Reprint edition.

Conflict Barometer. (2011). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 20, Germany: Printed in Heidelberg.

Conflict Barometer. (2012). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 21, Germany: Printed in Heidelberg.

Conflict Barometer. (2013). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 22, Germany: Printed in Heidelberg.

Conflict Barometer. (2014). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 23, Germany: Printed in Heidelberg.

Conflict Barometer. (2015). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 24, Germany: Printed in Heidelberg.

Conflict Barometer. (2016). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 25, Germany: Printed in Heidelberg.

Conflict Barometer. (2017). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 26, Germany: Printed in Heidelberg.

Czosseck, C., E. Tyugu and T. Wingfield (Eds.), (2011). *3rd International Conference on Cyber Conflict*, https://ccdcoe.org/sites/default/files/multimedia/pdf/2011_Proceedings_0.pdf.

Czosseck, C., R. Ottis and K. Ziolkowski (Eds.), (2012). 4th International Conference On Cyber Conflict, ,https://ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf.

Daban, Cihan, (2016). "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi", *Siber Politikalar Dergisi*, Cilt: 1, Sayı: 1, [http://cyberpolitikjournal.org/wp-content/uploads/2017/02/Journal_Dergi_pdf.pdf].

Denning Dorothy, (2001). "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", In Arquilla J., Ronfeldt D. (eds) *Networks and Netwars: The Future of Terror, Crime, and Militancy*, pp. 239-288.

Erendor M.E., "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", *Cyberpolitik Journal*, vol.1, no.1, pp.114-133, 2017.

Evans, Brad, (16.08.2013). Types of Conflict – Four Classifications, [http://www.typesofconflict.org/types-of-conflict].

Folarin, Sheriff F. (2013). Types and Causes of Conflict, Readings in Peace and Conflict Studies, [http://eprints.covenantuniversity.edu.ng/3241/1/Folarin%2025.pdf].

Gady, Franz-Stefan. (08.06.2012). *A Reality-Based Model for Cyber Conflict*, https://www.eastwest.ngo/idea/reality-based-model-cyber-conflict.

Geers Kenneth, (2011). Strategic Cyber Security, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn: CCD COE Publication.

Godwin, James, Andrey Kulpin, Karl F. Rauscher and Valery Yaschenko (Eds.), (2014). *Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2*, USA: The EastWest Institute, https://www.files.ethz.ch/isn/178418/terminology2.pdf.

Healey Jason and Karl Grindal, (2013). *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, Cyber Conflict Studies Association.

Healey Jason, (2016). "Winning and Losing in Cyberspace", *8th International Conference on*
Cyber Conflict: Defending the Core, N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.), Talinn: CCD COE.

Kalm Kaarel, (2013). "Illicit Network Structures in Cyberspace", 5th International Conference On Cyber Conflict, K. Podins, J. Stinissen and M. Maybaum(Eds), Talinn: NATO.

Karatzogianni, Athina (2005). *The Politics of Cyberconflict: Ethnoreligious Conflicts in Computer Mediated Environments*, PhD thesis, England: University of Nottingham, [http://eprints.nottingham.ac.uk/12112/1/423635.pdf].

Karatzogianni Athina, (2009). "Introduction: New Media and the Reconfiguration of Power in
Global Politics", *Cyber Conflict and Global Politics*, Athina Karatzogianni (Eds), NYC: Routledge.

Kosenkov Alexander, (2016). "Cyber Conflicts as a New Global Threat", https://pdfs.semanticscholar.org/a00e/3cba13b99b0acee9817002a925bba7ec646d.pdf.

Krishnamurti, J. (2002). *Çatışma Üzerine*, çev. Nurgül ve Deniz Demirdöven, 1. Baskı, İstanbul: Ayna Yayınevi.

Lawson Sean, (2012). "NATO & Cyber Conflict: Background & Challenges." Presented at The Shadow NATO Summit III. 14-15 May. George Washington University. Washington, D.C.

Lin, Herbert, (2013). "Cyber Conflict and National Security", Robert Art and Robert Jervis

(Eds.), *International Politics: Enduring Concepts and Contemporary Issues*, Eleventh Edition, USA: Pearson, pp. 476-489.

Maeve Dion , (2010). "Different Legal Constructs for State Responsibility", https://ccdcoe.org/cycon/sites/default/files/LegalProceedings2010.pdf.

Maness, Ryan C. and Brandon Valeriano, (2015). "The Impact of Cyber Conflict on International Interactions", SAGE: Armed Forces & Society, pp. 1-23.

Maybaum, M., A.-M.Osula and L.Lindström (Eds), (2015). *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Talinn: CCD COE, http://www.ccdcoe.org/cycon/2015/proceedings/CyCon_2015_book.pdf.

Melzer Nils, (2012). "Cyber operations and jus in bello", *Confronting Cyberconflict*, Vignard Kerstin (Eds), UNIDIR, http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf.

Nicholson, M. (1992). *Rationality and the Analysis of International Conflict*, England: Cambridge University Press.

Perkovich, George and Ariel E. Levite, (2017). *Understanding Cyber Conflict:14 Analogies*, Washington, DC: Georgetown University Press.

Pissanidis, N., H. Rõigas, M. Veenendaal (Eds.), (2016). *8th International Conference on Cyber Conflict: Defending the Core*, Talinn: CCD COE, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf.

Podins, K., J. Stinissen and M. Maybaum(Eds.), (2013). *5th International Conference On Cyber Conflict*, http://www.ccdcoe.org/cycon/2013/proceedings/cyconBOOK2013.pdf.

Rõigas, H., R. Jakschis, L. Lindström and T. Minárik (Eds), (2017). *9th International Conference on Cyber Conflict: Defending the Core*, Talinn: CCD COE, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2017_book.pdf.

Schmitt Michael, (2012). "Classification of Cyber Conflict", *Journal of Conflict & Security Law*, Vol. 17 No. 2, pp. 245–260.

Sharma Amit, (2009). *Cyber Wars: A Paradigm Shift from Means to Ends, Conference on Cyber Warfare 16-19 June*, https://ccdcoe.org/cycon/sites/default/files/VirtualBattlefield.pdf.

Singer P. W. and Allan Friedman, (2014). *Cyber Security And Cyber War What Everyone Needs To Know*, NYC: Oxford University Press.

Tekin Segah, (2013). "Çatışma Dili: Bir Söylem Analizi", Nezir Akyeşilmen (ed.), *Barışı*

Konuşmak: Teori ve Pratikte Çatışma Yönetimi, 1. Baskı, Ankara: ODTÜ Yayıncılık, ss. 87-107.

Tikk Eneken, (2010). "IP Addresses Subject to Personal Data Regulation" https://ccdcoe.org/cycon/sites/default/files/LegalProceedings2010.pdf.

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

Vignard, Kerstin, (2011). *Disarmament Forum: Confronting Cyberconflict*, Swirzerland: UNIDIR

Westcott, Nicholas, (July 2008). "Digital Diplomacy: The Impact of the Internet on International Relations", *Oxford Internet Institute*, Research Report 16.

Wingfield Thomas and Eneken Tikk, (2010). "Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen", https://ccdcoe.org/cycon/sites/default/files/LegalProceedings2010.pdf.

[https://www.project-syndicate.org/commentary/new-norms-to-prevent-cyber-conflict-by-joseph-s--nye-2017-08?barrier=accesspaylog].

[http://www.iapss.org/wp/2017/09/07/cyber-conflict/].

ISSN: 2587-1218

SİBER UZAYIN GÜVENLİKLEŞTİRİLMESİ: ABD ÖRNEĞİ

Upagül Rakhmanova[♣]

Özet

Bu çalışmada, ABD'nin siber uzayın güvenlikleştirilmesini nasıl hayata geçirdikleri araştırılacaktır. Bunun için öncelikle, Kopenhag Okulu tarafından geliştirilmiş güvenlikleştirme teorisi ve siber uzay kavramı irdelenecektir. Aynı zamanda, 1995'ten bu yana Amerikan hükümetinin siber alanı güvenlikleştirmek amacıyla kullandığı söz-edimlerinin etkili olup olmadığı da sorgulanacaktır. Ayrıca, siber uzayın güvenlikleştirilmesinde önemli rol oynayan kurumsal yapılanmaları analiz ederek, örgütlenmelerin yetki, sorumluluk, etkinlik ve faaliyetleri irdelenecektir. Son olarak, ABD'nin uluslararası düzeyde ülkenin siber uzay alanındaki amaç ve hedeflerini ortaya koyan 2003'ten bu yana yayınladıkları siber güvenlik strateji belgeleri üzerinde durulacaktır.

Anahtar kelimeler: Siber Uzay, Güvenlikleştirme, ABD, Kopenhag Okulu, Söz-edim

THE SECURITIZATION OF THE CYBER SPACE: THE CASE OF THE USA

Abstract

This paper explores how the American Government understands and characterizes cyberspace and its securitization. Adopting the framework of securitization theory, which was developed by Copenhagen School, paper seeks to understand and describe the role of speech-acts, that the American Government since 1995 engage in in order to securitize the cyber space. In this context, organizational structures, their responsibilities, activities that play an important role in securitization of the cyber space will be analized. Finally, it will focus on the cyber security strategy documents that the United States has published since 2003, which set out the goals and objectives of the cyber space.

Key words: Cyberspace, Securitizasion, USA, Copenhagen School, Speech-act

Giriş

♣ MA Student, Dept. of International relations, Selçuk University, upagul@gmail.com

Siber uzaya ve ayrıca siber güvenliğe olan ilgi her geçen gün artmaktadır. Ayrıca, her ülke kendi siber alanın korumaya ve güvenlikleştirmeye çabalamaktadır. Siber uzay kavramının herkes tarafından kabul edilen tanımı bulunmamasıyla beraber, siber uzay konusu günümüzde en çok güvenlik bağlamında ele alınmaktadır, zira hayatımızın hemen hemen her alanını etkilemektedir. Günümüzde artık, siber güvenlik sadece bireyler için değil, devletleri de ortadan kaldırabilecek kadar tehditleri oluşturabileceğinden, siber güvenlikle ilgili söylemler, "güvenlikleştirme teorisi" çerçevesinde incelenebilmektedir. Fakat, 1990'larda Kopenhag Okulu temsilcileri, siber güvenliği devletlerin varlığına bir tehdit olarak algılamıyordu, zira onlara göre siber güvenliğin o denemde diğer güvenlik sorunları üzerinde basamaklı (*cascading*) etkileri yoktu (Buzan, Waever, & De Wilde, 1998, s. 25). Ancak, 21.yüzyıla geldiğimizde, dünyada yaşayan insanların yarısından fazlasının internet kullanıcıları haline gelmesi, günümüzde bu durumu değiştirmiş bulunmaktadır.

"Güvenlikleştirme" kavramını akademik camiyaya Waever, 1995'te yazdığı *Securitization and Desecuritization* makalesi ile kazandırmıştır. "Güvenliği" bir *speach act* (söz-edim) olarak gören Waever'e göre, iktidar sahipleri bir konuya "güvenlik" olarak işaret etmekle, onu güvenlik sorunu haline getirmiş olurlar (Waever, 1995, s. 55). Güvenlikleştirme teorisi ise, daha sonra 1998'de Buzan, Waever ve Wilde tarafından kaleme alınarak, Uluslararası İlişkiler'de akademiyanın kullandığı terminolojisine kazandırılmıştır (McDonald, 2008, s. 566). Kopenhag Okulu, güvenlikleştirme teorisi ile, güvenlik çalışmaları'ndaki genişleyen tartışmanın orta noktasını yakalamada başarılı olmuştur (Hansen & Nessenbaum, 2009, s. 1158). Michael Williams, Kopenhag okulunun da defalarca dile getirdikleri gibi, güvenlik söyleminde, bir konu dramatize edilir ve yüksek öncelikli bir konu olarak sunulur demiştir (Williams, 2003, s. 514) Buna örnek olarak, Temmuz 2012'de ABD eski Başkanı Barack Obama, The Wall Street Journal'da yayınlanan bir fikir (*opinion*) yazısını verebiliriz. Bu yazıda, ülkeye karşı yapılan siber saldırıları, karşılaştıkları en ciddi ekonomik ve ulusal güvenlik sorunlarından biri olarak tanımlamıştır.

Bu çalışma ABD'nin siber uzayı nasıl güvenlikleştirdiğini ve ülke liderlerinin siber tehditlere karşı, dinleyicileri inandırmak amacıyla kullandıkları ifadelerin başarılı olup olmadığını irdelemeyi amaçlamaktadır. ABD'nin siber uzayı güvenlikleştirmesini inceleyen bu çalışmanın giriş bölümünün ardından gelen bölümde güvenlikleştirme teorisinden söz

edilecektir. Çalışmanın bir sonraki bölümünde ise Siber uzayın ne olduğu ve faklı tanımları ele alınacaktır. Makalenin son bölümünde ise ABD'nin siber uzayı güvenlikleştirmeyi nasıl yerine getirmeye çalıştığından bahsedilecektir.

Çalışmamız "güvenlikleştirme" ve "siber uzay" konularına odaklanmış olup, ABD'nin siber uzayı nasıl güvenlikleştirmeye çalıştıklarını ele almaktadır. Temel olarak siber uzay ve güvenlikleştirme teorisi üzerine yazılmış önemli eserleri ele aldığımız bu çalışmada, konunun toplumsal, siyasal ve bilimsel boyutlarıyla incelemeye ve konuya bir bütün olarak bakılmaya çalışılmıştır. Gerekli veriler ise, tarama tekniği ile toplanmıştır. Başvurulan referans kaynaklar, temel olarak siber güvenlik, siber tehdit, güvenlikleştirme, Kopenhag Okulu hakkında yazılan kitaplar ve makalelerden oluşmakla birlikte, özellikle güncel veriler ve ABD başkanlarının söylemleri için genel ağ ortamından yararlanılmıştır.

2. Güvenlikleştirme Teorisi

Güvenlikleştirme kavramı ilk olarak 1995 yılında Ole Waever tarafından *Securitization and Desecuritization* (Waever, 1995) makalesinde kullanılmıştır. Waever makalesinde "güvenliği" bir *speach act* (söz-edim) olarak görmüştür. Ayrıca söz-edimleri sadece iktidar sahipleri ürettiklerini öne sürmüştür. Ona göre, iktidar sahipleri belirli bir konuyu "güvenlik" problemi olarak isimlendirirken, devlet veya iktidarı elinde bulunduran elitler, bu "güvenlik" problemine karşı başvuracakları eylemleri otomatik olarak meşrulaştırmış olur. Bir konuya "güvenlik" olarak işaret etmekle, onu güvenlik sorunu haline getirmiş olurlar. Keza iktidar sahiplerinin "güvenlikleştirme" aracını, kontrolü elinde tutabilmek için kullanabileceklerini de yazmıştır. (Waever, 1995, s. 54). Kopenhag okulu temsilciler ise güvenlikleştirme kavramını daha ileri düzeye taşıyarak, daha doğrusu 1998'de yayımlanan *Security: a new framework for analysis* adlı kitabında onu bir teori haline getirmekle birlikte akademik yazıma kazandırmış bulunmaktalar. Güvenlikleştirme teorisi inşacı bir temele sahip olmaktadır, zira bu teoriye göre, güvenlik konuları güvenlik tehdidi olarak inşa edilmektedirler. Bu inşa edilmiş güvenlik konusu ise, söz-edimler ile tekrarlanarak, insanların diğer bir deyiş ile "hedef kitlenin" aklına enjekte edilir ki, bunun sayesinde tehdit olarak kabul ettikleri konulara karşı olağan üstü tedbirleri alabilmek meşru hale gelmiş olur. Bu, kimilerinin elinde bir araç haline gelebilmekteyken, kimileri için gerçekten bir tehdidin olduğuna insanları inandırmanın yararlı bir yolu olmaktadır. "Güvenlikleştire" – bu

öznelerarası ve sosyal olarak inşa edilir. Yani herhangi bir tehdit olarak gördüğü veya tehdit olarak sunmak istediği konuyu söz-edimler yoluyla güvenlik sorunu olarak hedef kitleye sunar. Bunun sonucunda kendi meşru olmayan eylemlerini hedef kitlenin kabul etmesini veya en azından alınacak tedbirlere tolere etmelerini sağlamış olurlar (Buzan, Waever, & Wilde, 1998, s. 31).

Waever'in 1995 makalesinde, "güvenlikleştirmek" sadece belli bir sorunu dile getirmekten ibaretti. Yani Waever 1995'te "güvenliği" dil teorisinin yardımıyla söz-edim olarak tanımlamıştır (Waever, 1995, s. 55). Daha doğrusu devlet temsilcisi, "güvenlik" kavramını dile getirerek belli bir gelişmeyi özel bir alana sokar ve bu gelişmeyi engellemek, bloke etmek için gerekli tüm araçları kullanma hakkını talep etmiş olur. (Waever, 1995, s. 55) Ancak, Kopenhag okulu ise, güvenlikleştirmenin sadece bir sorunu dile getirmekten ibaret olmadığını, söz-edimin güvenlikleştirme eyleminin sadece bir parçası olduğunu yazmışlardır. Onlara göre, "güvenlik", politikayı oyunun yerleşik kurallarının ötesine götüren ve meseleyi ya özel bir politika türü ya da siyaset olarak ele alan bir "hamledir". Güvenlikleştirme, bu yüzden siyasallaşmanın daha aşırı bir versiyonu olarak açıklanmıştır. (Buzan, Waever, & Wilde, 1998, s. 23).

1995 yılında vurgu *söz-edimde* ya da güvenlikleştiricide iken, 1998'de artık vurgu "güvenlikleştirici hamleye" taşınmıştır. Bu cümleyi açıklarsak, olağanüstü tedbirler ya da araçlar gerektiren bir tehdidin belirlenmesi ve bu durumun hedef kitle tarafından kabul edilmesi, güvenlik söyleminin dile getirilmesinden daha da önemlidir. (Williams, 2003, s. 526) Ayrıca, güvenlikleştirme eylemi üç temel öğeden oluşmaktadır. Bunlar - güvenlikleştirilmesi gereken konu, yani referans nesnesi; ikincisi, güvenlikleştiren aktör, başka deyiş ile hedef kitleye sürekli tekrarlayarak güvenlik konusunu enjekte eden kişi/grup; üçüncü öğe de işlevsel aktörlerdir, yani güvenlik alanındaki kararları önemli derecede etkileyen aktörler. (Balzacq, 2005, s. 178) Güvenlikleştirme eyleminin analizini yapmak mümkündür, bu ise korunması gereken konunun büyüklüğü ve seviyesi ile belirlenebilmektedir. Güvenlikleştirme teorisine göre, güvenlikleştirme analizinde üç ayrı düzey öngörülmüştür. Bunlar mikro, makro ve orta düzeylerdir. Kopenhag Okulu yazarları, söz-edimin örgütsel mantığına odaklanmanın kimin güvenlikleştirici aktör olduğunu belirlemede en iyi yol olduğuna inanmışlardır (Buzan, Waever, & Wilde, 1998, s. 40).

Kopenhag Okulu için, sorunlar dil aracılığıyla güvenlik sorunları (veya daha doğru bir şekilde tehditler) haline gelir. Dil, belirli aktörleri veya meseleleri belirli bir politik topluluğa tehdit eden konuma koyar ve dolayısıyla güvenlikleştirmeyi meşru yapar (McDonald, 2008, s. 568). Güvenlikleştirmenin ayırt edici özelliği, onun bir retorik yapıya sahip olasıdır. Yani, 'hayatta kalma' (*survival*) eyleminin önceliği, 'konuya anında, şimdi müdahale edilmezse, başarısızlığı düzeltmek için çok geç olacak' (Buzan, 1997, s. 14).

Yukarıda da bahsettiğiimiz gibi, güvenlikleştirme kendisi bir eylemdir, bir süreçtir (O'Reilly, 2008, s. 67). Bir konuyu alıp güvenlik tehdidi olarak gösterdikten sonra, geri kalan bütün diğer konular ikincil plana gitmiş olur. Güvenlikleştirilmesi gereken konu, öncelik kazanır ve tehdidin ortadan kalkmasına kadar diğer konuların önemi olmayacak gibi bir algı oluşur. Bu da, karar alan aktörlere her türlü tedbiri alarak, sorunu çözüme ulaştırma özgürlüğü verir. (Buzan, Waever, & Wilde, 1998, p. 24) Güvenlikleştirme eylemini gerçekleştiren aktör ise, bu durumun farkında ve olağanüstü tedbirler kullanmak istediği konuları güvenlik sorunu olarak etiketler. (O'Reilly, 2008, s. 66). Kopenhag okulu güvenlikleştirmeyi bir spektrum yardımıyla açıklamaktadır. Buna göre, her konu, "politize edilmemiş", "politize edilmiş" ve "güvenlikleştirilmiş" şeklinde sınıflandırılabilir. Mevcut şartlar altında her konu bu spektrumdaki yerini almaktadır. (Buzan, Waever, & Wilde, 1998, s. 24).

Bu teoriye göre, bir konuyu güvenlikleştirmek bu, söylemler üreterek hedef kitle üzerinde çalışmaktır. Bu manada güvenlikleştirme çalışmak, bir argümanın nasıl ve ne zaman hedef kitle üzerinde yeterli etkiyi yaparak onların normal şartlar altında kabul etmeyecekleri olağanüstü tedbirlerin alınmasını kabul etmelerini sağladığını araştırmak olmaktadır. Buna göre "güvenlikleştirme çalışmaları", kimin, hangi konuları, kimin için, neden, hangi sonuçlarla ve hangi şartlar altında güvenlikleştirdiğinin net olarak anlaşılmasını hedefler. Kısacası, güvenlikleştirme çalışırken araştırmacının görevi, bir konunun gerçek bir güvenlik sorunu olup olmadığının ortaya çıkarılması değil, güvenlikleştime eyleminin nasıl ve ne zaman gerçekleştiğinin, bunun öğelerinin (güvenlikleştirici, referans nesnesi, hedef kitle) neler ya da kimler olduğunun ve bunun sonuçlarının neler olduğunun ortaya konulmasıdır. (Buzan, Waever, & Wilde, 1998, s. 32) Fakat, başarılı bir güvenlikleştirme 3 aşamadan, veya daha doğrusu üç bileşenden oluşmaktadır. Bunlar, tehditin kendisi, acil tedbir ve olağan kuralların yıkılmasının ilişkilere tesir etmesidir. Bir de, bir konunun tehdit oluşturduğunu

ortaya koyan bir söz-edim kendi başına güvenlikleştirme oluşturmaz. Bu sadece bir hamledir, yani güvenlikleştirici hamledir.

Başarılı bir güvenlikleştirme, neyin dikkate alınması gerektiği ve kolektif olarak, yani bütün hedef kitlenin bir tehdit olarak karşılık verileceği konusunda ortak bir anlayışa varmalarıdır. (Buzan, Waever, & Wilde, 1998, s. 26).

Kopenhag Okulu, daha önceden geliştirmiş oldukları bölgesel güvenlik gibi diğer güvenlik yaklaşımlarını da güvenlikleştirme teorisinden sonra güncellemişlerdir. Güvenlikleştirme teorisini eleştirenler de vardır, onlara göre bu teori çok dar ve sınırlıdır. Zira güvenliği oluşturma eyleminin kendisi sınırlı tanımlanmıştır. Sadece baskın, iktidar sahibi aktörlerin konuşmalarına dayanmaktadır. Başka insanları devre dışı bırkamaktadır (McDonald, 2008, s. 564) ki, günümüzde sadece iktidar sahipleri değil, internet aracılığıyla sıradan bir insan da toplum içinde, hatta ülkeleri ve bölgelere kadar yankı yaratacak konuşmaları yaparak, etki yaratabilmektedir.

Sonuç olarak söylenmesi gereken nokta, bir konunun güvenlikleştirilip güvenlikleştirilmeyeceğini güvenlikleştirici aktör belirler. Onun verdiği bu karar her zaman politik karardır. (Buzan, Waever, & Wilde, 1998, s. 29) Bir konuyu güvenlikleştirmek, en kısa şekilde aşağıdaki gibi açıklanabilir. Ortada bir sorun var, onu güvenlik sorunu olarak etiketlemek, tekrar tekrar aynı konulardan bahsetmek, hedef kitleyi ikna etmek, onları inandırmak ve ortak düşünceyi inşa etmektir. Bunun sonucunda da yapılacak eylemleri otomatik olarak meşrulaştırmaktır.

3. Siber Uzay

Siber teriminin tarihsel ve felsefi kökleri genellikle Platon'un "Devlet" adlı yapıtındaki mağara alegorisine kadar uzanır. Ancak modern çağı ele alırsak, sibernetik teriminden türetilmiştir. Norbert Weiner tarafından 1948'deki ünlü *Cybernetics: Or Control and Communication in the Animal and the Machine* adlı yapıtında kullanmıştır (Choucri, 2012, s. 7). "Siber uzay" kavramını ise ilk kez bilim-kurgu yazarı William Gibson tarafından, 1984'te bir bilgisayar korsanının Matrix adı verilen bir bilgisayar sistemine sızarken yaşadıklarını anlatan *Neuromancer* adlı romanında kullanılmıştır (Singer W. & Friedman, 2014, s. 12). Enformasyon çağında herhang bir kelimenin önüne siber, bilgisayar veya

enformasyon gibi sözcükleri yerleştirmekle, yeni kavramları üretmek yaygınlaşmıştır (Cavelty, 2008, s. 21). Günümüzde siber uzay kavramının herkes tarafından kabul edilmiş tek bir tanımı yoktur. Ayrıca Gibson'un kullandığı maanadan farklı bir zemine kaymış bulunmaktadır. Bu yüzden çalışmamızda bir kaç tanımı verilecektir. Kimilerine göre siber uzay, ekranımızın ardındaki dünyayı işaret eden bir kavramdır. (Klimburg & Mirtl, 2012, p. 4) Ulusal sınırların geçerli olmadığı, devletler tarafından kontrol altına alınamamış ve askerler aracılığıyla koruma altına almanın imkansız olduğu alan ve bazen de İnternet'e karşılık olarak da kullanılan kavramdır. Bazıları siber uzayı harika ve "olmayan yer" (*no place*) olarak tanımlamaktalar. Bu ise dijital alemin fiziksel alanı aştığı anlamına gelir. Bilgi ve onu manipüle eden varlıklar elektronlar gibi - her yerde ve hiçbir yerdedir (L.Herrera, 2016, s. 67).

ABD Savunma Bakanlığı, siber uzayın vaftiz babası olarak kabul edilebilir zira bu, ARPANET gibi ağların ve eski bilgisayarların finansmanına dayanır. Yine de Pentagon bile bebeği büyüdükçe ayak uydurmak için çabaladı. Yıllar içinde siber uzayın ondan fazla farklı farklı tanımını yayınlamıştır. Bunların arasında "Soyut bilginin bilgisayar ağları üzerinden iletildiği kavramsal ortam" tanımı vardı, ama daha sonra bu tanım reddedildi, çünkü siber uzayın sadece iletişim ve büyük ölçüde hayali olduğu iddia edtmekteydi. Bir diğer tanım ise "elektronik ve elektromanyetik spektrumun kullanılmasıyla karakterize edilen bir alan" olarak tanımlanmıştır, fakat bu da bilgisayar ve füzelerin güneşten gelen ışığa kadar her şeyi kapsadığı için reddedilmiştir (Singer W. & Friedman, 2014, s. 13).

Günümüzde hayatımızı etkileyen faliyetlerin büyük kısmı siber uzayda/ortamda gerçekleşmektedir. Siber uzay, insan tarafından ve insanın hayatını kolaylaştırabilmek için yapılmış olsa da, kimileri bu alanı kötü niyet için kullanabilmektedir. Siber uzay, bireyleri daha önce mümkün olmayan şekillerde güçlendirmekte ve etkinleştirmektedir ve insan faliyetleri için oluşturulmuş yeni bir alandır. Siber uzaya ilişkin tanımların biri de 2003 tarihinde yayınlanan Amerika'nın Ulusal Siber Savunma Strateji belgesidir. Belgede siber uzay, ülkenin kritik altyapılarını etkileyen sinir sistemi olarak tanımlanmış olmakla birlikte, ülkenin ekonomisi ve ulusal güvenliği için sağlıklı çalışan bir siber uzaya dikkat çekilmiştir (The White House, 2003, p. 1).

Bir diğer tanıma göre, siber uzay herşeyden önce bir bilgi ortamıdır. Dijital ortamda oluşturulan, depolananan ve paylaşılan verilerden oluşmaktadır. Ama siber uzay tamamen sanal ortamdan ibaret değildir, zira veri depolayan bilgisayarları ve bilgi akışını sağlayan sistemleri ve altyapıyı içerir. Bu, ağa bağlı bilgisayarların internetini, kapalı intranetleri, hücresel teknolojileri, fiber optik kabloları da kapsar (Singer W. & Friedman, 2014, s. 14). Başka bir tanımda ise, siber uzay, devlet aktörleri tarafından sadece kısmen kontrol edilen veya kontrol edilebilen alandır. Bu alandaki güç, özel sektör aktörlerinin, özellikle de iş sektörünün elindedir. Daha iyi koruma önlemleri almak için gereken uzmanlık ve kaynakların çoğu hükümetlerin dışında yer almaktadır. Askeri ya da bu konuyla ilgili herhangi bir devlet kurumu, kritik (bilgi) altyapılara sahip değildir ve bunlara doğrudan erişimi yoktur. Onları askeri bir görev olarak korumak imkansızdır ve siber uzayı bir işgal bölgesi olarak görmek bir yanılsamadır. Militanlar ülkelerinin siber uzayını savunamazlar - ulusal sınırların mantığı uygulanmadığı için askerlerin ve tankların konumlandırılabileceği yer yoktur. (Cavelty, 2012, s. 151).

ABD'li siyaset bilimci Joseph Samuel Nye, "Nuclear Lessons for Cyber Security?" başlıklı makalesinde nükleer alan ve siber uzay arasında tüm benzerlikleri ve farklılıkları saymıştır. Nye, nükleer çağın başında bu güce sahip devletlerin kabul etmediği işbirliğini daha sonra kabul etmesine benzer bir sürecin siber uzayda da gerçekleşeceğini savunmaktadır. Siber uzayın sanal katmanında sınırların olmayışı ve bu durumdan kaynaklı egemenlik alanlarının belirsizliği, devlet dışı aktörlerin güç kazanmasına neden olmuştur (Nye, 2011, s. 37). Bu durumu güç yayılımı (diffusion of power) olarak kavramsallaştıran Nye, devletlerin kara, deniz ve hava boyutlarında olduğu gibi siber uzayda da bir güç olarak var olmalarına karşın, siber uzayın doğasının devletlerin tek aktör olarak bu alanda hâkim olmalarına izin vermeyeceğini belirtmiştir (Nye, 2011, s. 20). Bu bağlamda siber uzayda güç, büyük devletlerden diğer devletlere ve daha da önemlisi devlet dışı aktörlere yayılmaktadır (Nye, 2011). Bir bilgi ortamındaki güvenliğin kanonik hedefleri, bu tehdit kavramından kaynaklanmaktadır. Geleneksel olarak, üç hedef vardır: Gizlilik, Bütünlük, Erişebilirlik, bazen "CIA üçlüsü" olarak adlandırılmaktadır. Gizlilik, verileri gizli tutmak anlamına gelir. Gizlilik sadece bazı sosyal ya da politik amaç değildir. Dijital dünyada, bilginin değeri vardır. Bu bilgiyi korumak bu nedenle çok önemlidir (Singer W. & Friedman, 2014, s. 35).

Siber uzay konusu günümüzde en çok güvenlik bağlamında ele alınmaktadır, zira hayatımızın hemen hemen her alanını etkilemektedir. Hayatımızı her yönden kapsayan bu alanının güvensizliği ise herkesi, ister devletler olsun, ister Uluslararası Ögrüt veya şirket olsun, tedirgin etmektedir. Siber uzayı tanımlamanın zor olması, onun her an büyümekte olması veya küresel bir nitelik taşımasıyla sınırlı değildir. Bunun nedeni, günümüzdeki siber uzayın, ilk başta mütevazi bir şekilde ortaya çıkmasından çok farklı olarak tanınmaz hale gelmesindendir.

4. ABD'nin Siber Uzayı Güvenlikleştirmesi

Siber uzay alanında devlet tarafından güvenlikleştirme çabaları 1995 Clinton yönetimi sırasında başlamıştır. İlk etapta ABD siber uzayı ekonomik ve kültürel üstünlüğünü kabul ettirebileceği bir alan olarak değerlendirmiştir (Darıcılı, 2017, s. 350). Ciddi güvenlik mekanizmaları ise 11 Eylül 2001'den sonra başlamıştır. 2001'in sonlarında, FBI Başkanının ofisinde bir bilgisayar yoktu, hatta ABD Savunma Bakanı ona gelen maillerin çıktısını almak için asistanın yardımından yararlandığı, gelen maile cevabı da kalemle kağıda yazıp asistana verdikten sonra, asistanı ardından onları bilgisayarda tekrardan yazdığı bilinmektedir. Bundan on yıl sonra ülkeyi siber tehditten korumakla görevli olan İç Güvenlik Bakanı Sekreteri'nin 2012'de düzenlediği bir konferansta, "Gülmeyin, ama ben e-posta hiç kullanmıyorum" demesi, onun için güvenlik korkusu değildi. Onun için bu, sadece e-postaların faydalı olduğuna inanmamasıydı. 2013 yılında, Yargıç Elena Kagan, ABD Yüksek Mahkemesi yargıçlarının dokuzunun sekizini de aynı şekilde e-posta kullanmadıklarını açıklamıştı. Ama nihateninde bu insanlar, siber alanda neyin yasal olduğuna karar verecek olan insanlardır. (Singer W. & Friedman, 2014, s. 5).

Ocak 2009'da göreve başlanan Başkan Barak Obama, ABD siber güvenlik politikasının gözden geçirilmesini emretmişti. Obama'nın başkanlık döneminde konuşmalarında ABD'nin siber saldırılardan dolayı ciddi önlemler almaları gerektiğini sıkça dile getirerek yeni politikalar üretmiştir. Mayıs 2009'da Başkan Obama, politika incelemesini kabul etti ve ABD hükümet departmanlarının ve kurumlarının Beyaz Saray Siber Güvenlik Koordinatörü (WHCC- *The White House Cyber security Coordinator*) aracılığıyla siber güvenlik çabalarını koordine etmeye başladığını söylemiştir. WHCC, tüm ABD hükümet departmanlarının ve

ajanslarının, siber güvenlik stratejileri ve ABD siber güvenlik stratejisi ile uyumlu protokolleri uygulamaya koymalarını sağlamakla görevli olmuştur (Kiggins, 2014, s. 164).

Thierry Balzacq, bir konuşma eyleminin istenen etkiyi elde etmesi için, güvenlikleştirici aktörün "kendi dilini izleyicinin deneyimine göre ayarlaması" gerektiğini belirtmiştir (Balzacq, 2010, s. 9). 2009'da Obama'nın göreve başlamasından hemen sonra siber uzay alanında güvenlikleştirme işlemlerinin çok büyük tempolarla ilerlediğini görmek, hedef kitleyi inandırmış veya en azından susturmuş, kabullendirmiş anlamına gelmektedir. ABD Ordusuna bağlı Siber Komutanlığın (*Cyber Command*) generali, 2010'da Kongre'ye verdiği konuşmasında, Amerika silahlı kuvvetleri milyonlarca siber saldırıyla karşı karşıya olduğunu söylemiştir (Singer W. & Friedman, 2014, s. 68). Siber güvenlik konusunun Kongre'ye taşınması, artık önemli adımların alınacağı anlamına gelmekteydi. Obama'nın talimatıyla 2009 yılında hazırlanmış önemli bir belge Siber Uzay Politika Revizyonu *(Cyber Space policy review)* belgesidir. Bu belgede temel olarak, ABD siber savunma sisteminde görev alan resmi kurum ve kuruluşların, federal ve yerel düzeyde çok başlı yapısına eleştiride bulunularak, bu durumun giderilmesi için bazı tedbirlerin alınması gerektiği ve ulusal siber güvenlik sistematiğinin ancak bu kuruluşların birlikte ve eşgüdüm halinde hareket etmesi ile etkili olabileceği belirtilmektedir (The White House, 2009). Bundan sonraki önemli adım, yine Obama'nın talimatıyla hazırlanan Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık (*International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World Siber Uzay İçin Uluslararası Strateji)* isimli dökümanın olmuştur (The White House, 2011).

Michael Williams, Kopenhag okulunun da defalarca dile getirdikleri gibi, güvenlik söyleminde, bir konu dramatize edilir ve yüksek öncelikli bir konu olarak sunulur demiştir (Williams, 2003, s. 514) Buna örnek olarak, Temmuz 2012'de ABD eski Başkanı Barack Obama, The Wall Street Journal'da yayınlanan bir fikir (*opinion*) yazısını verebiliriz. Bu yazıda, ülkeye karşı yapılan siber saldırıları, karşılaştıkları en ciddi ekonomik ve ulusal güvenlik sorunlarından biri olarak tanımlamıştır. Modern Amerikan halkının çoğunun yaşamının bağımlı olduğu ağlara siber tehditlerin olduğunu, hemen harekete geçme ve düşmanlarından bir adım önünde olma fırsatı ve sorumluluğu olduğunu vurgulayan Obama, ulusal ve ekonomik güvenliklerinin uğruna, Senato'nun 2012'deki Siber Güvenlik Yasasını

geçirmesini rica ederek, büyüyen tehlikeye karşı savunmalarını güçlendirmelerinin zamanı geldiğini söylemiştir (Obama, 2012).

Günümüzde ise en son 23 Nisan 2015 tarihinde kabul edilmiş Siber Strateji belgesi (*"The Department of Defence Cyber Strategy*) yürürlüktedir. Bu belge siber ataklara karşı ABD çıkarlarını koruma, askeri ve gizli siber operasyonları planlama gibi operasyonlara rehberlik etme, görevleri verilmiştir. ABD'nin stratejik belgelerinde Çin, Rusya, Kuzey Kore ve İran saldırgan düşman olarak *(Key Cyber Threats)* tanımlamaları, bu ülkelere karşı alınacak olağan üstü karar ve eylemleri, sadece kendi ülkesi için değil bütün dünyaya aklamış veya en azından alışmalarını sağlamış olur.

Space News adlı haber sitesinin aktardığına göre, ABD'li General David Goldfein, 23 Şubat 2018, Orlando Hava Kuvvetleri Birliği Hava Harp Sempozyumu'ndaki konuşmasında ABD'nin 'uzay savaşlarında' üstünlüğü eline alması gerektiğini vurgulayarak, "Birkaç sene içinde uzaydan savaşabiliriz" ifadelerini kullanmıştır (Erwin, 2018). "Uzayda savaş" söylemini kullanarak, hedef kitlede bir nevi korku tohumlarını attıktan sonra konuşmasının devamında da, ABD Hava Kuvvetleri'nin bu çekişmeli alanda öncülük yapmaları gerektiğini, Amerikan ulusunun bunu talep ettiğini öne sürmüştür. Goldfein ABD ordusunun askeri ateş gücünü güçlendirmesi için Hava Kuvvetleri'nin hava, kara, deniz, uzay ve siber alem dahil tüm alanalardan gelen savaş alanı istihbaratını kullanması gerektiğini vurgulamıştır (Erwin, 2018). Diğer bir deyişle, önce dinleyicilere ülkenin tehlike içinde oldukları fikri enjekte ettikten sonra alınması gereken eylemleri öne sürmüştür. Aynı toplantıda konuşan ABD Başkan Yardımcısı Mike Pence de ABD'nin 'Dünya'da olduğu gibi uzayda da egemen güç olması gerektiğini' savunmuştur. (www.tr.sputniknews.com, 2018).

Şubat 2003'te kabul ettiği ilk Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji belgesi ile birlikte, başta Rusya ve Çin olmak üzere diğer devletlerin ve devlet dışı aktörlerin artan siber imkan ve kabiliyetlerini kendisine yönelik olarak askeri ve espiyonaj merkezli yeni tehdit odakları olarak kabul etmiştir. Belgenin asıl amacı, *ABD kritik altyapısını siber ataklara karşı korumak, ABD siber savunma sistemindeki açıkları tespit etmek ve gidermek, olası saldırılar karşısında uğranılabilecek zararı minimize etmek* şeklinde ifade edilmiştir (The White House, 2003). Belge yayınlandıktan sonra, kurumsal yapılanmalarını yeni şartlar dahilinde organize etmeye başlamıştır. Bu belge, ABD'nin siber uzay alanını tanımlayan, bu

alandaki hedef ve planlamalarını ortaya koyan, ulusal siber uzayın nasıl korunacağına dair planlanan sistemi belirleyen, siber uzay kaynaklı tehditleri tarif eden ilk geniş kapsamlı dokümandır.

Stratejik ve Uluslararası Çalışmalar Merkezi'nin (CSIS) başkan yardımcı olan James Andrew Lewis'in yazdığı rapora göre, askeri ve istihbarat açısından, gelişmiş asker kuvvetlerine sahip ve biri birine düşman olan ülkeler, gerçek anlamda siber saldırılar ile biri birine zarar verebilme riskine sahiptir. Birçok ülke askeri siber gücü edinmekteler, fakat Amerika'nın en tehlikeli rakipleri, siber alanında gelişmiş yeteneklerini ABD'ye göre "düşmanca" niyetle birleştiren Çin ve Rusya'dır. ABD'nin siber alandaki açıklarını kullanarak, ülkenin ekonomik, teknolojik ve askeri 'hegemonyasını' azaltmak için kullanmaktalar, ayrıca siber saldırıları askeri amaçta kullanabilecek kapasiteye sahip en iyi hazırlanmış muhaliflerdendir. Onların başarılarının örnekleri listelenemeyecek kadar çoktur. Yine bu raporda belirttiklerine göre, ABD'ye karşı yapılan saldırıların büyük çoğunluğu Rusya ve Çin'den gelmektedir. Amerika savaş içinde olmasa da, siber uzay tartışılır bir alandır. Lewis'e göre Rusya ve Çin ile siber çatışmanın risklerini yönetmek, Amerika'nın ulusal güvenliği için çok önemlidir, bu konudaki ilerlemeler, gelecekte istikrarsız devletler ve devlet dışı aktörlerle başa çıkmayı kolaylaştıracak daha istikrarlı bir ortam yaratılmasına yardımcı olacaktır. Ayrıca Rusya ve Çin için, şu anda sahip oldukları orantısız avantajları ve nispi cezasızlığı azaltarak istikrar elde edilebilir (Lewis, 2013, s. 4).

Kısacası, siber güvenlik kadar hiç bir sorun önemi bakımında bu kadar kısa zamanda ortaya çıkmamıştı (Singer W. & Friedman, 2014, s. 4), ayrıca siber uzay toplumun her kısmını etki ettiği için, iktidar sahipleri kolayca hedef kitleye kendi düşüncelerini enjekte ederek, olağan zamanda yapamayacakları veya yapmaları çok zor olacak eylemlerini hedef kitleye kabul ettirmiştir. Günümüzde ABD'nin resmi siber organizasyonu ABD Savunma Bakanlığı (*United States Department of Defense*), ABD İç Güvenlik Bakanlığı (*United States Department of Homeland Security* / DHS) ve ABD Gizli Servisleri (FBI / CIA) Şeklinde üçlü bir yapıdan oluşmaktadır. ABD'nin resmi siber organizasyonu oldukça karmaşık ve geniş bir yapıya sahiptir. ABD'nin ulusal siber savunma sisteminin sağlanması amacıyla birbirleriyle koordineli bir şekilde faaliyet yürütmek zorundadırlar. Karmaşık yapısı, ABD'nin federatif yönetim anlayışından kaynaklanmaktadır (Darıcılı, 2017, s. 339).

Siber tehditler konusunun son yıllarda bu kadar dikkat çekmesinin en önemli nedenlerinden biri, siber tehdit kavramlarının tehdit siyaseti sürecinde, ABD'li yetkililer ikna edici bir şekilde modern toplumların hayatının her alanını ettiklerini iddia etmeleridir. Tartışma giderek artan şekilde, her şeyin, örneğin, evlerin ve işyerlerinin enerjisinin ve sağlık bakım sistemlerinin etkinliğinin sağlanması dahil olmak üzere, bilgi sistemlerinin ve ağların güvenilirliğine bağlıdır. Bu kritik bilgi altyapıları, sürekli olarak veri alışverişi, devlet operasyonları, acil servisler ve ticaret için çok önemli olduğu için, kritik altyapıların omurgası olarak kabul edilir. Bilgiye/enformasyona olan bu bağımlılık - teknik güvenlik boşluklarından, teknolojinin karmaşıklığından, devam eden piyasa liberalizasyonundan ve kötü niyetli aktörlerin fiziksel ve siber saldırılarda bulunma konusundaki artan istek ve istekliliğinden kaynaklanan artan güvenlik açıkları ile birleştiğinde – en azından teoride de olsa, telekomünikasyon ve bilgi sistemlerini son derece savunmasız hedefler haline getirmektedir (Cavelty, 2007).

Devletler ve medya, tekrar tekrar siber tehditler hakkında bilgi dağıtırken, ölüm ve yaralanmalarla sonuçlanan gerçek siber saldırılar ve büyük ölçüde siber alandaki kötü niyetli aktörler tarafından tetiklenen büyük yıkıcı olayların tehditkar senaryoları sadece Hollywood filmlerinde veya komplo teorilerinin bir parçası olarak kalmıştır (Cavelty, 2008, s. 20).

5.Sonuç

"Siber uzay" kavramı, ilk başta kullanıldığı anlamdan çok farklı ve artık tanınmaz hale gelmişken, "güvenlikleştirme" kavramı da 1995'te ilk kullanılış biçiminden farklı zemine kayarak, uluslararası akademik ortama girmiştir. Siber uzay konusu günümüzde en çok güvenlik bağlamında ele alınmaktadır, zira hayatımızın hemen hemen her alanını etkilemektedir. Hayatımızı her yönden kapsayan bu alanının güvensizliği tedirgin etmektedir ki, bazı aktörler bunu güvenlikleştirmeye çalışmaktadır.

Devlet temsilcilerinin, bazen drurumu dramatize ederek, "güvenlik" kavramını dile getirip belli bir gelişmeyi, (bizim durumda siber güvenlik konusunu) özel bir alana sokarak, bu gelişmeyi engellemek, bloke etmek için gerekli tüm araçları kullanma hakkını hedef kitleden talep etmiş oldular, ve sonucunda da stratejik belgelerinde yazılan amaçlar doğrultusunda çalışmalarını yürütmek için olağan durumda almayacakları karar ve yapmayacakları eylemleri, bu "özel durumda" yapabilecekleri için, kendilerini önceden aklamış oldular.

ABD'de Clinton döneminde başlayan siber uzayın güvenlikleştirilmesine yönelik çalışmalar, Obama döneminde en yoğun şekilde geliştirilmiştir.

Güvenlikleştirme teorisine göre, bir konunun güvenlikleştirilip güvenlikleştirilmeyeceğini güvenlikleştirici iktidar sahibi aktör belirler. Onun verdiği bu karar ise her zaman politik karardır. (Buzan, Waever, & Wilde, 1998, s. 29) 2009 ile 2018 arasında Siber Güvenlik konusunda yapılan konuşmalar, kabul edilen stratejik belgeler, yeni kurumların oluşturulması, ister 2015 Ocak, Ulusal Siber Güvenlik İletişimi ve Entegrasyon Merkezinde Obama'nın yaptığı konuşma (Obama, 2015) olsun hepsi, 2012'deki ABD'ye karşı yapılan siber saldırıları, karşılaştıkları en ciddi ekonomik ve ulusal güvenlik sorunlarından biri olarak tanımlaması gibi siber uzayı güvenlikleştirmek amacıyla yapılmıştır.

Hedef kitleyi inandırmak amacıyla kullandıkları ifadelerin ve eylemlerin başarılı olup olmadığını irdelerken, kısmen da olsa başarılı olduklarını görmekteyiz. Çünkü yeni kurumların oluşturulması, siber uzayı güvenlikleştirmek amacıyla yapılan her hamle, bütçeden yüklü miktarda para gerektirir, ve sorunları zamanında Kongre'ye taşıyarak, Kongre'nin onayını almıştır. Bugün sorunlarla başedemezlerse, başka böyle şansının olmayacağını, veya geç kalacaklarını öne sürmüştür. Diğer örnek, ABD'li General David Goldfein, 2018 Şubat konuşmasında, bir kaç yıl sonra uzayda savaşabilecekleri fikrini ortaya atarak, dinleyici hedef kitle içine bir korku temelini attıktan sonra, ABD Hava Kuvvetleri'nin bu çekişmeli alanda öncülük yapmaları gerektiğini, ve bunu da Amerikan ulusunun talep ettiğini öne sürmüştür ki, olağanüstü tedbirler ya da araçlar gerektiren bir tehdidi belirlemiş oldu. Başka deyiş ile, uzayda savaş kavramını kullanmakla, "tehdidi" etiketlemiş oldu. Bunun devamında da ilgili kurumlardan, ve hedef kitleden "uzayda galibiyet" uğruna, gereken tedbirleri talep etme hakkını almış bulunmaktadır.

Kaynakça

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context . *European journal of international relations, 11*(2), 171-201.

Balzacq, T. (2010). A theory of securitization: origins, core assumptions, and variants. T. Balzacq içinde, *Securitization Theory: How Security Problems Emerge and Dissolve.* Routledge.

Buzan, B. (1997). Rethinking security after the Cold War. *Cooperation and conflict*, *32*(1), 5-28.

Buzan, B., Waever, O., & De Wilde, J. (1998). *Security: a new framework for analysis.* Lynne Rienner Publishers.

Buzan, B., Waever, O., & Wilde, J. D. (1998). *Security: a new framework for analysis.* Lynne Rienner Publishers.

C.Williams, M. (2003). Words, images, enemies: Securitization and international politics. *International studies quarterly*, *47*(4), 511-531.

Cavelty, M. D. (2007). *Cyber-security and threat politics: US efforts to secure the information age.* Routledge.

Cavelty, M. D. (2008). Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*, *4*(1), 19-36.

Cavelty, M. D. (2012). The Militarisation of Cyberspace: Why less may be better. *Cyber Conflict (CYCON)* (s. 141-153). 2012 4th International Conference on. IEEE.

Choucri, N. (2012). *Cyberpolitics in international relations.* . MIT press.

Darıcılı, A. B. (2017). ULUSLARARASI IX ULUDAĞ ULUSLARARASI İLİŞKİLER KONGRESİ - Dünya Politikasında Kriz ve Değişim. *AMERİKA BİRLEŞİK DEVLETLERİ'NİN SİBER KAPASİTESİNDE ROL OYNAYAN KURUMSAL YAPILANMALARIN ANALİZİ*, (s. 337-352). Bursa.

Erwin, S. (2018, Şubat 24). www.spacenews.com: http://spacenews.com/air-force-chief-goldfein-well-be-fighting-from-space-in-a-matter-of-years/ adresinden alınmıştır

Hansen, L., & Nessenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Hjalmarsson, O. (2013). The Securitization of Cyberspace.

Kiggins, R. D. (2014). US Leadership in Cyberspace: Transnational Cyber Security and Global Governance. J.-F. Kremer, & B. Müller içinde, *Cyberspace and International Relations.* (s. 161-180). Berlin: Springer.

Klimburg , A., & Mirtl, P. (2012). Cyberspace and governance-a primer.

L.Herrera, G. (2016). Cyberspace and sovereignty: thoughts on physical space and digital space. V. Mauer, M. Cavelty, & S. Krishna-Hensel içinde, *Power and Security in the Information Age* (s. 81-108). Routledge.

Lewis, J. A. (2013). *Conflict and Negotiation in Cyberspace, A Report Of The Technology And Public Policy Program.* Washington, DC: Center for Strategic and International Studies.

McDonald, M. (2008, December). Securitization and the Construction of Security. *European Journal of International Relations, 14*(4), 563–587.

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly, 5*(4), 18-38.

O'Reilly, C. (2008, September). Primetime Patriotism: News Media and the Securitization of. *Journal of Politics and Law, 1*(3), 66-72.

Obama, B. (2012, 07 19). *Wall Street Journal*. www.wsj.com: https://www.wsj.com/articles/SB10000872396390444330904577535492693044650 adresinden alınmıştır

Obama, B. (2012, 07 19). *Wall Street Journal, Opinion*. www.wsj.com: https://www.wsj.com/articles/SB10000872396390444330904577535492693044650 adresinden alınmıştır

Obama, B. (2015, 01 13). www.obamawhitehouse.archives.gov: https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent adresinden alınmıştır

Singer W., P., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

The White House. (2003). The National Strategy to Secure Cyberspace. Washington.

The White House. (2009, September 3). Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure. Washington, DC.

The White House. (2011, May). International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World .

Waever, O. (1995). Securitization and Desecuritization. R. D. Lipschutz içinde, *On security*. Columbia University Press.

Williams, M. C. (2003). Words, images, enemies: Securitization and international politics. *International studies quarterly*, *47*(4), 511-531.

www.tr.sputniknews.com. (2018, Şubat 28). Haziran 1, 2018 tarihinde www.tr.sputniknews.com: https://tr.sputniknews.com/abd/201802281032443091-abdli-general-birkac-yil-icinde-uzaydan-savasabiliriz/ adresinden alındı

ISSN: 2587-1218

CYBER DETERRENCE BY PUNISHMENT: ROLE OF DIFFERENT PERCEPTIONS

Nasser S. AlAzwani[♣]

and

Thomas M. Chen[♣♣]

Abstract

Nuclear deterrence based on mutual assured destruction seems to have successfully prevented a global nuclear war for decades. Can deterrence be effective for cyber-attacks between nation-states? The cyber environment is drastically different from the nuclear case. A major difference is the possibility of different perceptions by the states which may lead to a failure of cyber deterrence. In this paper, we compare differences between nuclear deterrence and cyber deterrence. We adapt a game theoretic model from the nuclear case to the cyber environment and show that differences in perceived payoffs can lead to attack strategies where deterrence fails in cyberspace.

Keywords: Cyber security; deterrence theory; cyber deterrence; game theory; cyber defense.

1 Introduction

States around the world have become more dependent on technology and integrated systems (Rinaldi, 2001). Recognizing potential vulnerabilities in critical infrastructures, cyber security is now a top national priority for many states. Undoubtedly, ICT (information and communication technologies) brings societies and multinationals closer culturally (Betz, 2017) but has introduced serious challenges at the same time. Technologically advanced states are more at risk of enemies exploiting their vulnerabilities to gain unauthorized access to network resources or to cause harm to systems or people.

♣ PhD Candidate, University of London, nasser.al-azwani@city.ac.uk.

♣♣ PhD Candidate, University of London. tom.chen.1@city.ac.uk.

ISSN: 2587-1218

It is well known that security was not a high priority in the original design of the Internet. Since the Internet was opened to public services, cybercrime and cyber-attacks have become commonplace (Carter, 2017). Cyber-attacks now threaten national security, and policy makers are challenged with dealing with threats from enemy state actors.

Cyber-attacks are possible because of vulnerabilities in critical infrastructure (Hughes, 2014), (Stoneburner, 2013). Control systems are increasingly connected to the Internet which allows adversaries from anywhere to carry out reconnaissance and remotely scan for vulnerabilities. An example incident was the malware attack on Ukraine's electrical grid that brought down approximately 75 percent of its electricity service (Sullivan, 2017). Unfortunately, the complexity of modern systems and networks make them difficult to manage in terms of identifying and mitigating vulnerabilities (Foreman, 2009).

Detecting and responding to cyber-attacks can be extremely costly. Actively responding to attacks with offensive counter attacks has been proposed but the problem is the difficulty of attributing cyber-attacks to the real attacker (Rid, 2015). Active responses also incur a risk of escalating conflicts to more serious levels (e.g., to military confrontations).

Clearly, it is preferable to deter cyber-attacks in the first place. It is mutually beneficial for all states to maintain a peaceful and cooperative cyberspace. However, it is not entirely clear how cyber deterrence can work. Although deterrence theory is well understood for nuclear weapons, the cyber environment is much different.

2 Traditional Deterrence

There is an extensive literature on the effectiveness of deterrence strategy as practiced in international relations (Langlois, 1989). During the Cold War, the threat of global nuclear war was a widespread concern. The main idea behind nuclear deterrence is that any attack by one state on another state would be met with a devastating retaliatory response. This response will minimize any expected gain to the first attacker. Mutual assured destruction was the basis of many national policies for national security (Morgan P. M., 1983).

History has provided examples of different international cases where deterrence was successful (Huth, 1984). Moreover, deterrence was considered the main reason for the

prevention of another nuclear world war as well as prevention of chemical or biological attacks (Powell, 1990).

Deterrence theory is based on the assumption that people will make rational choices. It has been used as the basis for social policies, for instance, to discourage people from committing a broad range of crimes (Morgan P. M., 2003). One of the best references that explains the development of general deterrence theory and its applications is Steff (Steff, 2016).

For successful deterrence, there is a need for defensive capabilities for observability, attribution, and readiness for retaliation (Schelling, 2008). Specifically, successful deterrence is predicated on three premises: (1) the deterrent should have a sufficient capability (2) the deterrent threat should be credible and (3) the deterrent threat should be communicated clearly to the adversary (Paul, 2009).

3 Cyber Deterrence

With the end of the Cold War and the escalation of cyber-attacks between states, a natural question is whether deterrence strategies used to prevent nuclear war can be equally effective to prevent cyber-attacks on critical infrastructure (possibly so-called "cyber warfare") (Elliott, 2011) (Kugler, R. L, 2009). The concepts of deterrence may be similar for cyber space, but in terms of practice, major differences between the natures of cyber and nuclear domains should be recognized.

Cyber deterrence is a proactive strategy rather than a reactive defensive strategy. There is a difference between cyber defense and deterrence. Defense happens after an attack has been initiated in order to mitigate damage from the attack or win the conflict. In contrast, deterrence aims to prevent the conflict altogether and maintain peace within the cyber space. Clearly, cyber deterrence should be preferred over defense, just as in healthcare, prevention of disease in the first place is better than curing disease after it happens. By implication then, cyber deterrence should have high priority from the perspective of national security policies.

As mentioned earlier, successful deterrence depends on three essential pillars (Quackenbush, 2011):

- A credible defense meaning that the defender will be able to force the attacker to give up ultimately (the gain for the attacker will be less than the loss).

- Readiness to retaliate in the event of an attack.

- Willingness to retaliate against the attacker.

The challenges of cyber deterrence raised in the literature such as attribution, retaliations, and escalation (Wei, 2015) can be addressed in the context of these three pillars.

Cyber deterrence depends on a strong defense. Technologies for cyber defense have made great advances for attack detection, mitigation and recovery, but technology offers limited defense (Multari, 2017). For example, Stuxnet was able to compromise an Iranian nuclear power plant despite Iranian precautionary controls (Farwell, 2011). Another example, malware hit the western part of Ukraine bringing down the electricity for more than six hours on December 23, 2015 (Zetter, K, 2016).

In traditional deterrence, there are two types of deterrence strategy: deterrence by denial and deterrence by punishment. These two strategies also rely on credibility, capability, and communication with opponent (Bendiek, 2015), (Lowther, 2012). Both strategies are discussed below in the cyber space context.

3.1 Cyber deterrence by denial

The objective of deterrence by denial in cyber space is to develop a strong cyber defense that will make it very difficult for cyber-attacks to succeed. Typical defenses (so-called defense in depth) consist of multiple layers including firewalls, intrusion detection systems, unified threat management, and encryption. The human element includes cyber security training and raising awareness of best practices.

In terms of the three factors mentioned earlier:

• Capability: states need to harden and strengthen their systems, particularly in terms of testing for vulnerabilities and patching.

• Communication: national and international cooperation may lead to agreement on norms or treaties between states.

• Credibility: investments in defenses must be convincing to potential attackers.

3.2 Cyber deterrence by punishment

Cyber deterrence by punishment is an alternative to deterrence by denial. In this strategy, a defending state threatens retaliation against any attacking enemy state. The retaliation should be perceived by the attacker to inflict more cost than the perceived gains. In order for retaliation to work, it must be possible to attribute the attacker. This is straightforward in the case of nuclear weapons but not that easy in the cyber domain where cyber-attacks may be stealthy.

• Capability: states must be able to attribute cyber-attacks, presumably easier with robust military or law enforcement agencies. International cooperation is often required for attribution, but the lack of an international framework for cooperation is a major challenge.

• Communication: states need to clearly advertise their readiness to retaliate against any attacker.

• Credibility: the threat of retaliation must be convincing to potential attackers.

4 Problem and Approach

Nuclear deterrence by punishment is straightforward in terms of capability, credibility, and communication. All states are aware of each other's capabilities and the consequences of attacking each other. Moreover, all states are aware of the readiness and willingness of other states to retaliate.

In contrast, the cyber domain involves more uncertainties. A cyber-attack may cause damage perceived differently by the attacker and defender. A critical target chosen by the

attacker may actually be less valuable to the defender. Depending on the perceived damage, retaliation may or may not happen. In this paper, we investigate the consequences of different perceptions about the value of assets.

Game theory has proven to be a useful tool for analyzing strategic and competitive situations like deterrence. A game models the possible actions within a conflict and helps the players understand their best choice of action. Different types of games have been studied, depending on deterministic or random, complete or incomplete information, pre-commitments, signaling or no signaling, cooperation or no cooperation, and so on (Wang, 2016).

Our approach is to start with the traditional deterrence game (developed for nuclear deterrence) and then adapt the game model to the cyber domain (Do, 2017). There is a large literature discussing cyber deterrence but little of it uses game theory. Analysis of the game model will help to understand conditions leading to success or failure of cyber deterrence.

5 Game model for traditional deterrence

Figure 1shows a simple two-player deterrence game in extensive form representing the traditional (nuclear) conflict. As usual, players are assumed to be rational and always seeking the best strategy to maximize their payoff. In this game, the players represent two nation-states in possible conflict. State A is the challenger threatening to attack State B, while B wants to deter the attack.

Since A is the challenger, A has the choice of first move which can to attack B or not. If A does not attack, B can attack pre-emptively or maintain the status quo. If A attacks, B can retaliate or not respond. It makes no sense for B to do nothing if A attacks. For deterrence to be effective, B should pre-commit to retaliate immediately if A attacks; thus, A is certain about mutual destruction if A attacks.

The payoffs for A and B, respectively, are noted as (Ai, Bj). It is assumed that payoffs are ordered: A1 < A2 < A3 < A4 and B1 < B2 < B3 < B4. The payoff for (status quo) should

be no change, so A3 = B3 = 0. This game has three possible strategic scenarios as shown in Fig. 1:

1. Status quo (no attack by either A or B);
2. A loses and B wins (no attack by A followed by a preemptive attack by B);
3. Mutual destruction (A attacks followed by retaliation by B).

The fourth outcome (A attacks and B does not respond) is not possible because B pre-commits to retaliate if A attacks. If A attacks

Hypothesis: State B can deter State A by a threat of sufficient and certain retaliation (deterrence by punishment).

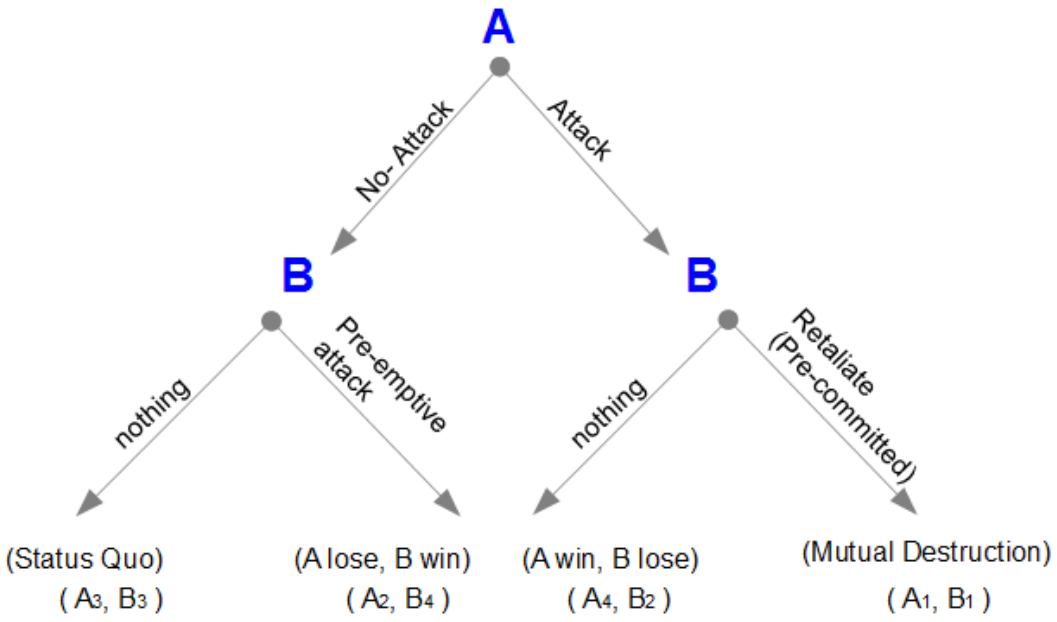


Figure 1: Deterrence game (Brams, 1985).

Games in extensive form are usually solved by backward induction. First, consider the subgame where A does not attack B. In the subgame, B has a choice to do nothing or pre-emptively attack A. The payoff for pre-emptive attack is higher, so B should choose to attack A. In this subgame, A should expect a loss of A2 (a negative payoff).

Next, consider the other subgame where A chooses to attack B. B is pre-committed to retaliate, and the result is mutual destruction. The payoff to A is A1 (a negative payoff). Working backwards, A has the choice to attack with payoff A1 or not attack with payoff A2. Since it is assumed A1< A2, it is better for A to not attack. Thus, A is effectively deterred from attacking B because of the threat of punishment. It might seem in this case that B will win and A will lose, because B will pre-emptively attack A with payoff B4. However, it should be pointed out that the game is symmetric. In other words, A will retaliate against B if B chooses to attack, so B is equally deterred from attacking A. Since A and B are mutually deterred from attacking each other, the status quo is maintained (Cimbala, 1998).

Again consider the subgames and work backwards. The first subgame is not changed. However, the subgame where A attacks has different expected payoffs now. The expected payoff for A is

$$E(\text{A's payoff}) = P\,A4 + (1 - P)\,A1 \qquad (1)$$

Working backwards, A has the choice to attack with payoff $P\,A4 + (1-P)\,A1$ or not attack with payoff A2. The incentive to attack is greater if

$$P\,A4 + (1 - P)\,A1 > A2 \qquad (2)$$

Or the probability that B will not retaliate is

$$P > \frac{A2 - A1}{A4 - A1} \qquad (3)$$

In this case, A may be tempted to attack B if A believes that there is a sufficient chance of "getting away with it" (i.e., B will not respond). For effective deterrence then, it is important for B to: (1) establish credibility for retaliation with nuclear capabilities and (2) communicate willingness, readiness, and pre-commitment to retaliate.

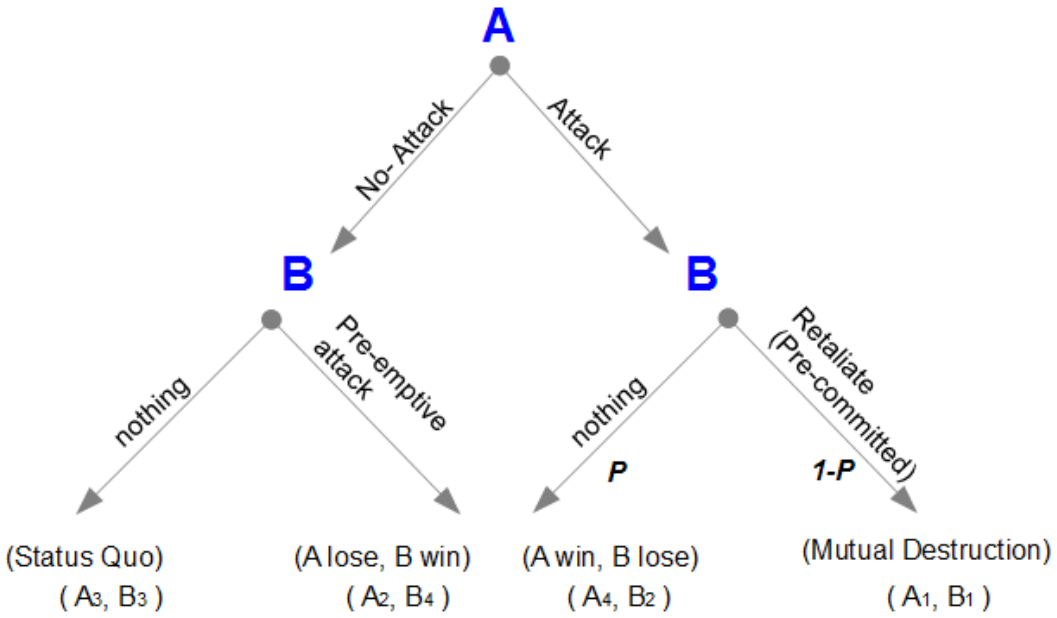


Figure 2: Deterrence game with uncertain retaliation.

6 Game model for cyber deterrence

The previous section described how states are deterred from attacking each other because of mutual assured deterrence. However, the situation is clearly different for cyber-attacks. It is well known that states conduct ongoing cyber campaigns against each other. Why does deterrence work for nuclear war but not for the cyber domain?

The targets and damages from cyber-attacks are different from nuclear attacks. Nuclear attacks are obviously devastating, cyber-attacks are much more varied. Some cyber-attacks are aimed at data theft while others more serious attacks are aimed at critical infrastructures (Shackelford, 2017). Thus, the payoffs (gains and losses) in a cyber deterrence game model are more difficult to ascertain (Philbin, 2013).

Critical infrastructure typically encompasses energy, telecommunications, financial services, water, and transportation, but there is not a universal agreement. These can span both public and private sectors. In the U.S., the definition of critical infrastructure has been expanded to include systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on securing, national economic security, national public health or safety (Moteff,

2003). They have different levels of importance in economic, social and military terms (Moteff. J, 2004).

The problem with cyber deterrence by punishment arises because state A does not fear retaliation from state B. This might happen because:

- A does not its loss from retaliation as much as B perceives the loss to be;
- B may not retaliate because the loss from A's attack is not serious enough to merit retaliation.

Both might happen when the two states have different perceptions about payoffs in the game.

In theory, cyber deterrence should be based on the same game model shown in Fig. 1. State A is certain of a loss from attacking B if B pre-commits to retaliation. The expected loss from attacking B should be greater than the expected loss from doing nothing. By symmetry, both states see the status quo as the rational strategy.

In the previous section, it was established that state A will be deterred if A1 < A2, which was assumed. However, this may not be A's actual perception of the payoffs if the specific target of retaliation by B was unintentionally chosen to be less valuable to A than believed. What if A perceives that the loss from mutual destruction, A1, is actually less (i.e., more positive) than the possible loss from doing nothing, A2? Then A's best strategy would be to attack B and risk mutual destruction.

Another possibility is that B may not choose to retaliate if A attacks. A pre-commitment to retaliation was assumed for mutual assured destruction. However, let us reconsider the second subgame in Fig.1. If state A attacks, B has a choice to retaliate or do nothing. Retaliation incurs a loss of B1 while doing nothing will be a loss of B2. It was assumed that B1 < B2, that is, B's actual best strategy is to do nothing if A attacks. However, this strategy was ruled out because it could encourage A to attack; a pre-commitment to retaliate is a prerequisite for deterrence. However, if B2 is a small loss that B can tolerate, then B may actually choose to do nothing. In any case however, B should "signal" (communicate clearly) it's pre-commitment to retaliate in response to an attack by A, in order to deter A, even if B does not actually follow through on retaliation.

7 Deterrence Strategy: (Target Selection)

In the previous section, we discussed that the payoffs in the cyber deterrence game can affected by the choice of targets. That is, the value of targets may not be perceived as expected by the other state. This can change the strategic choices of states leading to failure of deterrence.

Fig. 3 is a visualization of the value calculation that both states A and B carry out to decide on their best strategies. If A chooses to attack, it must weigh the perceived value of the target, and whether damage to the target will elicit a retaliation from B. In turn, B should weigh the perceived value of the target to retaliate against. For successful cyber deterrence, this target should be valuable enough to discourage A from attacking in the first place.

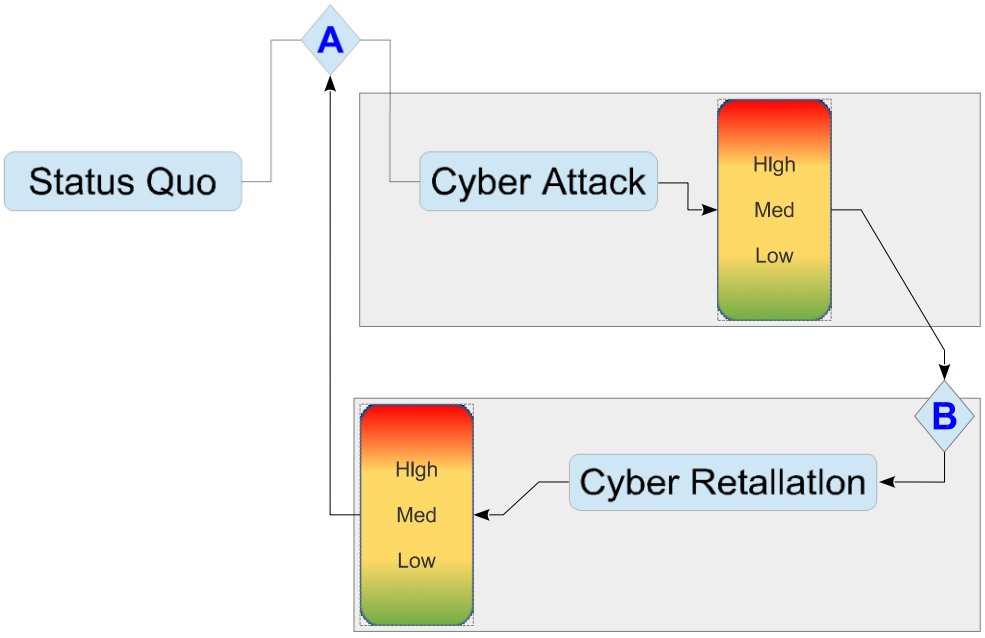


Figure 3: Attack and retaliation perceptions.

As the previous section established, misunderstandings of the game can arise from different perceptions of target values. For successful deterrence, it is important to minimize the differences in perceptions (Libicki, 2009). It is also important, as in nuclear deterrence, for each state to signal it's pre-commitment to retaliate to a valued target of its enemy, even if

the retaliation is not actually carried through. Deterrence by punishment can work only if the enemy fears a serious retaliation.

8 Conclusion

This paper has analyzed the traditional deterrence game model and has attempted to explain the role of threat of retaliation strategy in the success of nuclear deterrence. So far nuclear deterrence has seemed to work to avoid global nuclear war, but cyber deterrence has not worked. We have applied the deterrence game model to the cyber domain to explore reasons for the failure of cyber deterrence. One of the reasons may be different perceptions of target values, i.e., payoffs in the game model. Target selection plays a vital role in affecting the states' perceptions of the payoffs and ultimately their best strategic choices.
It is important that targets are chosen suitably, and pre-commitment to retaliation is signaled clearly between states, in order to minimize the difference in perceived payoffs. If both states understand the game clearly, then the principle of deterrence by punishment should work for cyber deterrence.

Kaynakça

Bendiek, A. &. (2015). Deterrence theory in the cyber-century. INFORMATIK, Bonn: Gesellschaft für Informatik, 553-570.

Betz, D. J. (2017). Cyberspace and the State: Towards a Strategy for Cyber-power. London: Routledge.

Brams, S. (1985). Superpower games: Applying game theory to superpower conflict. New Haven, CT: Yale University Press.

Carter, W. A. (2017). CYBERSECURITY LEGISLATION AND CRITICAL INFRASTRUCTURE VULNERABILITIES. Foundations of Homeland Security: Law and Policy, 233-249.

Cimbala, S. J. (1998). The past and future of nuclear deterrence. London: Greenwood Publishing Group.

Do, C. T. (2017). Game theory for Cyber Security and privacy. ACM Computing Surveys (CSUR), Volume 50 Issue 2, June 2017 Article No. 30 .

Elliott, D. (2011). Deterring strategic cyberattack. IEEE Security & Privacy, 9(5), 36-40.

Farwell, J. P. (2011). Stuxnet and the future of cyber war. Taylor & Francis, 23-40.

Foreman, P. (2009). Vulnerability management. New York: Auerbach Publications.

Hughes, J. &. (2014). Three tenets for secure cyber-physical system design and assessment. International Society for Optics and Photonics, vol. 9097, p. 90970A.

Huth, P. &. (1984). What makes deterrence work? Cases from 1900 to 1980. World Politics, 36(4), 496-526.

Kugler, R. L. (2009). Deterrence of cyber attacks. Cyberpower and national security,. Retrieved from Center for Technology and National Security Policy (CTNSP): http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf

Langlois, J. P. (1989). Modeling deterrence and international crises. Journal of conflict resolution, 33(1), 67-83.

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. . Santa Monica, CA: Rand Corporation.

Lowther, A. (2012). Deterrence: rising powers, rogue regimes, and terrorism in the twenty-first century. New York: Springer.

Morgan, P. M. (1983). Deterrence: A conceptual analysis . Sage Publications.

Morgan, P. M. (2003). Deterrence Now. Cambridge: Cambridge University Press.

Moteff, J. C. (2003). Critical infrastructures: What makes an infrastructure critical? Library of Congress Washington DC Congressional Research Service, 21.

Moteff. J, P. P. (2004). Critical infrastructure and key assets: definition and identification. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 20.

Multari, N. J. (2017). SafeConfig'17: Applying the Scientific Method to Active Cyber Defense Research. Proceeding CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. pp. 2641-2642). Dallas, Texas: ACM.

Paul, T. V. (2009). Complex deterrence: Strategy in the global age. University of Chicago Press.

Philbin, M. J. (2013). Cyber deterrence: An old concept in a new domain. . DEFENSE TECHNICAL INFORMATION CENTER, 32.

Powell, R. (1990). Nuclear deterrence theory: The search for credibility. New York : Cambridge University Press.

Quackenbush, S. L. (2011). Understanding general deterrence. In Understanding General Deterrence. New York: Palgrave Macmillan.

Rid, T. &. (2015). Attributing cyber attacks. Journal of Strategic Studies, 4-37.
Rinaldi, S. M. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems, 21(6), 11-25.
Schelling, T. C. (2008). Arms and influence. In Strategic Studies. London: Routledge.

Shackelford, S. J. (2017). From Russia with Love: Understanding the Russian Cyber Threat to US Critical Infrastructure and What to Do about It. Nebraska Law Review, Volume 96 | Issue 2 Article 5.

Steff, R. (2016). Strategic Thinking, Deterrence and the US Ballistic Missile Defense Project: From Truman to Obama. London: Routledge.

Stoneburner, G. G. (2013). Risk management guide for information technology systems. NIST.

Sullivan, J. E. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. The Electricity Journal, 30(3), 30-35.
Wang, Y. W. (2016). A survey of game theoretic methods for cyber security. In Data Science in Cyberspace (DSC) (pp. pp. 631-636). Changsha, China: IEEE International Conference on . IEEE.
Wei, M. L. (2015). The Challenges of Cyber Deterrence. JOURNAL OF THE SINGAPORE ARMED FORCES, 1-41.

Zetter, K. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. Wired.

THE CHANGING STRUCTURE OF WAR IN A CYBER-WORLD AND ITS IMPACT ON THE INTERNATIONAL HUMANITARIAN LAW

Mohammed Ishmeal[♣]

Abstracts

War as a social construct of dominating others to achieve ones interest at the expense of other in a competitive global community is an enigma to resolve in the discourse of International Humanitarian Law. Thus, the salience of the transformations of the structure of war in the midst of the current transition of geopolitics from a unipolar world to a seemingly multi-polar world reverberate the debate of international law within the domain of cyber technological weapons, specifically, International Humanitarian Law. This has raised many questions in the application of international humanitarian law in a world where electromagnet weapons, cyber weapons and high-tech defensive system are developed to counter enemy attack. This paper discuss the changing nature of war in a cyber-world bringing to bear its impact on the International Humanitarian Law. The paper posits that with the fast changes in war strategy and cyber oriented weaponry, an improved sophisticated and inclusive laws with a stronger institutional backing must be developed considering the socio-cultural and technological ideas of countries to increase the level of compliance.

Key Words: *International Humanitarian law (IHL), armed conflict, structure of war, law of war. Cyberspace, Cyber technology, Cyber weapons.*

INTRODUCTION

War has always instill fear in men whether the brave or weak men. This fear and out of necessity to win and survived in this competitive struggle of the anarchic world has pushed man to design weapons, strategies, sometimes in the forms of alliance to maintain his dominance and defend his existence. However, throughout history there has always been laws which governs and regulate every battle whether economic, political, religious or ideological battle. As a result, depending on the period these laws have evolved in time of space and

♣ PhD candidate at Selcuk University in the Department of International Relation, Konya, Turkey. Contact @ blkqatari@gmail.com

period of many civilization which had grace the world. From the great Egyptian, Kush, Assyrians, Mesopotamia, Aztec, Hindus Valley, Carthaginian, Greeks, Romans, Byzantines civilization battles to the religious battles of Israelites, the age of Christian crusaders and the Islamic Jihadist from the time of the prophet Muhammad (P.BUH).

The Crusaders and the Turkish Ottoman Empire wars and the subsequence dominance of the Empires which historians have referred to as "gunpowder empire" which included those of the Safavid Empire of Persia, the Mughal Empire in India, the Russian State, Spain and the Spanish New World(Braden, 2014:21-31), the British and French imperial ambitions in Africa. The gun powder technology was the beginning of western power that also ushered in United States of America in the 20th century who later developed highly technological weapons of dominance into the first decade of the 21st century. The 21st century ushered in a new development not only improved nuclear weapons, but also cyber-technological weapons, namely, Laser and hypersonic weapons, unmanned aerial vehicles, directed-energy weapons, lethal autonomous robots, defensive systems, and electromagnetic weapons.

The expansion of states armies and the development of complex coalition and allies circle to wage war against enemy combatant has changed the nature and structure of war where old rules that regulate wars are no more binding. This means that the laws of armed conflicts applications in some instance during war is not applicable during war.

Another fundamental change of war is the rise of actors such as terrorist groups, the employment of proxy forces by world powers and the hiring of mercenaries and private military and security companies in a growing military industrial world worth billions of dollars. Obviously this have enormous impact on the existing International Humanitarian Law (IHL). Although the law has not been perfect and totally applied, accepted and adhered to much to our expectations due to relativity of culture as agued by some scholars, yet in some instances it applications have saved millions of human life(Loc.gov, 2018). As the *Dagombas* will argue *Kpaha chara so dundo ya'aw* that a "wretched door is better than empty door"[1]. This philosophical proverb simple emphasized the fact that the law might not fulfill global community expectations totally, however, its existence is better for humanity. In the words of Louise 1979:

[1] This is a Dagomba philosophy. Dagomba is an ethnic group in the northern region of Ghana, West Africa. The Dagomba call their homeland Dagbon.

The most important principle of law today is commonly observed: nations have not been going to war, unilateral uses of force have been only occasional, brief, limited. Even the uncertain law against intervention, seriously breached in several instances, has undoubtedly deterred intervention in many other instances. Where political law has not deterred action it has often postponed or limited action or determined a choice among alternative actions(Louis, 1979:25-26).

From the above introduction, it is patent that the structure and nature of war has change with the intense geopolitics in a wider context of cyberspace amidst development of highly technological weapons and the changing forces of actors in events of war and peace. It stands to argue that the International Humanitarian Law is bound to be changed either directly or indirectly. Thus, the central purpose of this paper is to discuss the changes of the structure of war and it impact on the International Humanitarian Law. The paper evaluates the theoretical framework and review literature around the subject of enquiry. The paper further elaborates the historical development of international humanitarian law. And follows up with current changes and developments that seem to make application of International Humanitarian Law difficult drawing examples from past and current events. Finally, the paper conclude with looking beyond the challenges of international humanitarian law with a summary of events and recommendations discuss in the paper. The paper uses the term International Humanitarian Law, and the Law of Armed Conflict or War interchangeable as they are also use in most research to mean the same thing.

THEORETICAL FRAME WORK AND LITERATURE REVIEW

The academic discourse of war and law generates a very interesting theories which dates back to ancient times. During the internal armed conflict in Rome in a forceful argument defending the acts of Milo, Cicero pleaded, "... *silent enim leges inter armeda*."(ICRC, 2018). Allenby recently went further to argue that the idea of law governing war produces three theories. First could be attributed to the realist view that the idea of law governing war is a mistake and therefore must be disregarded since states will do anything to protect their national interest and whatever means used to achieve such target is legitimate and permissible.

Realist assume that in a world of anarchy where every man's hand is against each other, state are selfish and very inward to protect their national interest. The second group of theorists

argue from the standpoint of the morality of the law of war itself since war is evil, inhumane and savage act. Any form of law to minimize damage in a war is not reasonable and rationally weak. Thus, any form of law to regulate this uncivilized conduct (war) of human beings lack moral and human ethical foundation. For them a bird can never be a butterfly likewise a monkey and a gorilla may claim to be one but a gorilla is gorilla and a monkey is a monkey. This groups are usually regarded as pacifist. The third group argue through three shades, the law of *ad jus bellum* (law of going to just war), and the law of *jus in Bello* (law during war) and the law of *ad post bellum*. The latter is not well developed and not included in most work. Therefore, have no historical and practical trajectory to be discussed. For instance maj keith E puls's (2005) *Law 0f War Handbook* (Puls, 2005:11-12) only divided the theories into two and did not include *Jus post bellum.* All these theories developed individually and concurrently.

Jus ad Bellum is the law dealing with conflict management of the laws regarding how states initiate armed conflict? Under what circumstances is the use of military power legally and morally justified?(Loc.gov,2018) This law dates back to 335 B.C. to about 1800 A.D where most instances, determination of a "just cause" was a pre-condition to engage in war. It did not matter how inhumane a war may be, the fact that is justifiable in the face of the world's opinion, this clearly called for military engagement. Aristotle (335 B.C.) wrote that war should only be employed to (1) prevent men becoming enslaved, (2) to establish leadership which is in the interests of the led, (3) or to enable men to become masters of men who naturally deserved to be enslaved. Cicero refined Aristotle's model by stating that "the only excuse for going to war is that we may live in peace unharmed(loc.gov,2018).

The Era of Christian crusade and Islamic jihadist movements cited divine justifications to justify the cause of their war. From the medieval era, to the modern Era saw various modification of this theory and it continues to evolved in the 21st century. The United states invasion of Iraq (2003), Afghanistan (2001) and the intervention of United States and its allies in Libya (2011), Saudi Arabia and Arab allies intervention in Yemen (2015), Bahrain (2011) and the Russia annexation of Crimea (2014) and Russia and France involvement in Syria (2015) are a plethora of instance where countries engage in a conflict by justifying their involvement through United nations mandate or without united nations mandate. This law is normally justified through the United Nations (UN) charter of article 51 the rights to self-defense and "other-defense". Despite the fact that this law is not specific and well certain in

illustrations. The US, unilaterally, justified the war against Iraq based on previous UN votes concerning Iraq and weapons of mass destruction and on grounds of self-defense against terrorism. Opponent of the US-Iraq invasion argue that the war was illegal and a blatant violation of International law since UN Security Council did not give her a mandate through vote with specific to the Iraq invasion. Proponent also rationalized US argument which legitimizes US right to self-defense against external threat.

The second theory is the *jus in Bello* this refers to the regulation of conduct during War. The second body of law which deals with rules that control conduct during the prosecution of a war to ensure that it is legal and moral(loc.gov,2018). This second category is generally referred to as *International Humanitarian Law, or the Law of Armed Conflict.*

The development of this theory could be traced back to 4th century literature of *Sun Tzu's The Art of War* in Ancient China which set out a number of rules that was supposed to regulate the war at the time. The literature indicates what soldiers were permitted to do during war. The rules covers on how captives and innocent civilians should be treated including women and children. Another literature was the ancient Indians *Codified Book of Manu* around 4th B.C which provided in great detail regulation of war in great detail. The ancient Babylonians in the 7th century were reported to have treated both captured soldiers and civilians with respect in accordance with well-established rules(loc.gov,2018).

Maj Keith E Puls explained that the application of *Jus in Bello* during the early period which was preoccupied with *Jus ad bellum* (Just War) little attention was given to *Jus in Bello* and even when it was applied it came after *a just war* was established. Thus, it served as 'Chivalric Code' which regulated chivalry warfare as rules of fair play and good treatment(Puls, 2005:18).

The development of nation-state in the 17th and 18th century specifically between 1800-1918 was the worst of time as states abandon the moral justification of war and made war as part of national policy. Ironically, it was in this same period between Hague Conferences (1899-1907) which represented the last multilateral law recognizing not only in war as a legitimate device of national policy but also concentrated on avoiding war and minimizing suffering during war. This period saw a shift toward an absolute renunciation of aggressive war (Puls, 2005). From the era of League of Nations, Inter-Wars to the period of Post Wars, the theory

of *Jus in Bello* has shaped and regulated world conflicts to presents. This theory metamorphosed into law of war, law of armed conflict and widely known as *International Humanitarian Law*.

This theory is also built upon three fundamental principles which regulate the conduct of hostilities and clearly define rules during international armed conflict. These principle include principle distinction, proportionality and precaution. These principles sought to balance the right to human dignity, military target and achievement. The principle of distinction is also known as discriminations. It emphasize on the need for the combatant to distinguish themselves from non-combatant both military assets and civilian areas. It does not accept the use of civilian enclaves to target military assets, neither does it allow the use of civilian as human shield to achieve a military target.

The principle of proportionality seeks to enforced combatant to be proportional in their military activities to achieve military target. Thus, it is not appropriate for combatant or country to respond to border incident with nuclear bomb or any weapon of mass destruction. However, the law does not rule out colossal damage to human life and properties as far as the response is legal.

The principle of precaution cautions the use of nuclear and hydrogen weapons and biological weapons to avoid colossal damage to human life. This denies the use of *mala in se*, or evil in themselves like weapons of mass destruction and cluster bombs. Interestingly, the complex nature of a more horizontal world which include cyber and physical space, obviously, affect the nature and how actors engage in conflicts. Therefore, the above principles discussed scope of operation and limitation in the conflict zone are beginning to be narrowed and anachronistic.

HISTORICAL DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW

In any period of history there has been complex web of law either directly or indirectly emanating either customarily or treaty in one way or the other to regulate or justify a 'just war'. It is out of this welter of development from past that shaped international law in the 19th century. It is generally agreed that the 1864 adoption of Geneva Convention sowed the seed that geminated to become the law of armed conflict also known as *International*

Humanitarian Law. It is obvious that no civilization in the course of history whether Africans, European, Chinese or Indians, really, wanted to be witnessing the horrors of war. Although international humanitarian law developed as a European concept, the law of *jus ad bellum* and the *Jus in Bello* did not elude the people of the other parts of the continent. These concept were practically applied much same way in their tradition with a different understanding and philosophical designation. Among the Mole-Dagbon kingdom in Ghana, a group of professionals who were called *Lunsi*[2]were exclusively protected during war. This was not different from the other laws which were restricted to a specific region and only protect specific personalities of professions. Thus, the need and call for law to regulate the horrific war which was witnessed in the 19th century was not only natural but generally universal.

Henry Dunant memoire in 1959 at the battle of Solferino which he documented in a small hand book in 1962 *A Memory of Solferino(Dunant, 1986:147)* caused uproar and increased the awareness of evil fate of war in Europe. It was this memoir that led to the foundation of the International Committee of the Red Cross (ICRC, Cp.15). As armies became increased, the brutality of war became apparent in the 19th century in large scale as multitudinous of human death were recorded on the battlefield. The horrific nature led to an unexpected development which was a decisive factor in the foundation of the Red Cross and the adoption of the Geneva Convention of 1864. This incident were the precursor to subsequent further conventions on the laws of war(Schindler and Toman, 1998:vii). Further, most importantly, the second half of the 19th century gave rise to a growing conviction among generals, academicians , politicians, humanitarians and philanthropist that there was a great need of 'restraining the destructive force of war'(Oxford, 1880). This was followed by the 1899 and 1907 Hague Peace Conferences. This conferences for the first time through a compilation of available customarily laws agreed to regulate war. The peace conference emphasized on the minimization of collateral damage and suffering in a war and the necessity to discriminate and distinguish between combatant and non-combatant to minimize casualties and save more human lives. It is important to observe that this was necessary because of the change in war structure at the time.

[2] These were a group of drummers who served as journalist and documented the history of the war through reporting incidents that transpired. They were adept in memorization and the art was skillfully passed down from one generation to another through meticulous and methodic training from childhood.

Although the principle of distinction had appeared in the Declaration of St. Petersburg of 1868 document to 'specifically highlight this principle'. It stated that "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy not target civilians. This argued that non-combatant were not supposed to be targeted including the injured and prisoners of war who had seized to participate in the war.

Another principle of engagement which was developed was the means of warfare and the rights of belligerents to adopt such means of injuring the enemy. Article 12 of the Brussels Declaration of 1874; Article 4 of the Oxford Manual 1880; and Article 22 of Hague Regulations of 1899 and 1907 expressly restrained the warring parties to employ armed projectiles or materials of such nature to cause unnecessary sufferings. After the WW1 more laws were codified to refine and update the existing law to keep the League of Nations instruments in shaping the law of armed conflict. Thus, in 1929 the laws were revised and new two laws were additionally adopted. These new instruments period were the Protocols on the Prohibition of Poisonous Gases and of Bacteriological Methods (Geneva Protocol of 1925, No. 13) and the Protocol on Submarine Warfare (London Protocol of 1936, No. 74).

The aftermath of the Second World War witnessed another conference in the 1949 where the International Law Commission of the United Nations, at its first session, selected the topics for codification. Unfortunate, majority of the members of the Commission opposed due to the fact that they feared the public will lose confidence in the effectiveness of the means at the disposal of the United Nations for peace(Paoers, 2018). The 1949 convention framework maintained the existing laws and protected prisoners of war, wounded combatant, civilians and noncombatant. These were regarded as a carbon copy of the old principles. With emergence of new forms of war such as proxy war across former colonies and civil wars fell outside the label conventions of international armed conflict. Thus, in 1977 the laws of armed conflict was classified into two embracing the both international armed conflict and non-armed international conflict, these were Geneva Law and Hague law.

Geneva Law is mainly concerned with the protection of the victims of armed conflicts. It cover non-combatants and those who no longer take part in the hostilities like the injured. Whereas the Hague Law provides limitations or prohibitions of specific means and methods of warfare(Antonie and Quintin, 2011:52). It is worthwhile to mention that the cruelty and

insensitivity of civil wars and proxy wars raised many concern with regards to international human rights violation during armed conflict. The 1968 Tehran international conference under the auspices of UN General Assembly conference, The International Conference on Human Rights in Teheran, in 1968, organized by UN General Assembly provided an incentive, which adopted a resolution on "Human Rights in Armed Conflict" (No. 30). It declared that: The Provisions of the Hague Conventions of 1899 and 1907 were intended to be only the first step in the provision of a code prohibiting or limiting the use of certain methods of warfare and that they were adopted at a time when the present means and methods of warfare did not exist.

International Human Rights jurisprudence geared toward filling the loopholes in international humanitarian conflicts and raised the degree of violation of law of armed conflict as a crime against not just humanitarian law but a blatant crime against humanity. The issue of unintended aerial bombardment, landmines, genocide, siege, rape, drones attack, plane hijacking, hostages in urban centers and suicide all have contributed geared towards effecting changes in the dynamics of war making it difficult for the enforcement and compliance of the existing law of armed conflict. Thus, the prosecutions of persons suspected to have committed crime against humanity and human rights during an armed conflict became paramount under the International Criminal Court of Justice. This was made possible as a result of the adoption of Rome Statute of International Criminal Court.

International humanitarian law and international human rights joined forces to put pressure on actors to take responsibility of implementing the international humanitarian law either in international armed conflict or non-international armed conflict. This however, draws the difficulty in implementing the laws of armed conflict while reasonably derogating certain human rights for both military target, preventing security threat and balancing human rights at the same time. The uncertainty and unpredictability of state interest and actions and the continued widening of cyberspace and the development of sophistication modern technological weapons couple with changes in military forces and actors such as mercenaries, private military and security companies has transformed the nature and structure of war making it very complex and challenging for the implementation of IHL. The next section draws some of the hotspot in the law of armed conflict in relation to cyber-world current trends in international geopolitics.

NEW MODE OF WAR, CYBERSPACE AND TECHNOLOGIES AND ITS IMPACT ON INTERNATIONAL HUMANITARIAN LAW

The complex nature of war makes it very difficult not only to define but to predict war for it comes with different shades of ideals, shapes and forms with a purpose to triumph over perceived enemy whether directly or indirectly. Thus, if laws were going to regulate such a complex phenomenon like war then definitely changes would be expected in the codification of such laws in time of space, period and degree. Historically, the advancement of any civilizations in military technology, strategy of war and weaponry capability impacts on existing laws which guide, regulate, manage and control rules of engagement in international armed conflict and non-international armed conflict had gone through changes.

The end of the Second World War was followed by aggressive and competitive armed race during the Cold War between United States of America (USA) and Union of Soviet Socialist Russia (USSR). This competitive struggle to dominate was not only limited to ideological but military, social, economic, philosophical and political challenge and dominance. The aftershocks of this competition had a far reaching effect which shaped the international system and international humanitarian law. The competition of US and Russia to advance their weaponry system and military technology in order to hold sway hegemon over other countries culminated in the most advanced weapons ever to have developed in the history of weaponry and military technological history. Unfortunately, some of these sophisticated weapons such unmanned aerial vehicles, directed-energy weapons, lethal autonomous robots, cyber weapon, defensive systems, electromagnetic weapons are not listed in the current international humanitarian law and therefore the law does not directly addressed specific instruction of how to engage them in a war. Thus, generating a wide range of controversies and debate around these new system of technology.

Technological advancement in military activity provide military advantage but at the expense of changing structure of military and culture of war. This new structure of war have tremendous impact on the existing law of war. It also has the potential to reshape and redesign the law of armed conflict to suit contemporary times. In fact some of these weapons' are autonomous and semi-automatic with limited human control over the system. For instance the Israeli Iron Dome Air Defence missile system(Rafael, 2010) and the MBDA Sea Wolf

seaborne air defence missile system(MBDA, 2018) and the S400 and S300 Russian defence system. On March 1, 2018 in a State of Nation's address, Russian president Vladimir Putin announced a new breakthrough of highly sophisticated weapons which include Sarmat new intercontinental ballistic missile (ICBM), the Kinzhal hypersonic missile, the nuclear-powered cruise missile and the drone submarine that can be armed with both conventional and nuclear charges(RNA, 2018). The defensive weapon systems are used against inter alia hostile missiles, guided and unguided, ranging from relatively slow and early identified rockets guided missiles approaching the protected area at three times the speed of sound(RNA, 2018). For example, if hostile supersonic missiles are fired from close range, the reaction time of a missile defence system such as Iron Dome or Sea Wolf, from first identifying the hostile projectile to launching itself, is measured in a few seconds(Researcharchieve, 2018). No human is able and capable to, and indeed attempts to 'use' Iron Dome or Sea Wolf to shoot down the incoming missile in these circumstances: Iron Dome and Sea Wolf react and act automatically, from identifying the hostile missile, tracking and targeting it, and launching and guiding its own missile against the incoming missile(Researcharchieve,2018). Jooste argues that the human being is limited after vetoing a response to enemy approaching missile in a split of a second of which speed is three times faster that sound (ADBMD, 2009) And the human player after tapping the button does not have control and do not do anything(HRW, 2012). The controversy is that these defense system sometimes are put closer to civilian areas for the reason of defending civilian lives. This raises the question of principle of distinction making it difficult for opponent to comply with the rule. In Gaza incursion in the 2014 for instance rockets were short toward the defence system ***Iron Dome*** which became a military target. In most times it landed towards civilian areas. The fact that this system is not separated from civilians and it used as a combat device no matter the humanitarian intentions, arguably leaves this system without legal backing.

Although Iron Dome was very successfully when Israel used in August 2014 in Gaza in operation. They were able to defend Hamas attack of non-guided rockets, as well as mortars. It is reported that Iron Dome shot down between eighty five to ninety percent of incoming rockets against which it was launched(HRW, 2012). Equally noticeable is in the future despite Iron Dome humanitarian defensive argument the principle of military necessity may apply to specific target be it a military objective or a combatant. AP1 article 52(2) read:

> Insofar as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective

> contribution to military action and whose total or partial destruction, capture or neutralization in the circumstances ruling at the time, offers a definite military advantage.

Out of this difficult of compliance of the principle of military necessity against discriminating or distinguishing the civilian target of location and military target ignite a debate of recodification of some of this principles to include new technology of military strategy and structure of war.

Another critical area is the use of ***Drones***[3]. The evidence in Yamen, Pakistan and Afghanistan in US war against terrorism has left many innocent civilians dead. According to Schmidt *Self-evidently, it would be unlawful to use an autonomous weapon system to directly attack civilians or civilian object(Schmitt, 2012).* In the context of the principle of distinction it is obvious that military unmanned aerial vehicles military such as drones are not natural human combatant who could distinguished between military arsenal, non-combatant such as children, women and injured soldiers. As a result of pressure of the indiscriminate killing of drones US Armed Forces are designing measures and developing plans to manage the transition from manned combat aircraft to unmanned, remotely controlled unmanned aerial vehicles, and on to largely autonomous air vehicles. This indicate that under the complexities of the theater of war which keeps on widening in the face of terrorism the international humanitarians laws is far from fitting into the changing structure of war.

The new technology requires not just different skills, but fundamental shifts in military culture and organization and the laws and principle of armed conflict that govern it. The reduction of actors to combatant and civilians must be improve to include the weapons of enemies. Instead of distinguishing the civilians and combatant only weapons of enemies must also be distinguished and delineated by international humanitarian law to enable proper regulation of war. Schmitt in discussing this salient issue referred to the targeting of a hostile tank or tanks on the battlefield. My argument is that new offensive and defensive system such as Drones, Russia's S300, S400, Sarmat new intercontinental ballistic missile (ICBM), the Kinzhal hypersonic missile, the nuclear-powered cruise missile and the drone submarine and

[3] **Drones** are more formally known as unmanned aerial vehicles (UAV). Essentially, a **drone** is a flying robot. The aircraft may be remotely controlled or can fly autonomously through software-controlled flight plans in their embedded systems working in conjunction with GPS. internetofthingsagenda.techtarget.com/definition/**drone.**

the Israel-US built Iron Dome respectively are critical to law of armed conflict. It is worthwhile to state that all these military weaponry would fail to comply significantly on the principle of proportionality and accountability in the International Humanitarian Law if the law does not consider them in recodification of the law of war as stipulated in the Geneva Conventions. Although Schmidt agree that "because it is clear that autonomous weapon systems may be used in situations in which they are valuable militarily – that is, militarily necessary'', yet he strongly asked for human participation and to control the robot autonomous weapon system.

Humans must rather take charge of managing the autonomous and automatic weapons system since those machines lack the judgment to decipher themselves, how to apply the principle of proportionality and in judging military necessity. Humans must apply the principle; humans canwork with and judge when and how, with what degree of autonomy to apply the robots(Schmitt, 2012). The whole complex structure of war and the difficulty in applying International Humanitarian Law to regulate autonomous and automatic weapons in the form of robots is tacitly and succinctly explain by Sharkey:

> A robot does not have agency, moral or otherwise, and consequently cannot be held accountable for its actions. Moreover, if autonomous robots were used in limited circumstances in the belief that they could operate with discrimination, it would be difficult to decide exactly who was accountable for mishaps. Some would say that the commander who gave the order to send the robot on a mission would be responsible (last point of contact). But that would not be fair since it could be the fault of the person who programmed the mission, the manufacturer who made the robot, or the senior staff or policy makers who decided to deploy it. Or it could be claimed that the device was tampered with or damaged(Sharkey, 2014).

From the above it is obvious that the world system of military strategy keeps on changing and structure of war in that regard is dynamic not static. It is apparent that the international humanitarian law must begin to invest in understanding the whole plethora of world weapons system to be able to deal with the fast changing of warfare in international relation and the future of our world.

Cyber-technology have made it easy and simple to target necessary military areas across the global due to development of computer and internet system. Thus, treaty laws of armed conflict is becoming anachronistic with regards to new technological weapon system. A new form of cyber and media war, and the creation of detentions centers such as Guantanamo and the widening of the war theater and its growing space to include urban warfare and cosmopolitan engagement witnessed in Syria, Iraq, Yemen, and terror attack in US, UK, Turkey and France. The digital revolution has widened the cyberspace and the physical space of war. This has necessitated a new form of growing attempt by states and other actors to intensify the development and usage of some unmanned aerial vehicles, directed-energy weapons, lethal autonomous robots, cyber weapon, defensive systems, and electromagnetic weapons in the recent theater of wars in the global community. It therefore behooves the international community to asked critical questions whether the law of war and its principles must be reviewed to suit to changing times as the structure and mode of warfare changes or must stuck to the simplicity of the exiting international law of armed conflict which stipulates and direct rules of engagement. Taken the former and restructuring, redesigning and recodification of the international humanitarian law will be the best interest in protecting human rights, saving more lives and safeguarding the future of the world.

BIBLIOGRAPHIES

Braden R. Allenby. "Are new technologies undermining the laws of war?" *Bulletin of the Atomic Scientists*, Vol. 70(1) 21–31. 2014.

Collin Wills., *Unmanned Combat Air system in the Future Warfare Gaining Control of the Air. 2015.* Palgrave, Macmillan UK, England.

Dietrich, Schindler, and Toman, Jiri., *The Laws of Armed Conflict*, 3 rd. ed., Martinus Nijhoff Publishers, The Netherlands, (1988). p.VII

DUNANT Henry, *A Memory of Solferino*, ICRC, Geneva, 1986, p, 147 http://www.icrc.org

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2359949.

http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/4414/thesis.pdf?sequence=2

https://www.icrc.org/eng/assets/files/publications/icrc-0739-part-i.pdf.

https://www.loc.gov/rr/frd/Military_Law/pdf/law-war-handbook-2005.pdf.

https://www.loc.gov/rr/frd/Military_Law/pdf/law-war-handbook-2005.pdf

Human Rights Watch Report "Losing Humanity: The Case against Killer Robots" (November 2012) Human Rights Watch

Hun –Yan Liu "Categorization and legality of autonomous and remote weapon systems" ICRCR No 886 (Volume 12, 2012) 628.

MBDA. www.mbda-systems.com/products.

Michael N Schmitt "Autonomous weapon systems: A reply to critics" (2013) Harv Nat'l Sec J 2.

Michael N Schmitt and Jeffrey S Thurner "Out of the Loop: Autonomous weapon Systems and the Law of Armed Conflict" (2012) 4 Harv Nat'l Sec J 213.

Noel E Sharkey "The evitability of autonomous robot warfare" ICRCR No 886 (Volume, 2012)

Noel E Sharkey "The evitability of autonomous robot warfare" ICRCR No 886 (Volume, 2012) 788.

Philippus Jacobus Jooste "Autonomous Weapon Systems In International Humanitarian Law – Simply Just Another Weapon System".2014. LAWS 533. Research paper

William Boothy "Some legal challenges posed by remote attack" ICRCR No 886 (Volume 12, 2012) 579.

William Boothy. *Conflict Law: The Influence of New Weapons Technology, Human Rights and .Emerging Actors. 2014* TMC Asser press .Hague

CYBERSECURITY IN AFRICA: THE THREATS AND CHALLANGES

Alhassan Tahiru[♣]

Abstract

The world we live in today, has become more complex and more connected than ever before, and this growing complexity and interconnectivity is largely made possible by the forces of modern information, communications and transportation technologies. The world has become a global village mainly because of the rapidity in which socio-economic cleavages are getting interconnected, computers as well as other powerful devices and machines have connected people across oceans. Millions of people all over the world have now become "netizens," a new word coined to denote internet inhabitants. The use of ICTs, and the Internet, has undoubtedly become a matter of strategic importance. Africa's socio- economic political development can be attributed to information communication technology and the "internet of things "(IOT).In as much the internet has been a great pivot and an appetitive drive of all aspects of human life and endeavour, it equally comes with its own associated difficulties, challenges and powerful threats not to only national security but human survival at large.

This paper seeks to critically discuss cyber security in Africa and its accompanied challenges and problems. It further discusses the commanding threats cyber insecurity poses to the Africa as a continent. Relevant analysis is made in other to bring to fore the dire consequences the lack of cyber security mechanism subject a country like Africa, and further plausibly explained the need to protect and guide desirously the internet space of Africa since it is exposed to hazards of many kind.

METHODOLOGY

This paper qualitatively assesses relevant documents and frameworks in relation to this field and other important literatures, to develop an appreciable understanding of both the concepts of Cyber Security and accompanied challenges and threats, to provide a more focused analysis and a basis for this piece of work.

INTRODUCTION

♣ MA Student in Peace and Conflict Studies, Department of International Relations, Ankara Social sciences University, alhassantahir212@gmail.com

The first "electronic mail" was sent in 1971.The children of those scientists now live in a world where almost 40 trillion e-mails are sent a year. The first "website" was made in 1991. By 2013, there were over 30 trillion individual web pages (P. W. and Allan 2014).

Between the space of 40 years, there has been unprecedented participation in the information communication technology in every sphere of our lives. Africa as a continent is indisputably showing good signs of becoming a major player in Information Communication Technology. Possibly because of efforts by governments to cooperate with private and foreign companies in providing ICT infrastructures and digital services to citizens.

This indeed has help Africa to catch up with the rest of the globe in terms of connectivity. The expanding internet user base, fast internet access and the lack of effective cyber security or cybercrime laws is however posing a huge threat to the internet and cyber security space of Africa, which to some has made Africa a new cybercrime harbour. Statistics indicate that Africa is very prone to cyber-related threats due to the high number of domains coupled with very weak network and information security.

This paper discusses the digitalisation of Africa infrastructure systems vis-a-vee the challenges and threats the continent is faced with as far the growing base of internet access is concern. It explores to provide information and depict the clearest picture as to where the African continent stands with regards to cyber security.

For the purposes of comprehensibility, the paper is structured in four major areas, the first part looks at digitisation of State Infrastructures in Africa in which the level of infrastructure and internet connectivity is discussed. The second part encapsulates the phenomena of internet penetration and the expanded user base in Africa in its socio economic and political context.
The subsequent part is the thorough analysis of the challenges and threats the continent faces in cyber space and security, taking a trip into the cyber security documents of African countries coupled with "conventions" made at the continental level. The final part of part of this paper elaborated the strategies to combating cybercrime, and the conclusions part is where he relevancy of this piece of work is reasonably established.

The Digitalization of State Infrastructures in Africa

The African continent has witness a big and tremendous achievements in building ICT infrastructures and internet access in a very rapid pace.From less than 5% in 2007, Internet penetration to 28% in 2015.Substaining this trend means the continent will be comparable and up to par with the develop world in digital connectivity.

Today, wherever one looks, there are new digital resources in Africa: online newspapers, issues of scholarly journals, GIS maps, government documents, archives, and networks bringing online book reviews or e- conferencing. There is a proliferation of online distance learning or "virtual university "packages, some based in Africa. Students everywhere, including in Africa, are embracing new online learning models (Limb 2005; UNESCO 2004) Clearly the Internet Of Things(IOT) has changed the lives of many African citizens relying on the internet to perform daily activities such as education, socializing, communicating or even making money transfers through mobile phones.

In 2007, Africa's first undersea fibre-optic cable infrastructure to connect its eastern and southern parts with the rest of the world was established. Most African countries are now to some extent well-connected, cable wise, giving local ISPs the ability to provide cheaper and faster access types to internet. There is wide range of access services throughout the continent, including dial-up, digital subscriber line (DSL), fibre Enhanced Data rates for GSM Evolution (EDGE), 3G, 4G Long-Term Evolution (LTE), and satellite (cybercrime & cyber security trends in Africa, november,2016).

The West Africa Cable System (WACS), An ultra-high-capacity fibre-optic submarine cable system that links South Africa to Europe, spanning the west coast of Africa and terminates in the United Kingdom was equally developed which seeks to serve majority of western part of Africa.

With the above infrastructures in place, networks have expanded, and thousands of people have join the web of internet. The quest of achieving widespread affordable access to ICT in many parts of Africa is still on course and its excepted to achieve a commanding height in no too distance future. Several other infrastructure development projects are also underway in various parts of the continent. Key Sectors of the African economic infrastructures have been digitalize ranging from transport, energy, manufacturing, communications etc.

In terms of transportation, there has been some important growth of that sector. Transport cooperation's have putting in place digital technologies to ensure safe operations of the transport sectors. Using of advanced digital and software technologies has allowed trains to check the state of rail signals and to intervene when driver acts contrary. In effect, this has given the transport systems a human operators ability to analyse and make informed decisions on time and to anticipate conditions ahead.

For example, in south Africa there has been reshaping in the transport sector with the lunched of a state-of the-art Transport Management Centre (TMC), which is the nerve centre for the management of Bus Rapid Transit (BRT) system. The facility is vital in monitor activities along the transport corridor through CCTV cameras – improving quality of transport and prevent acts of crime. (ADMR,2017).

Kenya is leading the way of making customers and passengers pay transportations through a digital channel. Mobile-money(m-pesa) could be used in paying a taxi ride in Nairobi more easier than it is New York. This is becoming increasingly more accessible and convenience in Kenya causing other countries in Africa to follow suits.

The energy sector has received a fairly face lift of digitization. Electricity supply networks use digital communications technologies like GSM (Global System for Mobile Communications) or PLC (Power-Line Communications) to analyse, detect and react to local changes, are increasingly being incorporated into the African power utilities action plans(Deloitte ,2015) Many African countries have also adopted most efficient payments methods for electricity, ranging from mobile money to internet payments. Ghana, South Africa and other African countries for instance have introduced prepaid metering systems to improve revenue management and financial systems of the energy industries. New technologies have been also introduced to turn wind turbines into more reliable and productive energies. Kenya has the largest wind power project in Africa called the Lake Turkana Wind Power(LTWP), this is to power and distribute generated energies to fulfil diverse needs of citizens.

In the manufacturing industry there has been practical realisation of digitisation. Industries in Africa have resorted to the use of smart technologies, smart plants, smart machines and equipment for efficient processing and supply chain enhancements.

This level of smart technologies has accelerated the overall African Manufacturing Industries, an example of this technology is Siemens' Mind Sphere, which serves as the foundation for digital services such as preventative maintenance, energy data management and resource optimization in many African countries, although awareness of the significance and the potential of this exponential technology is still on a very low rate. (African Digitalization Maturity Report,2017).

The telecommunication sector has seen an explosion of access more than ever before. The number of users has grown tremendously throughout the region, low income countries where telecommunications are hardly accessible are now rapidly catching up with countries with improved communications such as Namibia and South Africa. In 1998, at the begging of telecommunications evolutions, south Africa alone accounted for 86 percent of the regions subscribers by 2008 Nigeria over took south Africa and become the region's biggest telecommunications markets. Networks as it were having been concentrating in urban cities more than rural areas in Africa, as in 2009,90 % of Africa's urban population and 48 % of its rural communities are within the catchments of network coverage.

The internet world statistics reports that; By 2020, about three-quarters of all mobile connections will be on 3G or LTE, and thereafter the impetus will favour LTE as operators are able to make use of spectrum released from the switch to digital TV. Overall forecasts suggest that mobile internet traffic across the region will increase 20-fold by the end of the decade and mobile data revenue in Africa is expected to double by 2019.it is indeed true that the information communications technologies, mobile networks, and internet have been a powerful and essential tool for governments, commerce, civil society and individuals in Africa and in the world as a whole.

Internet Penetration in Africa

In Africa currently more than 650 million unique mobile subscribers, more than 30% of the African population are now using the Internet, more than 120 million people are using Facebook and around 9% are general on social media and is growing each year, with South Africans among the world's leaders in time spent on social networks at 3.2 hours per day . Again, more than 80% of Facebook's users in Africa are visiting the site via mobile devices.

The global share of e-commerce for the Middle East and Africa was expected to rise from 1.6% in 2011 to 2.3% by 2016.

Globally 3.2 billion people are using the Internet by end 2015, of which 2 billion are from developing countries. For every Internet user in the developed world there are 2 in the developing world. (ICT Facts & Figures; the world in 2015) By end 2015, 34% of households in developing countries have Internet access, compared with more than 80% in developed countries. These statistics however show the steadily progress of internet penetration in Africa.in a much such penetration cannot be compared to that of developed country, it is important to note that its quite significant growth than before. Most African countries are still yet to realise high internet penetration, due to political instability or infrastructural challenges Below are the list of African countries with highest internet penetration and biggest internet user base.

The 10 countries with the highest Internet penetration rates are:

1. Morocco
2. Tunisia
3. Nigeria
4. Egypt
5. Kenya
6. Mauritius
7. Senegal
8. South Africa
9. Algeria
10. Uganda

The 10 African countries with the biggest Internet user bases are:

1. Nigeria
2. Egypt
3. Morocco
4. Kenya
5. South Africa
6. Tanzania
7. Algeria
8. Sudan
9. Uganda
10. Tunisia

(Source*; Internet World Statistics: Usage and Population Statistics)*

The high user base and huge internet penetration is good news to Africa. But the lack of effective laws and careful cyber security measures to police the internet space exposes users to several risks and vulnerabilities. Criminals and attackers launch malicious activities without any hesitancy or restrictions since they are unlikely to be apprehended nor prosecuted. Though the wider coverage and faster internet facilities benefit the users and businesses in Africa so it equally benefits attackers and criminals of cyber space.

In the subsequent page we will see the huge and wanton sums of monies Africa countries loose to cybercrime of which these resources could be used in the provision of basic amenities to citizens of the content.

The Threats and Challenges of Cyber Security in Africa

The internet of things (IOT)is becoming reality in Africa, adoption of technology in every sphere of lives continue to grow in a very surprising rate, mobile device ownership and social media use is increasing exponentially. This growing technology and digitization however comes with new risks which potentially undermines growth and achievements made in the internet space. The biggest risks confronting the cyber space is the global rise of cybercrime. The continent's Information Communication Technology's infrastructure has become an attractive target for cyber criminals and hackers.

In 2013, the total global direct cost of cybercrime reached an estimated $113 billion USD. In South Africa alone, 67% of adults reported experiencing cybercrime in the last year, which is estimated to have cost the South African economy $242 million USD. On average, cybercrime cost each cybercrime victim in South Africa US $274 per year. (https://us.norton.com/cyber-security-insights-2016)

Many Africans are still using outdated, or in many cases unlicensed, software. In fact, one of the drivers behind the increasing rates of cybercrime in Africa is the widespread use of outdated or unlicensed software programs. African Countries Lost atleast 2 Billion Dollars to Cyberattacks in 2016.According to the Business Software Alliance's annual Global Software Survey reports that approximately 57% of software used in Africa and the Middle East is unlicensed. Nearly one quarter of users in Africa are currently using the operating system, Microsoft Windows XP which was first released in 2001, and for which software patches were discontinued in 2014.

According to Serianu's Cybersecurity Report 2016, African countries lost at least $2 billion in cyber-attacks in 2016.In East Africa, Kenya recorded the highest losses with $171 million lost to cyber criminals. Tanzania lost $85 million while Ugandan companies lost $35 million. Nigeria lost about $550 million in 2016 alone. Ghana lost $50 million through cybercrime

related issues in 2015.Cote d'Ivoire lost $8,779,070 in 2014 and $ 6,636,530 in 2015., this according to Cisco 2017 Annual Cybersecurity Report.

The figures above shows the alarming and colossal amounts of money the African countries lost and continue to lose to cyber criminals. This by far has some great intended consequences to the economic growth and fiscal stability of many African countries. The continent is somewhat permissive to cybercrime due to poor cyber security capabilities, absence of effective and active legislations as well as lack of general awareness of cyber security measures.

As at September 2012, the top 10 African countries with the biggest number of malware-infections include;

1. South Africa
2. Egypt
3. Tunisia
4. Morocco
5. Comoros
6. Senegal
7. Guinea-Bissau
8. Nigeria
9. Ghana
10. Algeria

South Africa Is reported to be the 3rd highest with respect to cybercrime victims in the world with 80%, after Russia (92%) and China (84%).Findings by the International Data Group Connect; estimates that annually, cybercrimes cost the South African economy USD 573 million. Several commercial banks in Zambia were robbed of more than USD 4 million in the first half of 2013 because of sophisticated cybercrime collaborations between Zambians and foreigners. A 2011 Deloitte Touche survey found that financial institutions in Kenya, Rwanda, Uganda, the United Republic of Tanzania and Zambia had registered losses of up to USD 245 million due to cyber fraud. (Slimani,2016).

The State of Cyber Crime Documents and Legislation in Africa

The Protection of confidentiality, integrity and availability of computer data and systems against cyber-attacks is an essential and critical responsibility of all governments, particularly when ICT has become core potential for human and societal development. Governments cannot remain passive. They have the obligation to protect state structures as well as individuals against cyber crime of any kind.In the light of this, governments are expected to

take active, effective and preventive measures to control, minimize if not totally eliminate cybercrime and its related activities from their respective jurisdiction, though such is far reaching. It is through means of Comprehensive legislation and substantive cyber laws that this could be achieved.

A cursory overview of the 54 countries of Africa in terms of specific criminal law provisions on cybercrime and electronic evidence suggests that by April 2016:
11 States seemed to have basic substantive and procedural law provisions in place (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia) although implementing regulations may still be missing in one or the other country.

A further 12 States seemed to have substantive and procedural law provisions partially in place (Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe).

Most of African States (30) did not have specific legal provisions on cybercrime and electronic evidence in force. Draft laws or amendments to existing legislation reportedly had been prepared in at least 15 States (Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe). In some instances, bills had been presented to national parliaments, in others the fate of draft laws is uncertain.

Statistically speaking, 20% of African states have basic legal framework in place.22% have partial legal provisions in place, while 27% have drafts or amendments legislations in place and 31% have no frameworks nor laws in place.

The above statistics is not satisfactory as far as forward match towards combating cybercrime in Africa is concern. This explains the consistent and persistent penetration of cybercrime in the African society, consequently making the continent a haven for cyber criminals. The absence of these laws and practical legislations in majority of African countries only incubate hackers and create fertile grounds for cyber maliciousness to thrive.

Regional and Continental Approach to Cyber Security

African Countries have made attempted efforts to develop a continental and global approach as well as coherent strategy to promote peace and security in the cyber society. Among which include.

1. ***The African Union Convention on Cybersecurity and personal data*** **protection**

This convention seeks to address the legislative challenges and problems African countries are confronted with respect to cyber security, and as well look at the need for Harmonized legislations around Cyber Security and Personal Data Protection in Member States of the African Union. The 23rd African Union Assembly of Heads of State and Government, held in Malabo on 26-27 June 2014 adopted The African Union "Convention *on Cybersecurity and personal data protection"* Which is now known as *The Malabo Convention*.

The Malabo convention calls for the establishment of a Legal Framework for Cyber-security and Personal Data Protection and sets a wide and broad guidelines for subjugation and minimization of cybercrime and its related activities in the continent. It seeks reaffirm commitments of African Union Member States at all levels to build an information society that guarantees a high level of legal and technological security to ensure respect of online privacy and freedoms while enhancing the promotion and development of ICTs in Member States.

2.*Recalling the recommendations of the First Ordinary Session of the STC-CICT-1.*

An Ordinary Session of the Specialized Technical Committee on Communication and Information &Communication Technologies (STC-CICT-1) Was held in Addis Ababa, Ethiopia on August 31ST 31 August to 4 September 2015 to ensure that The African Union Commission follow up of the signing and ratification by Member States of the African Union Convention on Cyber-Security and Personal Data Protection and ; Member states to accelerate the signature and the ratification of the AU Convention, on the development of National Cyber-Security legislations and creation of national and regional Computer Emergency Response Team (CERT) and/or Computer Security Incident Response Team (CSIRT).

These are among others conventions and protocols by the regional body thus Africa Union to engage the attention of African countries to paying attention to the development of measures, policies and strategies to deal with issues of cyber security at regional and continental levels. Even though member states seem to be working on the recommendations but still efforts to win the war on cybercrime in Africa continue to hit a dead end.

CYBER SECURITY AND COMBATING CYBER CRIME IN AFRICA

The threats and risks posed by cybercrime and its related activities threatens the success chopped by Africa as far as the quest to achieve meaningful digitalise heights are concern. Drastic, and calculated measures need to be putting in place in order to nib this teething challenge in the bud minding the fact that significant efforts made.

Cybersecurity and cybercrime cannot be treated as any other rogatory laws particularly when there are clear facts and figures indicating the huge amounts of monies African countries are losing as result of loose measures that has given room and space for cybercrime to thrive. Governments must develop strategies and effective policies to address the emerging security issues associated with the criminal use of the cyber space by way of protecting individual users and critical state infrastructures. Some of these measures needs to be woven into the web of strategies to curtail cybercrime in Africa include.

National Policy

Joint and collaborative measures with stakeholders in cyber industries have the duty to develop a national cyber security policy which recognizes the importance of critical information infrastructures and capable of solving the cyber risks facing the countries as well as outline how objectives of such policies can be achieved.

National Strategy

Adoption of careful and appropriate national strategies towards fighting cybercrime is paramount. African Countries must implement effective national cyber security policy, particularly in the area of legislative reform, development, sensitization and capacity–

building, public -private partnership, and international cooperation among others to achieve the needed results of sanitising the cyber society.

Legislation Against Cybercrime

Effective and efficient legislative and regulatory measures against cybercrime must be enforced by African countries. Clear and substantive criminal offences that affects the confidentiality, integrity, availability and survival of information and communication technology must be encapsulated in legislative instruments.

National Regulatory Authorities

Governments as matter of urgency should confer specific responsibilities on institutions and agencies, either newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them an authority and legal capacity to act in all aspects of cyber security issues, including but not limited to response to cyber security incidents, and coordination and cooperation in the field of forensic investigations, prosecution etc. There should be the promotion of technical education and the education of information and communication technology professionals, within and outside government bodies in the area of cyber security and cybercrime protection.

Harmonization

African countries should develop a collaborative and harmonized efforts towards the fight against cyber-crime. such efforts should be woven towards strengthen the possibility of regional harmonization of these measures and strategy. This by far will protect the region in a very broader perspective rather than individual countries taking approaches which is not connected to the general strategy of the continent.

Conclusions

Albert Einstein was quoted as saying "Problems cannot be solved with the same levelA of awareness that created them." The internet has undoubtedly become a matter of strategic importance. A free, open, save and secure cyber space is an engine for economic growth and social development that facilitates communication, innovation, research and business

transformation. The increase in user base, speed internet penetration coupled weak cyber security measures in Africa presents new herculean threats and challenges to the continent.

Cyber security concerns are broader and to some extend complicated national security issue if not carefully handled by duty bearers can planch stable country into many challenges but yet few cybersecurity initiatives and real strategies have been effectively implemented at both regional and continental level.

A strategy and cybersecurity frameworks based on a common approach and common understanding are needed among Member States of the African Union.

The intent and purpose of this paper is to unearth and bring to bear the state of cyber security and cybercrime in Africa. The challenges and threads that is facing the continent which has cause whooping amount of resources going down into the drain due to lack of or loose measures in place as far the protection and preserving the sanctity of the cyber community is concern.

The paper explained the extent of digitisation of state infrastructure in Africa and the level of internet penetration. It gone further to look at the challenges and threats confronting Africa amid growing internet penetration and a transition to a more technology-based continent. Countries with cyber security documents and approach by the regional body thus the African Union in providing solutions to cybercrime is fairly discussed. Lastly measures and possible solutions towards combating cybercrime is equally catalogued and enumerated. Cyber threats represent global problems and they need global frameworks as instruments to promote security and stability in cyberspace

REFRENCES

AU.(2017).*A global approach on Cybersecurity and Cybercrime in Africa* ; retrieved from; https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf on 15th January 2018.

Dall'Omo, S.(2017). *African Digitalization Maturity Report*, Southern and Eastern Africa.

Deloitte (2015). *Sub-Saharan Africa Power Trends: Power disruption in Africa*.Availableat:https://www2.deloitte.com/content/dam/Deloitte/za/Documents/energy-resources/ZA_AfricaPowerTrendsReport_EnergyResources_200515

ICT Facts & Figures, The World 2015 retrieved from; https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

Kharouni, L.(2013). *Africa A New Safe Harbor for Cybercriminals*? Trend Micro Incorporated Research Paper.

Slimani, M.(2016).*Enhancing Cyber Security in Africa: New challenges for regional Organizations* ?

Symantec.(2017).https://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

Williams, M.D.J., Mayer, R. and Minges, M.(2016). .*Africa's ICT Infrastructure Building on the Mobile Revolution:*

Yedaly, M. and Wright,B(2016).*Cyber Crime & Cyber Security Trends in Africa*.

GÜNCEL SİBER GÜVENLİK TEHDİTLERİ: FİDYE YAZILIMLAR

Soner ÇELİK*

Barış ÇELİKTAŞ**

Özet

Son yıllarda bilgi teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte bilişim sistemlerini tehdit eden zararlı yazılımların çeşitlenerek etkilerinin arttığı düşünülmektedir. Günümüzde fidye yazılımları siber ortamlarda saldırganlar tarafından etkili bir siber saldırı aracı olarak kullanılmaktadır. Fidye yazılımları 2000'li yılların ortalarından günümüze kadar etkisini arttırarak devam eden güçlü bir saldırı yöntemi olarak saldırganlar tarafından kullanılmaktadır. Buradan hareketle son birkaç yılda artış gösteren fidye yazılım saldırıları, geniş güvenlik bütçelerine sahip çok uluslu büyük firmalardan devlet kuruluşlarına, küçük işletmelerden bireylere kadar birçok kesimi etkilemektedir. Fidye yazılımlarının önümüzdeki dönemde tehdit düzeyini ve etkisini arttırarak daha kolay erişim ve daha fazla finansal kazanç sağlama motivasyonlarıyla sayılarının artması beklenmektedir. Fidye yazılımlarındaki şifreleme düzeyi, ticari güvenlik ürünlerinde görülen şifreleme seviyesine hızlı bir şekilde yaklaşmaktadır.

Bu çalışmada, kişileri, kurum ve kuruluşları üst düzeyde tehdit eden fidye yazılımları ele alınmıştır. Fidye saldırılarında kullanılan yöntemler araştırılmış, farklı fidye saldırı tipleri incelenmiş ve bilişim sistemlerine verdiği zararları azaltmayı sağlayacak etkili bir mücadele için çözüm önerileri sunularak fidye yazılımlarına karşı farkındalık oluşturulması amaçlanmıştır.

Anahtar Kelimeler: Siber Tehditler, Siber Güvenlik, Fidye Yazılım, Güvenlik Farkındalığı

Contemporary Cyber threats: Ransomware

Abstract

* Doktora Öğrencisi, Süleyman Demirel Üniversitesi, İİBF-Uluslararası İlişkiler Bölümü, E-posta: sonercelik85@gmail.com

** Doktora Öğrencisi, İstanbul Teknik Üniversitesi, E-posta: celiktas16@itu.edu.tr

In recent years, the development of information technology and information systems with widespread threats, which experienced an increase and diversify the effects of malware is known from cyber-attacks. Nowadays, ransomware is used by cyber attackers as an effective tool for attacking cyberspace. Ransomware has been used by attackers as a powerful attack method that continues to increase from the year 2000 to the day. From here, ransomware attacks that have increased in the last few years have affected many sectors, from large multinational companies with large security budgets, to government agencies, small businesses to individuals. It is expected that the ransomware will increase the threat level and influence in the coming period and increase the numbers with easier access and motivation to provide more financial gain. The level of encryption in ransomware is rapidly approaching the level of encryption seen in commercial security products.

In this study, ransomware which threatens people, institutions and organizations at high level is discussed. It was aimed to raise awareness of ransomware by presenting solution proposals for an effective struggle to investigate the methods used to attack, investigate the different types with the changes they have undergone, and reduce the damage to the information systems.
Keywords: Cyber Threats, Cybersecurity, Ransomware, Security Awareness

GİRİŞ

Günümüz dünyası için fidye kavramı yeni bir olgu değildir. İnsanlık tarihi boyunca fidye, eski Roma'dan korsanlığa ve günümüz rehine alma olaylarına kadar saldırganların kullandığı yaygın bir taktik olmuştur. Bugün ise saldırganlar bu taktiği siber dünyada uygulamaya başlamıştır. Saldırganlar, sistemleri güvence altına almak amacıyla keşfedilen şifreleme teknolojilerini kullanarak kendileri için kazanç sağlamak için son derece etkili ve kolay bir şekilde fidye yazılım saldırılarını kullanabilmektedir.

Bu tehlikeli yazılımlar reklamlar, bilgilendirme mailleri ve sosyal mühendislik saldırıları gibi çeşitli yöntemlerle kullanıcıların bilgisayarlarına kolayca bulaşabilmektedir. Fidye yazılımlar, bulaştığı sistemlerdeki dosyaları çözülmesi zor olan şifreleme algoritmaları ile şifreleyerek özel anahtarlar üretmekte ve bu anahtarlar özel bir sunucuda ayrı olarak tutulmaktadır. (Luo, X. , Liao, Q., 2007, s. 197).

Ayrıca şifreleme işleminin yanı sıra, fidye yazılımın yerleştiği bilgisayarın kayıt defterine girilen kod ile bilgisayar her açıldığında zararlı yazılımın çalışması sağlanmaktadır. Netice olarak kullanıcı, saldırganın istemiş olduğu ücreti ödeme yapmadığı durumda sahip olduğu sistemdeki elektronik verileri kaybetmesi veya erişememesi ile tehdit edilmektedir. Mağdur, talep edilen ücreti saldırganın belirlediği sınırlı bir süre içinde ödeme yapması için uyarı ekranı ile Bitcoin, MoneyPack, Ucash ve Kashu gibi günümüz sanal para ödeme sistemlerine yönlendirilmektedir. Saldırganlar ayrıca ek bir tedbir olarak veriyi kurtarma girişimlerini engellemek için mağdurun kendisinin denediği her hatalı şifre anahtarı girişinde verilen bu süreyi azaltılmaktadır. Ödeme yapılıp teyit alındığında saldırganlar dosyaların şifresini açacak anahtarı iletmekte; aksi durumda elektronik veriler erişilemez olmakta veya kaybedilmektedir. (Uitsec Teknoloji, 2014, s. 3).

Fidye yazılımlar 2010 yılı itibarı ile siber dünyada saldırganlar için ciddi bir gelir kaynağı haline gelmiş ve zararlı fidye yazılım türevlerinin gün geçtikçe artmasına neden olmuştur. Birçok anti-virüs firması tarafından yayınlanan raporlarda, fidye yazılımlarının geçmiş yıllara göre 2017 sonunda 3 kattan fazla bir artış göstermektedir. Son dönemlerde gerçekleşen saldırılardaki saldırı vektörleri ve motivasyonları dikkate alındığında, fidye yazılım saldırılarında kullanılan teknolojiler ve araçlar çok gelişmiş, saldırı şiddeti ve hacmi artmış, saldırı hedeflerinde stratejik öneme sahip kamu kurum ve kuruluşları, çeşitli altyapılar, hastaneler, üniversiteler ve büyük ölçekli firmalar bulunmaktadır. (J.Crowe, 2017, s. 2).

2017 yılında Barkly firması tarafından yayınlanan istatistiklere göre, şirketler ortalama 40 saniye de bir fidye yazılım saldırısına uğramakta ve her 10 zararlı

yazılımdan 6 adedi fidye zararlısı olarak karşımıza çıkmaktadır. Ayrıca hedeflenen şirketlerin %71'ine fidye zararlısı bulaştırılmıştır. İstenen fidye tutarı yaklaşık olarak 1,077 dolara yükselmiştir. Saldırganlar tarafından talep edilen ödemeyi yapan 5 şirketten 1'sine dosyalarına erişim hakkı verilmemiştir. Bu şirketlerin %72'si sahip olduğu verilere ortalama 2 gün ve üzeri süreyle erişim sağlayamamıştır. Netice olarak küresel anlamda fidye yazılımların tahmini zararı **5 milyar dolar** olacağı tahmin edilmektedir. (Barkly, 2018, s. 4).

Kişilere ve kurumlara farkında olmadan büyük zararlar veren ve yakın tarihlerde gerçekleşen fidye yazılım saldırıları incelendiğinde, netice olarak bu saldırılara karşı yeterli önlemlerin alınmadığı ortaya çıkmaktadır. Bu makalede fidye yazılımlara karşı kesin bir korunma sağlanamasa da bu tür yazılımlara karşı daha etkili bir mücadele için yapılması gerekenler açıklanmaya çalışılmıştır. Yapılan incelemede, fidye yazılımların başlangıcından itibaren günümüze dek geçirdiği evrim ve gelecekte nasıl bir hal alacağı değerlendirilerek alınabilecek muhtemel tedbirler önerilmiştir.

FİDYE YAZILIM (RANSOMWARE)

Fidye yazılım, siber suçlular tarafından mobil telefonlar, bilgisayarlar ve diğer bağlantılı cihazlar üzerindeki elektronik verileri fidye için elinde tutup, bu dosyalara yeniden erişim için para talep ettikleri her türlü zararlı yazılımlardır. Basitçe ifade etmek gerekirse, fidye yazılım, bilgisayar sistemlerine veya dosyalara erişimi kısıtlayan ve veri sahibine geri yüklenen erişim karşılığında fidye ödemekle yükümlü kılan zararlı yazılımlardır. Yakın geçmişte yaygın olarak kullanılan fidye yazılım örnekleri arasında CryptoLocker ve WannaCry yer almaktadır. (https://renew.stratus.com.tr/cryptolocker/index.html, 2018).

Bu saldırılardan WannaCry incelendiğinde günümüzde gerek devletlerin gerekse de bireyler ve özel şirketlerin siber uzay kaynaklı tehditler ile doğrudan karşı karşıya kalabildikleri açıkça görülmektedir. Eşi görülmemiş

büyüklükte bir fidye yazılımı saldırısı olan "WannaCry", tüm dünyadaki organizasyonları ve bireysel kullanıcıları etkileyebilmeyi başarmıştır (Darıcılı, Siber Uzay ve Siber Güvenlik Nedir?, 2017, s. 233).

Fidye yazılımlar (ransomware), isminden de anlaşılacağı gibi, bulaştırıldıkları sistemlerde kullanıcıya bir ekran uyarısı görüntüleyerek, kullanıcı dosyalarını şifrelediklerini ve kısıtladıkları sistem erişiminin yeniden açılması için fidye ödenmesi gerektiğini belirtmektedirler. Bir zamana kadar fidye yazılımlara yapılan ödeme, geleneksel para birimlerinin doğal olarak izlenebilir nitelikte olması nedeniyle fidye yazılımların oluşturulmasında sorumlu kişi veya gruplar için önemli bir problem olmuştur. Fakat Bitcoin vb. ödeme sistemlerinin ortaya çıkışı ile ödeme talebinin bu sistemler üzerinden gerçekleşmesiyle siber savunma ekipleri ve kolluk kuvvetleri tarafından saldırganların tespiti zorlaşmıştır.

Ayrıca fidye yazılımlarının dünya genelinde yılın en önemli siber tehdidi olmaya devam ettiği; özellikle finans, sağlık ve telekomünikasyon kurumlarına yönelik fidye yazılım saldırılarının artış gösterdiğini tespit edilmiştir. Bu durumu daha da vahim hale getiren hususun, bazı fidye yazılımlarının kaynak kodunun temel yazılım bilgisi ile ele geçirilebilir olması ve Bitcoin kullanımının yardımı ile organize saldırıların kolaylaştırılması olarak gösterilmektedir. Bu konuda dikkat çekici bir nokta da fidye yazılımlarıyla ilgili Amerikan Federal Araştırma Bürosu (FBI) tarafından yapılan çarpıcı tespitlerdir. FBI'a göre Amerika Birleşik Devletleri (ABD) şirketleri geçen yıl içerisinde 25 milyon dolar fidye ödemiş durumdadır ve 2016 sonunda bu rakamın 200 milyon dolardan fazla olmasını bekleyen FBI, fidye yazılımlarıyla baş etmek için herkese 'İnternette güvenliğe dikkat' çağrısı yapmaktadır. (Hallam-Baker, 2016, s. 2).

Günümüzde fidye yazılımlar iki tür olarak karşımıza çıkmaktadır. Birincisi **(locker-ransomware)** kilitleyicilerdir. Bu tip fidye yazılımlar genellikle bilgisayarın veya aygıtın kilitlenmesi ve daha sonra kullanıcının ona erişimi sağlamak için bir ücret ödemesini istemektedir. Kilitlenen bilgisayarlar

kısmen, yalnızca kullanıcının fidye yazılımı ile etkileşime girmesine ve fidye ödemelerine izin vereceği şekilde açık bırakmaktadır. (Fasheem, 2017, s. 52).

İkinci tür ise, kurbanın kişisel dosyalarını şifreleyerek dosyalara erişilmesini engelleyen (**crypto-ransomware)** şifreleyicilerdir. Bu tür fidye yazılımlar, bilgisayarda depolanan değerli verileri bulmak ve şifrelemek için tasarlanmıştır. Mağdur şifre çözme anahtarı almadıkça şifrelenen verilere ulaşamamaktadır. Her iki durumda da mağdur fidye ücreti ödemeye zorlanmaktadır. Dolayısıyla saldırıya uğramış elektronik verilere fidye ödenene veya şifre çözme anahtarı sağlanıncaya kadar erişilememektedir. (Fasheem, 2017, s. 52).

Bunlara ilave olarak bu zamana kadar Windows tabanlı sistemlere yönelik çıkan fidye yazılımları çoğunlukla son kullanıcıları hedef almıştır. Fakat günümüzde fidye yazılımları artık son kullanıcıları hedef almaktan çok kurum ve kuruluşları da hedef almaya başlamıştır. Çünkü kurum ve kuruluşların kaybedecekleri veriler veya kilitlenecek sistemleri, son kullanıcılara göre daha kritik olduğu için saldırıya uğrayan kurum ve kuruluşun imajı ve itibarı zedelenecek; netice olarak toplum önünde güvenilirliği kaybolacaktır. Bu nedenle kurumların istenen fidyeyi ödemesi son kullanıcılara göre daha muhtemel olmaktadır. Bunun ilk örneği olarak, 2015 yılında ortaya çıkan ve web sunucularını hedef alan ilk linux ransomware yazılımı (Trojan.Ransom. Linux.Cryptor) görülebilir. Bu zararlı yazılım sonucunda 2000 adet web sayfası zarar görmüştür. (Kaspersky Security Bulletin, 2015, s. 4) Siber saldırganların başarılı bir fidye yazılımı saldırısı gerçekleştirmek için uyguladıkları genel yöntemler asgari olarak aşağıda belirtilen aşamaları içermektedir;

1. **Bir sistemin veya cihazın kontrolünün ele geçirilmesi:** Bu adım saldırganlar tarafından tek bir bilgisayar, cep telefonu veya yazılımı çalıştırabilen başka bir sistemin kontrol altına alınması şeklinde olabilmektedir. Çoğu fidye yazılımı saldırısı, kullanıcıları web tarayıcısında bir ek açma veya kötü amaçlı bir bağlantı izlemesi için kandırmak için sosyal mühendisliği kullanan saldırı vektörü ile başlamaktadır. Netice olarak

saldırganın ilk amacı bir sisteme kötü amaçlı yazılım yükleyip kullanıcıyı kontrol altına almaktır.

2. **Kullanıcının sistemdeki elektronik verilerine erişmesini önlenmesi:** Saldırganın bu adımdaki işlemi şifreleme, kilitleme ekranları veya basit korkutucu taktikler yoluyla olabilmektedir.

3. **Veri sahibine fidye için ödenmesi gereken miktarı ve ödeme metodunun bildirilmesi:** Bu aşama kısmen belli olabiliyor olsa da saldırganların ve kurbanların çoğu zaman farklı diller konuştukları, dünyanın farklı yerlerinde yaşadıkları ve çok farklı teknik yeteneklere sahip oldukları unutulmamalıdır. Ayrıca farklı ödeme yöntemleri geliştirilmiş olup kullanıcının bu ödeme metotları hakkında bilgi sahibi olmadığı düşünülerek ayrıntılı açıklama yapılmalıdır.

4. **Veri sahibi tarafından yapılan ödemenin kabul edilmesi ve teyidi:** Saldırganlar, kullanıcının veriyi kurtarma girişimlerini engellemek için belirli bir ödeme süresi vermekte ve bu süre mağdurun veriyi kurtarmak için denediği her hatalı şifre girişinde azaltılmaktadır. Ödeme yapılıp teyit alındığında program, dosyaların şifresini açmakta; aksi durumda elektronik veriler erişilemez olmakta ve kaybedilmektedir.

5. **Ödeme alındığında veri sahibine tam erişim verilmesi:** Saldır ödemeleri kabul ederek ve cihazlara erişimi iade etmeyerek kısa sürede başarabilir, ancak zamanla bu da planın etkililiğini yok edecektir. Değerli eşyalarının iade edileceğine inanmadıklarında fidye ödemezsiniz.

Saldırganlar yukarıda belirtilen aşamalardan herhangi birinde başarısız olması halinde fidye yazılımı saldırısı nihai amacına ulaşamamaktadır. Fidye yazılımlar kavramı onlarca yıldır var olmakla birlikte, güvenilir şifreleme ve şifre çözme gibi aşamalar içeren saldırı adımlarını tamamlayabilmek için geniş bir ölçekte gerekli olan teknoloji ve teknikler sadece birkaç yıl öncesine kadar mevcut olmamıştır. Ancak günümüze baktığımızda, 2017 yılında en önemli güvenlik tehditlerinden biri fidye yazılım saldırı türüdür. Yukarıda saldırı aşamaları anlatılan bu tehdit türünün geçmişten günümüze geçirdiği evrimsel değişimi incelemenin alınacak önlemler ve öneriler açısından faydalı olacağı değerlendirilmektedir. (Trendlabs, 2018, s. 2).

FİDYE YAZILIM SALDIRILARI GEÇMİŞTE NASILDI?

1989: AIDS Truva Atı

Bugün yeni yeni tanımaya başladığımız bu bilgi güvenliği tehdidinin ortaya çıkışı, yani **ilk yaygın olarak bilinen fidye yazılım saldırısı** olayı yaklaşık 30 yıl önce gerçekleşmişti. 1989'da Harvard akademisyeni Joseph L Popp, Dünya Sağlık Örgütü'nün AIDS konulu konferansına katılıyordu. Konferansa hazırlanırken, delegelere göndermek için "AIDS Hakkında Bilgilendirme" başlıklı 20.000 disk hazırlamıştı.

Fidye yazılım saldırısı kapsamında Dr. Popp tarafından kullanılan taktikler, o gün koşullarında oldukça karmaşık gözükmekteydi ama en önemlisi, siber suçluların bugünün kripto fidyeciliğine dönüşmesi için öğrenecekleri ve tanımlayacakları çeşitli tasarım kusurları içermekteydi. Popp'un ilk sosyal mühendislik saldırısı zekiceydi, popüler ilgi çekici bir kültürel konuyu saldırı aracı olarak kullanmıştı. Bununla birlikte, AIDS, arka planda, AUTOEXEC.BAT başlatma komutunu kötü niyetli talimatlarla değiştiriyordu. Kurbanın ana bilgisayarının önyüklemesi ile fidye bildirimi kullanıcının ekranına sunularak tüm dosya dizinleri ve dosya adları, özel bir şifreleme algoritmasıyla şifrelenmişti. Ekranda, Panama'daki bir posta ofisine 189 dolar gönderdikten sonra sisteminin normal haline geri döneceğini bildiren bir mesaj gösterilmişti.

Dr. Popp'un yaratıcılığı zamanının ötesindeydi ve başka birisinin fidye yazılım fikrini benimsemesine ve internet çağında kullanmasına kadar 16 yıl geçti. Dr. Popp gerçekleştirdiği bu olay sebebiyle tutuklandı ancak zihinsel sağlığının kötü olması nedeniyle yargılaması yapılamamıştır. Ayrıca o tarihlerde bu tür olaylarla ilgili yeterli yasal düzenlemeler yapılmamıştı. Ancak Dr. Popp gerçekleştirmiş olduğu fidye yazılımdan kazandığı geliri AIDS araştırmalara destek olarak vermeye söz vermişti. (https://www.techrepublic.com/blog/it-security/ransomware-extortion-via-the-internet/, 2018).

2005-2008: GPCoder

Yeni fidye yazılımı örnekleri ortaya çıktığında, Dr. Joseph L Popp çoktan unutulmuştu ve bilgi dünyası internete dönüştürülmüştü. Tüm avantajlarıyla **internet ortamı**, her türden kötücül yazılımın siber saldırganlar tarafından daha kolay dağıtılmasını sağlamış ve devam eden yıllarda saldırganların Dr. Popp tarafından kullanılanlardan çok daha güçlü şifreleme yöntemleri geliştirmelerine izin vermiştir.

Çevrimiçi dağıtılan fidye yazılım ürününün ilk örneklerinden biri de GPCoder Truva Atıydı. İlk kez 2005 yılında tespit edilen GPCoder, Windows sistemlerine bulaştı ve çeşitli uzantılara sahip dosyaları hedef aldı. Bulduktan sonra, dosyaları şifrelenmiş biçimde kopyalıyordu ve orijinallerini sistemden siliyordu. Yeni şifreli dosyalar okunamıyordu ve güçlü RSA-1024 şifreleme yönteminin kullanılması, dosyaların kilidini açmak için yapılan girişimlerin başarılı olamayacağı konusunda garanti veriyordu. Kullanıcıların ana ekranında, fidyenin nasıl ödeneceği ve etkilenen dosyaların kilidinin nasıl açılacağına dair ayrıntıları içeren bir .txt dosyasına kullanıcıları yönlendiren bir ileti görüntüleniyordu. 2008 yılının ortalarıyla beraber, Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip ve MayArchive gibi Truva atları, daha karmaşık RSA şifreleme şemalarını daha da artan anahtar uzunlukları ile beraber kullanmaya başlamıştır. (http://www.securityfocus.com/news/11523, 2018).

2009-2011: Nakit ödeme-Vundo

Değişimin ilk belirtileri 2009 yılında ortaya çıkmaya başladı. Bu tarihte bilinen bir 'korku'(scareware) zararlısı olan Vundo taktik değiştirdi ve fidye yazılımı olarak işlev görmeye başladı. Daha önce, Vundo bilgisayar sistemlerine bulaşıyor ve daha sonra kendi güvenlik alarmını çalıştırarak kullanıcıları sahte bir şekilde düzeltmeye yöneltiyordu. Bununla birlikte, 2009 yılında analistler, Vundo'nun kurbanların bilgisayarlarındaki dosyaları şifrelemeye başladığını ve bunları çözmek için gerçek bir anahtar sattığını fark etti. Bu, **saldırganların fidye yazılımlarından para kazanabileceklerini hissettikleri ilk olaydı**. Anonim çevrimiçi ödeme platformlarının yaygınlaşması sayesinde, kitlesel boyutta fidye alımı da

kolaylaşıyordu. Ek olarak, fidye yazılımının kendisi de giderek daha karmaşık bir hal almaktaydı. (Symantec Labs, 2009, s. 4).

2011 yılına gelindiğinde, yılın ilk çeyreğinde, 60,000 yeni fidye yazılım saldırısı tespit edildi. 2012 yılının ilk çeyreğine kadar, bu sayı 200.000'e yükseldi. Symantec'in araştırmacıları 2012 yılının sonunda, fidye yazılım karaborsasının **5 milyon dolar** değerinde olduğunu ve bunun gelecekte artacağını tahmin ediyordu. (https://www.cnet.com/news/ransomware-a-growing-menace-says-symantec/, 2018).

2011: Truva Atı WinLock

2011'de yeni bir fidye yazılım formatı ortaya çıktı. **WinLock Truva Atı, 'Kilitleyici' fidye yazılım türünde bilinen ilk yaygın zararlı** olarak düşünülmektedir. Kurbanın cihazındaki dosyaları şifrelemek yerine kilitleyici fidye yazılım türü, cihaza girişi imkânsız hale getirerek kullanıcının erişimini kısıtlamaktaydı. (Security Response, 2017, s. 4).

WinLock Truva Atı, eski taktiklerinde olduğu gibi orijinal ürünleri taklit eden bir fidye yazılım trendi başlattı. Windows sistemlerini etkilemek için Windows Ürün Etkinleştirme sistemini kopyaladı ve bir etkinleştirme anahtarı satın alana kadar kullanıcıları kilitledi. Saldırıya biraz masumiyet eklemek için, sahte etkinleştirme ekranında görüntülenen mesaj, aslında kurbanlara Windows hesaplarının dolandırıcılık yüzünden yeniden etkinleştirilmesi gerektiğini söyledi. Ayrıca kullanıcıların makinelerinin kilitlerini açabilmeleri sağlayacak bir kodu vermek için kullanıcılardan bir SMS (yaklaşık 10 dolar civarında tutan) göndermelerini istiyordu. Bu dolandırıcılık faaliyeti, Rusya ve çevre ülkelerdeki pek çok kullanıcıyı etkilemiştir. Raporlara göre grup bu saldırılardan toplamda **16 milyon dolardan** fazla para kazanmıştır. (https://www.pcworld.com/article/204577/article.html, 2018).

2012: Reveton ve 'Polis' Fidye Yazılımı

Yazılım ürünlerini taklit ederek sahte lisans ücretleri ile kurbanları kandırmak konusundaki değişim, sözde "polis" fidye yazılımlarının ortaya çıkması ile

başladı. 2012'de **Reveton** olarak bilinen büyük bir fidye yazılımı yayılmaya başladı. Dosya bir kolluk kuvveti ajansından bilgisayarın lisanssız yazılım veya çocuk pornosu gibi illegal aktiviteler için kullanıldığını iddia eden bir uyarı göstermekteydi. Bu davranışından ötürü, genelde **"Polis Truva atı"** olarak da anılmaktadır. (http://www.thejournal.ie/gardai-garda-police-trojan-scam-virus-logo-locking-488837-Jun2012/, 2018).

Başlangıçta Avrupa'da yayılmış olan Reveton, ABD'de de görünmeye başlayacak kadar yaygınlaştı ve kurbanlara FBI tarafından gözetim altında tutulduklarını ve cihazlarının kilidini açmak için 200 $ ceza ödemelerine karar verildiğini söyledi. Uyarı, sistemlerinin kilidini çözebilmek için, Ukash veya Paysafecard gibi anonim nakit hizmetleri kullanarak bir ücret ödemeleri gerektiğini söylemekteydi. Bilgisayarın bir kolluk kuvveti tarafından takip edildiği hissini oluşturmak için, ekranda bilgisayarın IP adresini ve kurbanın takip edildiği hissini vermek için kurbanın webcaminden bir kamera görüntüsü göstermekteydi. (https://www.techworld.com/news/security/ransom-trojans-spreading-beyond-russian-heartland-3343528/, 2018).

2013: CryptoLocker

2013 yılının ikinci yarısında, siber güvenlik mücadelesine yeni bir yaklaşım getiren şifreleme fidye yazılımının farklı türü ortaya çıktı. Şifreleme fidye yazılımlar, 2013 sonlarına doğru fidyeyi Bitcoin platformunu kullanarak toplayan CryptoLocker'ın yaygınlaşması ile tekrar yaygın hale gelmiştir. 2048-bit RSA anahtar çifti üreten ve bunu bir komuta-kontrol sunucusuna gönderen ve dosyaları belirli dosya uzantılarından oluşan bir beyaz liste kullanarak şifreleyen ve "**CryptoLocker**" olarak bilinen bir truva atı ile Eylül 2013'de tekrar ortaya çıkmıştır. (https://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware, 2018).

CryptoLocker, 2 Haziran 2014'de US Adalet Bakanlığı tarafından resmen ilan edildiği üzere, Gameover ZeuS botnetinin ele geçirilmesi ile durdurulmuştu. Adalet Bakanlığı, botnetin yöneticisi olduğu gerekçesi ile Rus

hacker Evgeniy Bogachev hakkında iddianame düzenlenmişti. Cryptolocker 234.000'den fazla bilgisayara bulaşmıştı ve bunların yaklaşık yarısı ABD'de bulunmaktaydı. Bir tahmin, Cryptolocker'ın ortaya çıkmasından bu yana ilk iki ayda fidye ödemelerinin **27 milyon dolardan** fazla yapıldığını göstermekteydi. (https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware, 2018).

Cryptowall

Windows işletim sistemini hedef alan bir başka büyük fidye virüsü olan CryptoWall, ilk olarak 2014'de görülmüştür. CryptoLocker, Gameover Zeus botneti ele geçirildiğinde 2014'te büyük oranda durduruldu, ancak o zamana kadar onun yerini almak için hazır olan birçok taklitçi oluşmuştu. Bunlardan biri olan CryptoWall, Tor ağı ekranının arkasında üretilen ve kimlik avı dolandırıcılıkları yoluyla dağıtılan aynı RSA genel-özel anahtar şifrelemesini çalıştıran en dikkat çekici yazılımdı. Bir CryptoWall türü, birkaç büyük web sitesini hedef alan ve 2014 Eylül sonlarında Zedo reklam ağında yapılan bir kötücül reklam kampanyası parçası olarak dağıtılmıştır; reklamlar dosyayı indirmek için tarayıcı eklenti istismarlarını kullanan sahte web sitelerine yönlendirme yapmaktadır. Dosyaları şifrelerken, kötü amaçlı yazılım gölge kopya servisi bilgilerini de silmekte bunun yanında parolaları ve Bitcoin cüzdanlarını çalan bir casus yazılım yüklemekteydi. (http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/, 2018).

CryptoWall ayrıca Bitcoin'in fidye saldırılarında oynadığı rolün arttığını da doğruladı. 2014 yılına kadar, kripto para birimi tercih edilen ödeme yöntemiydi. Ön ödemeli elektronik krediler anonimdi ancak aklama yapmadan nakit çıkışı yapmak zordu; oysa Bitcoin ticaret yapmak ve doğrudan işlem yapmak için normal para birimi gibi çevrimiçi olarak kullanılabilirdi. 2015'e gelindiğinde, **CryptoWall'un tek başına 325 milyon dolar** kazandığı tahmin ediliyordu. (https://terramedusa.com/dosyalari-sifreleyip-bitcoin-isteyen-zararli-yazilim-325-milyon-dolar-kazandirdi/, 2018).

2016: Locky ve KeRanger

Agresif kimlik avı tabanlı dağıtımıyla **Locky**, dağıtım hızı ve ölçeği açısından kendisini takip eden WannaCry gibilerine bir emsal oluşturdu. Doruk noktasına geldiğinde, günde 100.000 yeni sisteme bulaştığı bildirilmişti, gün geçtikçe daha fazla suçluyu dağıtımına teşvik etmek için ilk kez Android araç kitleri tarafından kullanılan franchise sistemini kullandı. Aynı zamanda, sağlık hizmeti sağlayıcılarını hedef alarak WannaCry saldırısının habercisi oldu; yazılımın yaratıcıları, önemli kamu servislerinin, sistemlerini yeniden çalışır hale geitrmek için fidyeleri çok daha hızlı ödediklerini anlamıştı. (Palmer, 2017, s. 2).

2016, ayrıca Mac sistemlerini etkileyen ilk fidye yazılımların ortaya çıktığı yıldı. **KeRanger,** Time Machine yedeklemelerini ve diğer Mac dosyalarını şifrelediği için özellikle yıkıcı bir yazılımdı. Time Machine, Mac'lerde bir sorun oluştuğunda önceki sürümlere geri dönme yeteneği sağlıyordu. KeRanger'dan kısa bir süre sonra birden fazla işletim sistemine bulaşabilen ilk fidye yazılımı ortaya çıktı. JavaScript'te programlanan Ransom32, teoride Windows, Mac veya Linux'ta çalışan tüm cihazları etkileyebilirdi. (Wikipedia, 2016).

2017: WannaCry ve Diğerleri

2016 yılındaki fidye yazılım saldırılarının ölçeği ve karmaşıklığı göz önüne alındığında çoğu siber güvenlik uzmanı, en büyük fidye yazılım saldırılarının ve veri ihlallerinin yer alacağı gerçek bir küresel olay gerçekleşeceğine kısa bir zaman kaldığına inanıyordu. WannaCry bu endişelerin yersiz olmadığını doğrulamıştır.

12 Mayıs 2017'de, dünya tarafından tanınacak olan bir fidye yazılım olan WannaCry'ın ilk kurbanları İspanya'da ortaya çıkmıştır. Fidye zararlısı kısa bir süre için farklı ülkelerde farklı şehirlerde yüzlerce bilgisayara ulaşmıştır. Aradan zaman geçtikçe etki alanı genişlemiş ve **WannaCry kendisini bu tarihe kadarki en büyük fidye saldırısı** olarak kaydettirmiştir.

WannaCry fidye zararlısını bu kadar etkili kılan ve insanları şok eden şey bu kadar nasıl hızlı yayılabildiğidir. Herhangi bri botnet ya da indirmenin yapılacağı bir web sitesi bulunmamaktaydı. Bunun yerine, WannaCry zararlısı bilgisayarların bilinen güvenlik açıklarını hedef alan yeni yöntemine imza atmıştır. Bir ağdaki bir bilgisayara bulaştıktan sonra, aynı güvenlik zafiyetine sahip olan bilgisayarları hızlı bir şekilde bulup kendini otomatik olarak enfekte etmekteydi. WannaCry'ın aynı zamanda çok fazla popüler olması ve gündemde kalmasının basit ama temel nedeni de bu olmuştur. Dahası "WannaCry" fidye yazılımı küresel ölçekte en çok sağlık, üretim, enerji (petrol ve gaz), teknoloji, gıda ve içecek, eğitim, kamu, medya ve iletişim sektörlerinde olumuz etkisini hissettirerek, büyük çapta maddi zarara neden olabilmiştir (Darıcılı, Siber Uzay ve Siber Güvenlik Nedir?, 2017, s. 233).

Bunun yanında birçok güvenlik uzmanını şok eden asıl olay, WannaCry'ın Windows'ta kullandığı güvenlik zafiyetinin yıllar önce ABD Ulusal Güvenlik Ajansı (NSA) tarafından tespit edilmiş olduğu gerçeğiydi. Fakat tüm dünyayı böyle bir zararlı hakkında uyarmak yerine, NSA sessiz kalmış ve bu zafiyeti bir siber silah olarak kullanmak için kendi istismar kodunu geliştirmeyi tercih etmiştir. Saldırı, Europol tarafından eşi benzeri görülmemiş şekilde tarif edilmiştir. (http://www.bbc.com/news/world-europe-39907965, 2018).

WannaCry'ın hemen arkasından gerçekleşen başka bir uluslararası fidye yazılım saldırısı, dünyanın dört bir köşesinde binlerce bilgisayarı hedef almıştır. **Petya** olarak bilinen bu saldırıda en dikkat çekici olan şey, WannaCry tarafından kullanılan aynı Windows güvenlik zafiyetinin kullanması ve NSA'nın planladığı ve geliştirdiği bir yazılımın ne kadar güçlü olabileceğini göstermiştir. Ayrıca, WannaCry saldırısının ardından çeşitli ortamlardan duyurulan ve yaygın olarak kullanılmaya başlanan bir yamaya rağmen kullanıcıların sürekli olarak güvenlik güncelleştirmeleri etkinleştirmelerinin ne kadar zor olduğunu göstermiştir.

FİDYE YAZILIMLARA KARŞI ETKİLİ MÜCADELE

Pratikte bilinen anti virüs yazılımları ve sandbox çözümleri yeni nesil zararlılara karşı büyük oranda başarısız olmaktadır. Bu durumun en büyük nedeni ise dijital imzalarını sürekli değiştirme yeteneğine sahip yeni nesil zararlıların artık imza tabanlı ve statik analizler ile tanınamamasıdır. Fidye yazılım geliştiricisi kötü niyetli saldırganlar, geliştirdikleri yöntemler ile sezgisel ve davranış tabanlı otomatik analiz mekanizmalarını kolaylıkla atlatabilmektedir. Bazı durumlarda ise bu teknolojilerin yeni zararlıları keşfetmede geç kalabildikleri görülmektedir. Önceki bölümlerde anlatıldığı gibi fidye yazılım saldırılarının mevcut durumuna nasıl dönüştüğünü anlamak, siber suçluların neden bazı taktik veya yöntemler kullanıp kullanamayacağını ve onlara karşı nasıl savunacağımızı daha iyi anlamamızı sağlamaktadır.

1. Yedekleme ve Veri Kurtarma

Fidye yazılım saldırılarına karşı en iyi savunmalardan biri yedekleme ve veri kurtarma işlemlerinizdir. Şifrelenmiş dosyalarınızı yedeklerinizden kurtarabiliyorsanız, organizasyonunuz üzerinde çok az veya hiç etkileri olmayan başarılı bir fidye saldırısını zararsız bir şekilde atlatmışsınız demektir. Yedeklemeler zararlı yazılımın erişemeyeceği bir yerde tutulmalıdır. Saldırganların, değerli dosyaların şifrelenmesi çabalarının bir parçası olarak yedeklemeleri hedefledikleri bilinmektedir. Ancak bir eksilik olarak dosyaların **yedekten kurtarma sürecinin test edilmesi**, yedekleme kadar önemli bir faaliyet olarak karşımıza çıkmaktadır. Kurtarma işleminizi hiç test etmediyseniz, yedeklemelerinizin düşündüğünüz kadar güvenli olmadığını fark edebilirsiniz.

Yedeği alınacak kritik sistemlerin **yedekleme politika ve prosedürlerini** (back-up policy) yazılı olarak hazırlanmalıdır. Sistemin kullanım dışı kalması durumunda, sistem herhangi bir veri kaybına uğramadan yeniden başlatılabilmesi sağlanmalıdır. Ayrıca yedekleme işleminin düzenli olarak yapılabilmesi ve takvimlenmesini sağlayan mekanizmalar ile yedekleme işlemlerinin sonlanma durumunu ve hatalarını raporlayabileceğine bir yönetim sistemine sahip olunmalıdır.

2. Ağ Yapısı ve Yönetilmesi

Fidye yazılım saldırına karşı yeterli ağ tasarım gereksinimlerinin sağlandığından emin olmak için, **ağ yapılarının izlenmesi ve doğru şekilde yönetilmesi** gerekmektedir. Güncel ağ topolojisi bir an önce çıkarmalı ve bu iş periyodik olarak takip edilmelidir. Ağ yönetimi genel olarak aşağıdaki fonksiyonları içermelidir:

- Ağdaki yapılandırma değişikliklerinin takibi ve yönetilmesi,
- Ağ paylaşım izinlerinin tek merkezden takibi ve yönetilmesi,
- Ağ hatalarının tanımlanabilmesi,
- Performans seviyelerinin takibi,
- Ağdaki uç noktalarının güvenli erişimin sağlandığından emin olması için düzenli olarak izleme yapılması ve raporlanması.

Genel bir ağ yönetim mimarisi aşağıdaki bileşenlerden oluşmalıdır:

- Ağ Yönetim Sistemi (NMS: Network Management Sistem): CiscoWorks, SolarWinds, HPE NNMi, gibi ürünleri kullanarak ağ sistemi bileşenlerinin izlenmesi ve yönetilmesi,
- Ağ Yönetim Protokolü: Ağ cihazları ve Ağ Yönetim Sistemleri arasında bilgi değişiminin yapılabilmesi için protokol desteğinin sağlanması. (Örneğin SNMPv3 gibi),
- Yönetilen Cihazlar: Yönlendirici (Router) veya Anahtar (Switch) gibi ağ cihazlarının, NMS tarafından yönetilmesi.
- Yönetim Ajanları: Yönetilen cihazlardan ağ yönetim bilgilerini toplayan ve kayıt altına alan yazılımlar.

Günümüz BT dünyasının siber güvenlik gereksinimleri olan Güvenlik Duvarları, IDS, IPS, WAF gibi çözümlerin ağ yapısına entegrasyonu gerekmektedir. Bunun yanında yukarda belirtilen güvenlik gereksinimlerini karşılamak için ağ trafiği izolasyonunun sağlanması gerekmektedir. (Örneğin, MPLS / VRF'ler (sanal özel ağ yönlendiricileri / ileticiler) ile genel yönlendirme kapsüllemesi [GRE] gibi tünel oluşturma). Bu sayede güvenlik, performans ve yönetilebilirlik değerleri en yüksek seviyede tutulabilmektedir.

3. Güvenlik Farkındalığı Eğitimi

İyi yetiştirilmiş ve bilinçlendirilmiş **insan kaynağı,** herhangi bir kurum veya kuruluşa ait sistemlerin güvenlik temelini oluşturmaktadır. Kurum ve kuruluşlar, siber güvenlik planlarını gerçekleştirmek için gerekli uzmanlığı sağlamalı ve fidye yazılım saldırılarına karşı ilk savunma hattının insan olduğu unutulmamalıdır. Dünyaca ünlü bilişim firmalarının son yıllarda yaşadığı bilgi güvenliği ihlal olayları detaylıca incelendiğinde, sorunun ana kaynağının çalışanların bilgi güvenliği farkındalıklarının eksikliği olduğu ortaya çıkmaktadır. Çalışanların farkındalık seviyelerinin arttırılmasında en önemli maddelerden biri, düzenli olarak eğitim verilmesi ve eğitimler sonrası farkındalık senaryolarını içeren saldırı simülasyonlarının gerçekleştirilmesidir. Güncel saldırı yöntemleri ve bunlara karşı alınabilecek önlemlerin senaryolar eşliğinde eğitim yapılması ve sonrası gerçekleştirilecek **farkındalık seviyesi ölçüm/değerlendirme sınavı** ile katılımcıların farkındalık seviyesindeki artışı da somut olarak görülebilmektedir.

4. Yama yönetimi ve güncelleme süreçlerinin gözden geçirilmesi

Fidye yazılım geliştiricileri sıklıkla bilinen açıklara sahip güncel olmayan yazılımlardan faydalanıp kullanıcıların sistemlerine sessizce sızarak virüsleri bulaştırabilmektedir. Eğer yazılımlarınızı sıklıkla güncelliyorsanız fidye yazılımlarının bulaşmasına karşı daha korumalı olduğunuz söylenebilir. Bazı yazılım üreticileri güncellemelerini düzenli olarak (Microsoft ve Adobe her ayın 2. salı günü) yayınlamaktadır, ancak bazı acil durumlarda bu standart zamanlar dışında da güncelleme yayınlanmaktadır. Kurum ve kuruluşa özgü yama yönetimi takibi yapılması bu tür zararlılarla mücadele anlamında önem arz etmektedir.

5. Anti-spam / malware korumasının özelleştirilmesi

Düzenli olarak güncellenen, ileri düzey özelleştirilmiş anti spam koruması fidye yazılım saldırılarına karşı etkili bir önlem olmaktadır. Yeterli kurum veya kuruluşa özgü ayarları yapılmış spam önleme servisleri, e-posta sunucusu yazılımlarımı ile eş zamanlı çalışmasıyla çok daha güvenli ve yüksek oranlarda verimlilikle hizmet vermeleri sağlanabilir.

6. Ağınızın korunması için yeni nesil güvenlik sistemlerinin kullanılması

Güvenlik duvarınız, imza tabanlı algılama yaklaşımlarını da içermelidir ancak sürekli olarak güncellenen bir tehdit özet akışına dayalı bilinen tehditleri de engellemelidir. Sandboxing (kum havuzu analizi), sürekli olarak görünen yeni bir fidye yazılımın saptanması için alternatif bir yöntem olarak **Olay yanıtı planlaması.**

"Biz fidyeyi ödeyelim ama bize şifre çözme anahtarı vermezlerse **?**" Birçok kuruluş güvenlik olaylarına nasıl yanıt vereceğini ancak bir saldırıya uğradıktan sonra öğrenmektedir. Maliyetini ve zararını azaltmak için bir saldırı gerçekleşmeden önce **olay yanıtı planınızın** olması önemlidir. Etkili bir olay yanıt planı, üç temel özelliğe bağlıdır: tehditlere karşı koruma, tehditleri algılama ve yanıtlama. Koruma; olayları önlemek, algılama; tehditleri erken belirlemek ve yanıt; saldırganı uzaklaştırıp sistemleri geri yükleyerek bir ihlalin etkilerini azaltmak içindir.

Muhtemelen kurum ve kuruluşunuzda bir ihlal olayına yönelik genel tepki planınız vardır ancak, fidye yazılım saldırıları diğer zararlı yazılım olaylarından çok farklı ve özel bir iyileştirme süreci gerektirdiğinden bu saldırı türüne özgü bir yanıt planı geliştirmeniz önerilmektedir. Olay gerçekleşmeden önce bir ekibin toplanması kuruluşunuz için çok önemlidir ve olayların nasıl ele alındığını olumlu yönde etkilemektedir. Kaynakları izlemek için doğru araçlara sahip olunması bu ekibin bir güvenlik olayını düzeltmek üzere doğru adımları uygulamasına yardımcı olabilmektedir. Olay yanıt planında bu tür senaryoları ne kadar ayrıntılı düşünüp planlarsanız, yanıtlama sürenizde o kadar kısa olacaktır.

7. Tehdidi Anlama

Günümüz fidye yazılım saldırılarından korunmak için ekonomik sınırlar dâhilinde güvenliği sağlamak için uygulama bazında tedarik ve operasyonların zaman ve maliyetini azaltacak risk odaklı bir yaklaşım izlenmelidir. Bu riske dayalı yaklaşım, belirli uygulamalar bağlamında

belirlenmiş riskleri ele alarak gelecekte yapılacak güvenlik yatırımlarını kolaylaştıracağı düşünülmektedir.

Doğru bir güvenlik risk analizi yapmak için güvenlik ekipleri, yönetilen varlıklara yönelik fidye yazılımları tehdit ailesini tam olarak bilmelidir. Potansiyel tehditlere karşı güvenlik risklerini belirlemek, bu riskleri değerlendirmek ve her bir riske nasıl cevap verileceğine karar vermek maksadıyla kurum ve kuruluşlar için **tehdit modelleme metodolojisi** gereklidir. Tehdit modelleme fidye yazılımlarla mücadele için temeldir ve organizasyonların doğru kontrolleri belirlemesini ve bütçe içinde etkili karşı tedbir oluşturmasını sağlar.

8. Hasarın Kontrol Edilmesi

Gerçekleşen fidye yazılım saldırısına yönelik olarak potansiyel delil ve bilgi toplanması olay sonrası inceleme ve tehdidin tekrar ortaya çıkmaması için önem arz etmektedir. Yinelemeyi önlemek için ele alınması gereken zayıf noktaları ve sistem zayıflıklarını belirlemek için zararlı yazılımın kaynağı analiz edilmelidir. Ancak önce düşünülmesi gereken başka şeyler vardır. Örneğin, saldırıya uğrayan sisteminizde nelerin eksik olduğunu biliyor musun? Saldırgan fidye yazılım ile dosyalarınızı şifrelediğini iddia ediyor, ancak önemli bir şeyi kaybettiniz mi?

Bu kapsamda olay müdahale ekipleriniz mevcutsa, en son yedekleri veya hizmetin sürekliliğini ve güvenliğin ihlal öncesi durumuna dönüş için alternatif çözümleri belirlemek size hasarın etkisini azaltacaktır. Olay müdahale ekibinin saldırıyı tüm yönleri ile analiz etmek için adli verileri kullanması gerekmektedir. Bir fidye yazılım saldırısı durumunda olay müdahale ekiplerinin tüm bilgileri aklında tutması, elle bir rapor oluşturması zaman almaktadır. Son yıllarda kuruluşları etkinleştirmek için otomatik çözümler kullanılabilir hale gelmiştir. Otomatik adli analiz araçlarının uygulanması saldırıyı kapsamlı olarak anlamak açısından olay müdahale ekibinin yeteneğini büyük ölçüde arttırmakta ve iyileştirme için yol gösterici olmaktadır. Bu araçlar olay analizi için önemli ölçüde zaman azaltmakta ve bilgi güvenliği personelinin saldırıları anlayarak daha etkili ve verimli şekilde yanıt verebilmelerini sağlamaktadır.

Hatırlanması gereken önemli nokta, yanıtınızı planlamaya başlamadan önce bir yanıtın gerçekten gerekli olduğundan emin olmanızdır. Modern fidye yazılımı, en değerli dosyaları ve güçlü şifreleme standartlarını öncelik sırasına koymak için uygulama beyaz listelerini kullandığından, kaba kuvvetle erişmenizi önlemek için durumunuzun idealden daha az olduğunu bulacaksınız ancak kontrol etmeniz zarar vermez. Ekran kilitleyen fidye yazılımını ve kripto fidye yazılımının bazı türevlerini algılayabilen, ücretsiz şifre çözme araçları, farklı güvenlik üreticilerinden kolayca temin edilebilir. Bunlar, şifre çözme anahtarlarına ödeme yapmamak için kullanılabilir. Farklı durumlarda, söz konusu fidye yazılımın kum havuzu (sandbox) analizi, kötü amaçlı yazılım davranışını belirlemenize yardımcı olabilir. Bu ayrıca fidye yazılımın yeteneklerini, rutinlerini ve kullanılan taktiklerini tespit etmeyi artırabilir ve gelecekteki olayları önleme yollarını belirlemek için kullanılabilir.

9. Operasyonel Temizleme

Fidye yazılımından kurtulma işlemi iki adımdan oluşmaktadır: Zararlı yazılımın bulaştığı **sistemin temizlenmesi ve şifrelenen dosyaların şifresiz hale geri getirilmesi**.

a. Fidye yazılımın birçok çeşidi, şu anda çoğu güncel anti virüs yazılımı tarafından tespit edilip temizlenebilmektedir. Dolayısı ile öncelikle zararlı yazılımın bulaştığı bilgisayar, zararlı yazılım tespit edilip temizlenene kadar, farklı anti virüsler ile taratılmalıdır.

b.

b. Ancak, fidye yazılımların birçok türevi olduğu ve sürekli olarak şekil değiştirdiği göz önüne alındığında, tespit edilememe ihtimali de oldukça yüksektir. Dolayısı ile tam olarak temizlik için, bulaştığı bilgisayara format atılarak, tekrar işletim sistemi kurulması gerekmektedir.

c. Üst maddede açıklandığı gibi zararlı yazılımı temizlemek, şifrelediği dosyaların şifresini çözmemekte, sadece fidye yazılımın daha fazla dosyanızı şifrelemesini engellemektedir.CryptoLocker vb. fidye yazılımlar, şifrelemede RSA-4096 / AES-256 benzeri çok güçlü şifreleme algoritmaları kullanmaktadır. Dünyada şifre kırma yöntemlerinde gelinen son durumda,

belirtilen algoritmanın kaba kuvvet (brute force) yöntemiyle kırılabilmesi için milyonlarca yıldan çok daha fazla süre gerektiğinden, söz konusu algoritmalar kırılamaz kabul edilmektedir

e. Fidye yazılımların birçok türevi olması, ayrıca saldırganların her bir bilgisayar için farklı anahtarlara sahip virüsler üretmesi nedeniyle, zararlının şifrelediği dosyaların çözülmesi için bir çözücü yazılım üretilmesi de mümkün olamamaktadır. Dolayısı ile şifrenin çözülmesi günümüz şartlarında şifre anahtarını bilmeden mümkün değildir (CryptoLocker vb. fidye saldırılara karşı çözüm geliştirdiğini ifade eden internetteki birçok hilekâra karşı dikkatli olunmalıdır).

f. Halihazırda genel şifre çözme amaçlı geliştirilen yazılımlar, maalesef fidye yazılımlar için kullanılamamaktadır çünkü fidye yazılım ailesinin 20'den fazla bilinen türevi vardır ve sürekli değişiklik arz edebilmektedir.

g. Denenmesi gereken ilk işlem, zararlı yazılım dosyaları şifrelemeyi müteakip orijinal halini hızlı silmiş olabileceği umularak, fidye yazılımın bulaştığı sürücülerde veri kurtarma (File recovery) yazılımları ile silinmiş olan orijinal dosyaları geri getirmeye çalışmaktır. Geri getirme ortamı olarak harici USB disk/bellekler tercih edilmelidir.

h. Yapılabilecek diğer işlem ise, dosyaların virüs tarafından şifrelenmeden önce alınmış bir yedeği varsa, o yedeğin kullanılmasıdır. Bu kapsamda, genel tedbirler olarak;

(1) Kritik dosyalarınızın belirli aralıklarla yedeğini tek yazımlık CD/DVD'lere almanız tavsiye edilmektedir (Tek yazımlık DVD'lerde bulunan dosyaların, DVD'nin yapısından dolayı fidye yazılımlar tarafından şifrelenmesi teknik olarak mümkün değildir).

(2) Bilgisayarlardaki işletim sistemlerinde, dosyaların değişmesi (silinmesi, içeriğinin değişmesi vb.) durumunda otomatik olarak bir önceki versiyonunun arşivlenmesini sağlayan imkânlar bulunmaktadır. Bu işlevleri açık olan bilgisayara fidye yazılımlar bulaşsa bile, şifrelenmeden önceki versiyonlara geri dönülmek suretiyle zararının telafi edilmesi sağlanabilir. Ancak; fidye yazılımların bazı gelişmiş türlerinde, oturumu açan kullanıcının yetkisi var ise, zararlı yazılım, işletim sisteminin tuttuğu eski dosya

versiyonlarını da silmektedir. Bu durumda bu işlevler maalesef işe yaramayacaktır.

10. En Kötü Senaryo Durumu

Fidye yazılım tarafından şifrelenen dosyalara ait anahtarı almak için bir fidye ödemek, bir kurum veya kuruluşun son başvurması gereken çözüm olmalıdır. Şüphesiz ki saldırganlara yapılan ödemeler, suç örgütlerine fon sağlanmasına yardımcı olmaktadır. Bu hususu da unutmamak gerekir. Şifreli verilerinizden yedekleriniz yoksa bile, ödeme yapmadan önce aşağıdaki seçeneklerinizi göz önünde bulundurun:

• Şifrelenen verileri yeniden yaratabilir misiniz?

• Dosyaların yeni bir sürümüyle güncellenebilecek eski bir sürümünü bulunmakta mıdır?

•Zararlı yazılımın erişemediği, verilerinizi barındıran ve etkilenmeyen başka bir sisteminiz mevcut mudur?

Kısacası, ayrıntılı bir mücadele yöntemi ve bu durumun tekrar oluşmasını önlemek için siber güvenliğinize yönelik tedbirlerinizi geliştirmeniz gerekmektedir. Son olarak normale dönüşün gerçekleşmesi için çok katmanlı güvenlik anlayışını içeren bir yaklaşımınız olmalıdır. Güncellenmiş varyantlar ve fidye yazılım aileler ile hemen hemen her gün yenisi yayınlanan zararlı yazılımların hızlı gelişimi, siber suçluların bunu kârlı bir saldırı biçimi olarak gördüğünü göstermektedir.

Fidye yazılım saldırıları ile mücadelede güvenlik için çok katmanlı bir yaklaşım, olası tüm giriş noktalarının fidye yazılımından korunmasını sağlamada hayati öneme sahip olmaktadır. Bu tehdit türünün getirdiği riskleri en az düzeye indirmek için çok katmanlı, adım adım bir yaklaşımdan yararlanılması kurum ve kuruluşlar için fayda sağlayacağı düşünülmektedir. Kurum ve kuruluşun mevcut yapısında gerçekleştirilecek analiz çalışmaları göz önünde bulundurularak kendine özgü bir güvenlik anlayışı oluşturulması gerekmektedir.

Çok katmanlı bu yaklaşımda aşağıdaki katmanlar ve katmanlarda kullanılması önerilen uygulamalar genel hatlarıyla şunlardır;

- **E-posta ve Web Koruması**: Fidye yazılımlar, kullanıcılarınıza, e-postalara ve web ağ geçitlerine erişmeden engellenmelidir. E-posta ağ geçidinde fidye yazılımı tespiti daha derin bir e-posta inceleme seviyesi ile daha iyi hale getirilmelidir. Koruma sisteminiz e-posta ağ geçidinizle birlikte çalışarak, fidye yazılımlarının sisteminize taşınması için sıklıkla kullanılan oltalama e-postalarını ve zararlı e-posta eklerini engellenmelidir. E-postalar dışında, kullanıcılarınız kasıtlı olarak zararlı olacak şekilde tasarlanmış ya da ele geçirilmiş web sitelerine tıklayarak da fidye yazılımlarından etkilenebilir. Sıfırıncı gün açıklarını ve tarayıcı açıklarını tarayarak vir URL'nin fidye yazılımı için bilinen bir iletim aracı olup olmadığını belirlemek için gerçek zamanlı web analizi yapılmalıdır.
- **Uç Nokta Koruması:** Fidye yazılımlar, verilerinizi kurtarmak için sizleri ödeme yapmaya zorlamadan önce uç noktada yakalanmalıdır. Son kullanıcıya ulaşan fidye yazılımın dosyalarını sadece çalışma zamanından önce değil, çalışma sırasında da analiz eden yüksek yoğunluklu makine öğrenimi bir tedbir olarak uygulanmalıdır. Uygulama kontrolü ile uygulama beyaz listeleri oluşturmalıdır. Bu kontrol ile sadece bilinen iyi uygulamaların yürütülmesine izin verilerek fidye yazılımları gibi bilinmeyen uygulamaların da yürütülmesi engellenmelidir. Birden fazla dosyanın hızlı bir şekilde şifrelenmesi gibi fidye yazılımlarıyla ilişkili şüpheli davranışlar için davranış izleme ile şifreleme süreci otomatik olarak durdurularak fidye yazılımın sistemdeki verilerde daha fazla zarara yol açmadan kontrol altına alınması sağlanabilir.

- **Ağ Koruması:** Ağınızdaki fidye yazılımlar tespit edilip engellenmelidir. E-posta ve web yaygın fidye yazılımı giriş noktalarıdır ancak diğer ağ protokolleri ve saldırı yöntemleri de kurum ve kuruluşları fidye yazılım saldırılarına maruz bırakabilir. Fidye yazılımların, tüm siber saldırı aşamaları boyunca model ve davranış tabanlı analiz yapılarak komuta-kontrol sunucu trafiğinin tespit edilip engellenmesi gerekmektedir.

- **<u>Sunucu Koruması</u>:** Fidye yazılımların, en değerli veri dosyalarınızın bulunduğu sunucularınıza sızması engellenmelidir. Fidye yazılımları giderek daha fazla sunucuyu hedef almaktadır. Örneğin SAMSAM (SAMAS olarak da bilinen) gibi yüksek profilli örneklerde saldırganlar fidye yazılımını sızdırmak için bilinen yazılım açıklarını kullanmaktadır. Sunucular ve uygulamalar için bir koruma oluşturup, bir yama veya onarım uygulanana kadar bilinen yazılım zayıflıklarından yararlanılmasını önlenmelidir.

SONUÇ

Geçtiğimiz son birkaç yılda artış göstererek yaşanan fidye yazılım saldırıları, geniş güvenlik bütçelerine sahip çok uluslu büyük firmalarından devlet kuruluşlarına kadar çoğu kurum veya kuruluşun; kullanıcılarını, sistemlerini ve süreçlerini en son tehditlerden ve akıllı siber saldırganlardan tamamen koruyamadıklarını göstermektedir. Saldırganlar hedef olarak güvenlikte en zayıf halka olan kullanıcılara yöneltmekte ve bu sayede istedikleri verilere ulaşabilmektedirler. Çoğu vakada karşımıza çıkan saldırıların temel zafiyetler; çalınmış yetkiler, güvenlik yamaları yüklenmemiş bir sistem veya dikkatsiz bir kullanıcı olmaktadır. WannaCry örneğinde de açıkça görüldüğü üzere, devletlerin güvenliklerini sağlama noktasında, geleneksel güvenlik anlayışına göre şekillenmiş tüm kurum ve stratejilerini, etkili bir siber saldırı ve siber savunma kapasitesi oluşturmak adına yeniden organize etmesi de gerekmektedir (Darıcılı, Siber Uzay ve Siber Güvenlik Nedir?, 2017, s. 234).

Siber saldırganlar istediklerini bir kere elde ettikten sonra, kolayca bunu istismar ederek diğer kurum ve kuruluşlara ait değerli verileri de çalabilmektedirler. Bu açıdan siber tehdit istihbaratının elde edilmesinde ve analizinde vazgeçilmez bir unsur olan kurumlar ve kuruluşlar arası **bilgi paylaşımı**, üzerinde durulması gereken bir konu olarak karşımıza çıkmaktadır. Fidye yazılım saldırıları ile mücadele kapsamında kurumlar ve kuruluşlar arası işbirliğine dayanan güvenlik istihbarat teknolojileri kullanılarak siber atakları tespit etme ve kontrol altına alma konusunda daha etkin bir mücadele yapılabileceği değerlendirilmektedir.

CryptoLocker, WannaCry, Petya, ve daha birçok fidye zararlı yazılımı ortaya çıkmaya devam edecektir. Ancak geliştirilen zararlı fidye yazılımlarının saldırı noktaları ve etki hacimleri, saldırılarda kullanılan yöntemlerle doğrudan ilişkilidir. NSA, TAO, CIA gibi birimler tarafından geliştirilmiş ve sızdırılan bu siber silahların sistemlerde ne tür zafiyetleri sömürebileceğini önceden tespit etmek için gönüllü inisiyatiflerin yanında resmi araştırma birimleri oluşturulmasına zemin hazırlanması çok büyük önem arz etmektedir.

Bu gibi gizli servislerin çeşitli işletim sistemleri içerisinden önceden tespit ettikleri zafiyetler aracılığı ile dünya genelindeki tüm ülkelere APT (Advance Persistent Threat) saldırıları gerçekleştirdikleri, bizlerin ise bu zafiyetlerden ancak WannaCry veya Petya gibi dünya genelini etkisi altına alabilecek ve kritik altyapıları zarara uğratacak çapta saldırılar meydana getirdiğinde haberdar olabildiğimiz gerçeğinin altı önemle çizilmelidir. Bu noktada somut adımlar atılarak APT saldırılarının önüne geçilmesi için **milli-yerli ürün ve hizmetler** temelinde acil tedbirler hayata geçirilmelidir. (Sarı, 2017).

Ancak ne tür bir aksiyon alınırsa alınsın hatalardan mutlaka ders çıkarmaya özen gösterilmelidir. Neyin yanlış gittiğini ve gelecekte nasıl engelleneceğini belirlemek için kurum veya kuruluşun işleyişine **özgün bir mücadele yöntemi** belirlenmesi gerekmektedir. Güvenlik açığı ve yama yönetimi, güvenlik farkındalığı eğitimi, sıkı e-posta tarama önlemleri ve kapsamlı bir off-site yedekleme planı gibi mantıklı siber hijyen programların mevcut olduğundan emin olunmalıdır.

Sonuç olarak; çalışmada anlatılmak istenen mücadele yöntemlerinin kullanılması ve fidye yazılım saldırılarına ilişkin bahsedilen temel güvenlik tedbirlerini uygulanmasıyla birçok saldırıdan korunmak ve saldırılardan en az seviyede zarar görecek şekilde hazırlanmak mümkündür. Bu noktada, son kullanıcı güvenlik farkındalığın artırılması ve kurumların siber güvenlik personelinin uzmanlık derecesinin iş bölümü yapılarak üst seviyede tutulmasına yönelik çalışmaların yapılması da oldukça önem arz etmektedir. Çalışmanın sonunda Benjamin Franklin'in bir sözünü hatırlatmakta fayda

görülmektedir: **"İyileşmek için tedavi görmektense, hasta olmamak için tedbir al."**

REFERANSLAR

Darıcılı, A.B. (2017). Siber Uzay ve Siber Güvenlik Nedir? Bursa, Dora Yayınları, s. 233-234.

Fasheem, S. (2017). Detection and Avoidance of Ransomware. *IJEDR, Volume 5, Issue 1*, s. 52.

Gollman, D. (2011). *Computer security*. New York: Wiley.

Hallam-Baker, P. (2016). Ransomware, Everywhere: What's The Science Behind It? s.1.

J.Crowe. (2017). *Must-Know Ransomware Statistics.*

Luo, X. , Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention. *Information Systems Security*, s.195-202.

Sarı, D. A. (2017). Ransomware ve Son Varyantlar Analizi. *Cezeri Siber Güvenlik Akademisi Yayınları, 1*.

Uitsec Teknoloji. (2014). *Cryptolocker Analiz Raporu.*

Ulaştırma Denizcilik ve Haberleşme Bakanlığı(2017), www.udhb.gov.tr/images/duyurular/74bc0128f065b41.pdf

[Erişim Tarihi: 05.12.2017].

Wikipedia. (2016). https://en.wikipedia.org/wiki/KeRange [Erişim Tarihi: 10.12.2017].

Palmer, D. (2017). https://www.zdnet.com/article/locky-ransomware-why-this-menace-keeps-coming-back/ [Erişim Tarihi: 17.12.2017].

Barkly. (2017). *https://blog.barkly.com/ransomware-statistics-2017* [Erişim Tarihi: 5.10..2017].

Kaspersky Security Bulletin (2015). https://securelist.com/kaspersky-security-bulletin-2015-overall-statistics-for-2015/73038/ [Erişim Tarihi: 15.12.2017].

Microsoft Azure (2017) https://docs.microsoft.com/tr-tr/azure/security-center/security-center-incident-response [Erişim Tarihi: 10.11.2017].

Security Response. (2017). https://medium.com/threat-intel/ransomware-history-3165f10ab5a5 [Erişim Tarihi: 16.12.2017].

Symantec Labs (2009) https://www.symantec.com/security-center/writeup/2009-022723-4223-99 [Erişim Tarihi: 17.12.2017].

Trendlabs, T. M. (2018). https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2017-annual-roundup-the-paradox-of-cyberthreats [Erişim Tarihi: 12.04.2018].

Trend Micro (2015). http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/. [Erişim Tarihi: 17.12.2017].

BBC News(2017). http://www.bbc.com/news/world-europe-39907965 [Erişim Tarihi: 11.12.2017].

Robert L. (2008). http://www.securityfocus.com/news/11523. (2018, 4 20) [Erişim Tarihi: 11.12.2017].

The Journal (2012). http://www.thejournal.ie/gardai-garda-police-trojan-scam-virus-logo-locking-488837-Jun2012/. [Erişim Tarihi: 05.02.2018].

ESET. https://renew.stratus.com.tr/cryptolocker/index.html. [Erişim Tarihi: 17.12.2017].

TerraMedusa Secure (2015)https://terramedusa.com/dosyalari-sifreleyip-bitcoin-isteyen-zararli-yazilim-325-milyon-dolar-kazandirdi/ [Erişim Tarihi: 07.03.2018].

CNeT (2012) https://www.cnet.com/news/ransomware-a-growing-menace-says-symantec/. [Erişim Tarihi: 11.02.2017].

Department of Justice (2017) https://www.justice.gov/archives/opa/documents-and-resources-gameover-zeus-cryptolocker-press-conference ([Erişim Tarihi: 11.12.2017].

PCWorld (2010) https://www.pcworld.com/article/204577/article.html. (2018, 4 22). [Erişim Tarihi: 11.12.2017].

TechRecuplic (2010) https://www.techrepublic.com/blog/it-security/ransomware-extortion-via-the-internet/ [Erişim Tarihi: 11.12.2017].

TechWorld (2012) https://www.techworld.com/news/security/ransom-trojans-spreading-beyond-russian-heartland-3343528/ [Erişim Tarihi: 11.12.2017].

The Guardian (2013) https://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware. ([Erişim Tarihi: 21.01.2018].

FBI News (2016) https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise [Erişim Tarihi: 14.02.2018].

SİBER UZAY VE İNSAN HAKLARI

[*]Anıl Cumali ÇOKBİLDİK

Özet

Siber uzayda insan hakları mevzuatının en önemli parçaları, ifade, görüş, kişi özgürlüğü ve mahremiyet hakkıdır. İfade özgürlüğü, kişi güvenliği ve özgürlüğü, özel yaşamın gizliliği ve kişisel verilerin korunması sık sık ihlal edilen hakların başında gelmektedir. İletişim ve bilişim alanındaki teknolojilerin artmasına paralel bir biçimde ortaya çıkan bu güvenlik sorunları geç te olsa bilişim hukukuna yönelik adımların atılmasını sağlamıştır. Bu çalışmada sırasıyla insan hakları ve siber uzayın tarihsel gelişimi, siber uzay ve insan hakları ilişkisinin boyutları, siber uzayda ihlal edilen insan hakları ve bu hakların korunmasına yönelik atılan ulusal, bölgesel ve uluslararası çalışmalar incelenmektedir.

Anahtar Kelimeler: Siber Uzay, İnsan Hakları, Hukuk.

CYBERSPACE AND HUMAN RIGHTS

Abstract

The most important parts of human rights legislation are the right to expression, opinion, personality and privacy in cyberspace. Freedom of statement, personal security and freedom, private life and the protection of personal data are often violated. These security issues, which emerged in parallel with the increasing technology in the field of communication and information technology, made it possible to take steps towards information law in the late stage. This study examines the historical development of human rights and cyber space, the dimensions of cyber space and human rights relation, human rights violations in cyberspace, and national, regional and international studies on the protection of these rights.

Keywords: Cyberspace, Human Rights, Law.

GİRİŞ

Tarih boyunca teknolojide meydana gelen gelişmeler, insan yaşantısı üzerinde birçok değişime ve dönüşüme neden olmuştur. Özellikle 80'li yıllardan itibaren küreselleşme faaliyetlerinin hız kazanması ve teknoloji alanında yaşanan gelişmeler bu değişim ve

[*] Selçuk Üniversitesi Uluslararası İlişkiler Bölümü Yüksek Lisans Öğrencisi. Ulaşmak İçin: cokbildikanilcumali@gmail.com

dönüşümün daha hızlı bir biçimde gerçekleşmesine neden olmuştur. Enformasyon çağı olarak adlandırabileceğimiz bu çağa girişi sağlayan en önemli faktör ise internetin ortaya çıkması olmuştur. Bilgi ve iletişim alanında baş döndürücü bir hıza kavuşmamızı sağlayan internet sayesinde (küreselleşmenin de bir uzantısı olarak) sınırlar ortadan kalkmış bireylerin istedikleri bilgiye ulaşabilme kapasitesi artmıştır (Kıvılcım, 2013: ss.222-223).

İnternetin yaygınlaşması ile siber uzay dediğimiz sanal dünyanın sınırları ise kestirilemeyecek ölçüde genişlemiştir. Bugün, gündelik yaşantımızda farkında olmadan gerçekleştirdiğimiz çoğu işlem teknolojik gelişmelere ve internete bağlı olarak karşımıza çıkmaktadır. İnternet yaygınlaştıkça hız ve yoğunluk onu kullanan bireylere paralel bir biçimde daha da artmıştır. Bugün dar bir perspektiften bakıldığında online bir şekilde gerçekleştirdiğimiz alışverişler, eğitim ve sağlık hizmetleri, haberleşme ve iletişim faaliyetleri internetin hayatımızı kolaylaştıran unsurları olarak karşımıza çıkmaktadır (Ünal, 2009: ss.132-134).

Bilgi ve iletişim alanında yaşanan teknolojik gelişmelerin insanlık açısından birçok fırsatı beraberinde getirdiği bir gerçektir. Ancak bu gelişmeler birçok riski ve tehdidi de bünyesinde barındırmaktadır. Özellikle internetin bu kadar yaygınlaşması siber uzay dediğimiz alanda güvenlik sorunlarının ortaya çıkmasına neden olmuştur. Siber uzay, bir anda ortaya çıkan ve sınırları belli olan bir kavram değildir. Bir benzetme yapılacak olursa, evren gibi genişlemeye devam eden ve genişledikçe içerisinde birçok aktörün yer aldığı/alacağı ve eksileceği bir alan olarak düşünülmektedir (Bryant, 2001, s.142).

İnternet ağlarının yayılması ile birlikte siber alanda faaliyette bulunan aktörlerde birbirine daha çok bağlanmıştır. Bu nedenle bu alan sadece fırsatlardan ve kolaylıklardan herkesin eşit bir biçimde yararlandığı bir ortam olarak düşünülmemelidir. Kişisel verilerin çalınması, dolandırıcılık ve sahtekârlık faaliyetleri, özel hayatın gizliliğine yönelik ihlaller, tehdit ve şantaj, siber zorbalık, çocuk pornografisi, ahlak kurallarının ihlali, kiralık katil ilanları, insan kaçakçılığı, uyuşturucu tacirliği, terörist faaliyetler, şirket ve devletlerin stratejik ve gizli olan belgelerinin çalınması ve satılması gibi faaliyetler bu alanda karşımıza çıkan tehditlerden ve suçlardan bazılarıdır (Malhotra, 2016: ss.145-148).

Bu çalışmada: Siber uzay ve insan hakları arasında ilişkinin boyutları nelerdir? Siber uzayda insan haklarını korumak mümkün müdür? Siber uzayda ihlal edilen insan hakları nelerdir? Siber uzayda sahip olduğumuz hak ve özgürlükler nelerdir? Siber uzayda insan haklarını

koruma mekanizmaları var mıdır? Gibi sorulara cevap verilecektir. Ayrıca çalışmada insan haklarını merkeze alan bir yaklaşımla siber uzayda yer alan aktörler arasındaki işbirliğinin kısıtlı olmasının nedenleri analiz edilecektir. Bu soruların cevaplanması kapsamlı bir literatür taramasına, çalışmada adı geçen anlaşmaların ve sözleşmelerin incelenmesine, güncel gelişmelerin dikkate alınmasına, kronolojik sıralamaya, örneklendirme ve karşılaştırmaya dayanmaktadır.

1. İnsan Hakları ve Siber Uzay İlişkisi

İnsan Hakları ve Siber Uzay alanları arasındaki ilişkilerin daha iyi analiz edilebilmesi için tarihsel arka planlarını ve gelişmelerini incelemek gerekmektedir. Bu iki alan birbirinden bağımsız bir gelişim süreci gösterse de özellikle 90'lı yıllardan itibaren internetin yaygınlaşması ile birlikte etkileşim içerisine girmiş ve birbirlerini yakından ilgilendiren alanlar olmuşlardır. İnsan haklarının kökenleri siber uzay alanına göre daha eskiye dayanmaktadır. Bu nedenle öncelikli olarak insan haklarının tarihsel gelişimi incelenecek sonrasında siber uzay alanı hakkında tarihsel arka plan gelişmeleri ele alınacaktır.

1.1. İnsan Haklarının Tarihsel Gelişim Süreci

Yaklaşık 2500 yıllık bir geçmişi bulunan insan hakları, tarihsel süreçte önce düşünsel alanda yani filozofların felsefi bakış açılarında ve tartışmalarında ortaya çıkan, sonrasında ise sözleşmelerde, anayasalarda ve uluslararası anlaşmalarda yer alan bir kavram olarak karşımıza çıkmaktadır. Temel olarak ve basit bir ifadeyle insanın korunması gerektiği konusunda ortak kanıya dayanan değerler bütünü olarak ifade edilmektedir. İnsan Hakları kavramının II. Dünya Savaşı'ndan sonra Birleşmiş Milletlerin kurulmasıyla ortaya çıktığı ifade edilse de köken olarak Doğal Hukuk teorisine dayanmaktadır (Küçükali ve Akbaş, 2016: s.71).

Doğal Hukuk Teorisi, kurallarını tanrısal bir güç ya da akıldan alan, toplumlar tarafından oluşturulmayan, doğada kendiliğinden yer alan haklar ve evrensel ilkelerden oluşan, zamandan ve mekândan bağımsız, herkes için geçerli olan ilkeleri ifade etmektedir (Toku, 2004: s.236). Bu teorinin ortaya çıkmasında ve gelişiminde katkıda bulunan kişiler arasında Platon, Aristo, Cicero, Seneca, Confucius, Aquinas, Grotius, Locke, Hobbes, Rousseau gibi ünlü düşünürler bulunmaktadır. Örneğin, Aristo doğa için haklı olan her şeyin yasalara göre

haklı olmayabileceğini ifade etmiştir. John Locke insanın bazı haklarının sırf insan olmasından kaynaklandığını ve bu durumun toplumsal sözleşme öncesindeki doğal durumunda da geçerli olduğunu ileri sürmüştür. Hobbes ise insanın yaşamla birlikte doğal haklara sahip olacağını söylemiştir. Grotius ise insanın doğasında yer alan bir takım temel hakların bulunduğunu ve bu hakların evrensel ve değiştirilemez olduğu görüşüne sahiptir (Kılıç, 2015: ss.99-101).

İnsan hakları bir mücadelenin ürünüdür ve bu mücadele boyunca özgürlük, kölelik, bireyin hak ve ödevleri, ahlak felsefesi, toplumsal sözleşmeler gibi konular tartışılmıştır. Bu tartışmalar köleliğe başkaldırıdan, günümüzde tartışılan siber güvenlik, barış hakkı, çevrenin korunması, vicdani ret gibi kavramlara doğru genişlemiştir. Elbette ki bu değişim ve gelişmeler, hem yukarıda ifade edilen felsefi ve entelektüel gelişmelere hem de aşağıda ifade edilecek olan dünya tarihindeki bazı önemli olaylara bağlı olarak şekillenmiştir (Ünal, 1994: ss.50-52).

1.2. Birinci Kuşak Haklar

Tarihsel olarak bakıldığında insan haklarının gelişiminin genel olarak üç aşamada gerçekleştiği görülmektedir. İlk aşama 17. ve 18. Yüzyıllardaki gelişmelere bağlı olarak gerçekleşmiştir. Bu dönemde özellikle Avrupa'da Rönesans, Reform ve Fransız Devrimi'nin etkisi ile bireysel haklar, özgürlük, adalet, eşitlik kavramlarının geliştiği ve daha sık kullanıldığı görülmektedir. Yine toplumsal sözleşme teorileri ile birlikte bireylerin vazgeçilmez ve devredilmez hak ve özgürlüklerini koruma görevi devlete yüklenmiştir. Devlet eğer bu görevini yerine getiremez ise yapılan sözleşmenin ve devletin meşruluğu ortadan kalkacaktır görüşü benimsenmiştir. Böyle bir durumda halk direnme hakkını kullanarak devlete itaat etmeyecektir (Engin, 2014: ss.206-207).

Fransız Devrimi bu anlamda verilebilecek en iyi örnek olarak karşımıza çıkmaktadır. Devrim ile birlikte ilan edilen 1789 Fransız İnsan ve Yurttaş Hakları Bildirisi insan hakları açısından son derece önemli anlamlar ifade etmektedir. İngiltere'de 1215 Magna Charta ve Amerika Birleşik Devletleri'nde 1776 Bağımsızlık Bildirisi ulusal nitelikli bildirilerdi. Ancak Fransız Bildirisi sadece Fransız yurttaşlarını değil tüm insanlığı kapsayan evrensel bir nitelik taşımaktadır. Bu bildirideki haklar insanın nerede ve ne zaman yaşarsa yaşasın sırf insan olmakla sahip olduğu haklar olarak karşımıza çıkmaktadır. Bu bildiride yer alan haklar daha

çok birincil kuşak haklar olarak nitelenen haklar (yaşama ve özgürlük hakkı, düşünce ve ifade özgürlüğü, kölelik yasağı vb.) olarak karşımıza çıkmaktadır. (Rude, 2015: ss.25-26).

1.3. İkinci Kuşak Haklar

İkinci aşama 19. Yüzyılın ikinci yarısında sosyalist akımların düşüncelerine paralel bir biçimde şekillenmiştir. Bu dönemde ekonomik, sosyal ve kültürel hakların öneminin dile getirilmesi, sadece bireyin özgürlüğünün yeterli olmadığının anlaşılması ikincil kuşak hakların ortaya çıkmasında etkili olmuştur. Bu haklar aynı zamanda pratik açıdan devletin bireye yönelik bir hizmette bulunmasını ve sorumluluk almasını gerekli kılan haklar olarak görülmektedir. Çalışma hakkı, sendikal özgürlükler, grev ve toplu sözleşme hakkı, sosyal güvenlik hakkı gibi haklar bu kategoride yer almaktadır (Cıngı, 2009: ss.11-12).

Özellikle Marksizm akımı zamanın özgürlük anlayışını eleştirerek sadece birincil kuşak hakların yetersiz olduğunu ve bu anlayışın değiştirilmesi gerektiğini savunmuştur. Örneğin bireyin konut dokunulmazlığı hakkının olmasına karşın bir konutunun olmaması bu hakkı işlevsiz bırakmaktadır. Sosyal ve ekonomik yetersizlikler insan hak ve özgürlüklerinin kullanılabilmesine engel olmaktadır. Bu nedenle bu hakların kullanılabilmesi için devlet üstüne düşen görevleri yerine getirmelidir (Algan, 2007: s.48).

1.4. Üçüncü ve Dördüncü Kuşak Haklar

Üçüncü aşama ise 20. Yüzyılın ikinci yarısında insanın yaşadığı çevreye uyumlu ve barışık, doğal, kültürel, sosyal ve ekonomik bir bütünlük içinde olması görüşüne dayanarak ortaya çıkmıştır. Üçüncül kuşak haklar olarak ta ifade edebileceğimiz haklar bu dönemde ortaya çıkmış böylece ulusların sosyal, kültürel, ekonomik kaynaklarını korumaya ve gelecek kuşaklara aktarılmasına yönelik haklar belirlenmiştir. Bunların içinde barış hakkı, tarihsel kalıntıları ait oldukları yerde görebilme hakkı, gelişme hakkı gibi haklar yer almaktadır (Kaboğlu, 2011: s.227).

İnsan haklarının tarihsel aşamaları incelendiğinde son yirmi yıllık dönemde ortaya çıkan dördüncü kuşak haklar tartışmalarına da ayrı bir parantez açmak gerekmektedir. Bazı araştırmacıların siber uzay hakkı, farklı olma hakkı, bilimin kötüye kullanılmaması hakkı, engelli çocukların özel eğitimden yararlanması hakkı, oyun hakkı gibi hakları dördüncü kuşak

haklar olarak değerlendirdiği görülmektedir. Bazı araştırmacılar ise bu hakların da üçüncü kuşak haklar içerisinde yer aldığı, ayrı bir kuşak içerisinde değerlendirilmesine gerek olmadığı görüşünü savunmaktadır. Bu noktada önemli olan husus çalışmanın odak noktası olan siber uzayın üçüncü kuşak haklar içerisinde ya da dördüncü kuşak haklar içerisinde değerlendirildiğinde insan hakları ile etkileşim halinde olduğunun anlaşılmasıdır (Turhan, 2013: s.369).

İnsan hak ve özgürlüklerinin belirlenmesine yönelik bu aşamalar ulusal ya da uluslararası koruma mekanizmalarının ortaya çıkması ile anlam bulmuştur. Bu hak ve özgürlüklerin teminat altına alınması, ihlal edilmemesi bazı standartların belirlenmesi ile mümkün olmuştur. Dünyada insan haklarını korumak ve geliştirmek için atılan adımlara bakıldığında Birleşmiş Milletler ve Avrupa Konseyi'nin yapmış oldukları çalışmalar ön plana çıkmaktadır. BM ve Avrupa Konseyi nezdinde hazırlanan sözleşmeler ve bildirilerden bazıları şunlardır:

Birleşmiş Milletlerin çalışmaları arasında İnsan Hakları Evrensel Beyannamesi, Ekonomik Sosyal ve Kültürel Haklar Sözleşmesi, Soykırım Suçunun Önlenmesine ve Cezalandırılmasına Dair Sözleşme, Çocuk Haklarına Dair Sözleşme, İşkence ve Diğer Zalimane, Gayri İnsani ve Küçültücü Muamele ve Cezaya Dair Sözleşme vb. sözleşmeler bulunmaktadır. Avrupa Konseyi'nin çalışmaları arasında ise Avrupa Sosyal Şartı, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme, Çocuk Haklarının Kullanılmasına İlişkin Avrupa Sözleşmesi, Terörizmin Önlenmesine Dair Avrupa Sözleşmesi, Cinsel Sömürü ve İstismara Karşı Korunması Sözleşmesi vb. sözleşmeler yer almaktadır. (TBMM Başkanlığı, https://www.tbmm.gov.tr/komisyon/insanhaklari/mevzuat_TIHB.htm, (Erişim Tarihi: 24.07.2018).

Çalışmanın bu kısmında detaya girilmeden insan haklarını ele alan hukuki metinlerin bir kısmına yer verilmiştir. Ancak görüldüğü gibi insan hakları ve siber uzay arasındaki etkileşimle birlikte ortaya çıkan sonuçların uluslararası hukuki karşılıklarına değinilmemiştir. Siber uzayda hak ve özgürlüklerin, yerine getirilmesi gereken ödev ve sorumlulukların hukuksal karşılıklarının anlaşmalarla ya da sözleşmelerle güvence altına alınıp alınmadığı çalışmanın sonraki kısımlarında incelenmektedir. Öncelikle siber uzayın ne olduğu, hangi alanları kapsadığı, aktörleri ve tarihsel gelişiminin açıklanması gerekmektedir. Böylece insan hakları ve siber uzayın hukuksal zeminde analizinin yapılması daha anlaşılır olacaktır.

2. Siber Uzayın Tarihsel Gelişim Süreci

İkinci Dünya Savaşı'nın hemen ardından başlayan Soğuk Savaş dönemi dünyayı iki kutuplu bir sistem haline getirmiştir. ABD ve SSCB'nin başını çektiği Batı ve Doğu Bloğu arasındaki mücadele, yaratmış olduğu rekabetçi ortam nedeniyle hem ABD hem de Sovyet Rusya'nın birbirlerini askeri ve psikolojik anlamda sürekli test etmelerine neden olmuştur. Böyle bir ortamda testlerden elde edilen yeni bulgularla hem kendilerinin hem de kendilerine bağlı olan devletlerin savunma sistemlerini güçlendirmeye yönelik adımlar atmışlardır. Hızlı bir silahlanma yarışı, füze sistemlerinin ortaya çıkması ve geliştirilmesi ve ardından uzaya taşınan rekabet siber uzay teknolojisinin altyapısının oluştuğu ve gelişmeye başladığı dönem olarak karşımıza çıkmaktadır (Darıcılı, 2017, ss.2-3).

Siber uzayın gelişimi özellikle internetin gelişimi ile birlikte ele alınmaktadır. 1957 yılında SSCB tarafından uzaya ilk yapay uydu olan Sputnik gönderilmiştir. Buna tepki olarak ABD Savunma Bakanlığı tarafından Arpa (Advanced Research Projects Agency) adında bir birim oluşturulmuştur (Bıçakçı, 2014: s.103). Birbirinden bağımsız bilgisayarların bir ağ üzerinden birbirine bağlanmasına yönelik araştırma birimine ise Arpanet adı verilmiştir. Daha çok askeri temele dayanarak kurulan bu birim ilk veri transferini 1969 yılında gerçekleştirmiştir. Araştırma amaçlı olarak 1974-1976 yılları arasında Intranet adıyla kullanılmıştır. Arpanet'in faaliyet alanı gittikçe genişlemiş ve askeri kanadı Mılnet olarak ayrılmıştır. Arpanet ise zamanla Internet adını almıştır (Bıçakçı, 2014: s.107).

Zamanla nükleer silahların, balistik füzelerin her iki devlet lehine de gelişim göstermesi ise dehşet dengesi olarak ifade edilen bir durumun ortaya çıkmasına neden olmuştur. Bu dengenin bozulmasını sağlayacak olan gelişme 23 Mart 1983 tarihinde ABD Başkanı Ronald Reagan'ın Stratejik Savunma Teklifi (Strategic Defence Initiative- SDI) ile gerçekleşmiştir. Bu teklif ABD'nin nihai hedefi olan caydırıcılığın gerçekleşmesi amacıyla savunma gücünü arttırmayı içermekteydi. Bu plan o dönemde Yıldız Savaşları olarak ifade edilmiştir (Darıcılı, s.11). SSCB bu durumun kendisi için son derece tehlikeli bir sonuç doğuracağının farkına varmıştır. Özellikle ekonomik açıdan bu hamleye karşılık verebilmenin maliyetinin de ülkeyi zor durumda bırakacağını görmüştür. SSCB 1980'lerde RMA (Revolution in Military Affairs) Programı ile silahlı kuvvetlerini modernize etmek istemiştir. Bu program Mareşal Nikolai Orgakov tarafından başlatılmıştır. Bu program ile birlikte ağ teknolojileri, teknolojik

altyapılar ve teknik operasyonlar ile eylem kapasitesi yüksek, daha stratejik ve etkin bir yapının oluşturulması sağlanmıştır (Chapman, 2003).

1983 yılına gelindiğinde TCP/IP (Transmission Control Protocol and İnternet Protocol) protokolüne geçilmiş ve internet ticari amaçlı olarak kullanılmaya başlanmıştır. TCP/IP karşılıklı olarak birbirine bağlı veri iletişimini sağlayan bilgisayar ağını ifade etmektedir. 1989 yılında internetin küreselleşmesinde ve geniş kitlelere sunulmasında öncülük eden isim olan İngiliz Fizikçi Tim Berners-Lee tarafından "World Wide Web" (www) ortaya çıkarılmıştır. Ayrıca "Hypertext" olarak bildiğimiz http sistemini geliştirmiştir. İnternetin kullanılmaya başlanması ve giderek yaygınlaşması denetimini zor bir hale getirmiştir. (Turhan, 2006: s.16).

1989 yılında Berlin Duvarı'nın yıkılması ile SSCB çöküş sürecine girmiştir. 1991 yılında ise kendisine bağlı devletlerin bağımsızlıklarını kazanmasıyla dağılmıştır. Soğuk Savaş'ın getirmiş olduğu rekabet ortamı sonraki yıllarda da devam etmiştir. Bunun nedenleri arasında 1980'lerden itibaren artan küreselleşme akımı, teknolojik gelişmeler ve bilgi toplumuna geçiş gösterilmektedir. Yeni teknolojik gelişmeler (cep telefonu, kredi kartı, internetin ortaya çıkması ve yaygınlaşması, online işlemler, robotik sanayi, ağ teknolojisi ve fiber optik, uydu teknolojilerinin yayılması ve yaygınlaşması vb.) aynı zamanda yeni ekonomik gelişmelerin de önünü açmıştır (Erendor, 2017: ss. 120-121). Küreselleşmenin de etkisiyle yeni ekonomik düzen ülkelerin birbirlerine eskisinden daha çok bağlanmasına ve rekabetin hemen her alanda artmasına neden olmuştur. Bu nedenle Soğuk Savaşın temel aktörleri olan ABD ve Rusya arasındaki rekabet günümüzde Çin, Almanya, İngiltere, Fransa, Japonya, Hindistan, Güney Kore, Kuzey Kore, Kanada gibi ülkelerinde içinde bulunduğu daha geniş bir perspektiften değerlendirilmektedir (Balay, 2004: ss.62-63).

2.1. Siber Uzay

Siber uzayın tarihsel gelişimi ise çok eskilere dayanmamakla birlikte daha çok 20. yüzyılın ikinci yarısındaki teknolojik gelişmelere paralel olarak ilerlemiştir. Siber teriminin kökeni incelendiğinde bu terimin sibernetik kavramından geldiği görülmektedir (Sezgin, 2016: s.562). Sibernetik kavramını ilk kullanan kişi makine-canlı iletişimini inceleyen ve bu alanda yapmış olduğu çalışmalarla sibernetik biliminin kurucu babası sayılan Louis Couffignal'dır. Siber uzay kavramı ise ilk kez William Gibson tarafından 1980'li yılların başında yazmış

olduğu "Neuromancer" adlı bilimkurgu romanında kullanılmıştır (Gibson, 1984). Siber uzayın tanımlanması konusunda farklı yorumlar bulunmaktadır. Bu tanımlamalardan bazıları şunlardır:

- Amerika Savunma Bakanlığı tarafından yapılan tanımlamada; telekomünikasyon ağları ve teknolojik altyapılar sayesinde birbirine bağlı bilgi teknolojilerinin bulunduğu (bilgisayar vs.) küresel bir alan olarak ifade edilmektedir (America Defence Ministry, https://www.defense.gov/portals/1/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf, Erişim Tarihi 22.07.2018).
- Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamdır (Ulaştırma Denizcilik ve Haberleşme Bakanlığı, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf, Erişim Tarihi: 22.07.2018).

Bu tanımlamalardan yola çıkarak bir siber uzay tanımı yapacak olursak:
Siber uzay, bilgi ve iletişim ağlarıyla, dijital bir yaşam alanı olmasının yanı sıra, farklı amaçları olan çok sayıda aktörün yer aldığı, küresel ve bağlantısal bilgi teknolojilerinden oluşan bir alandır.

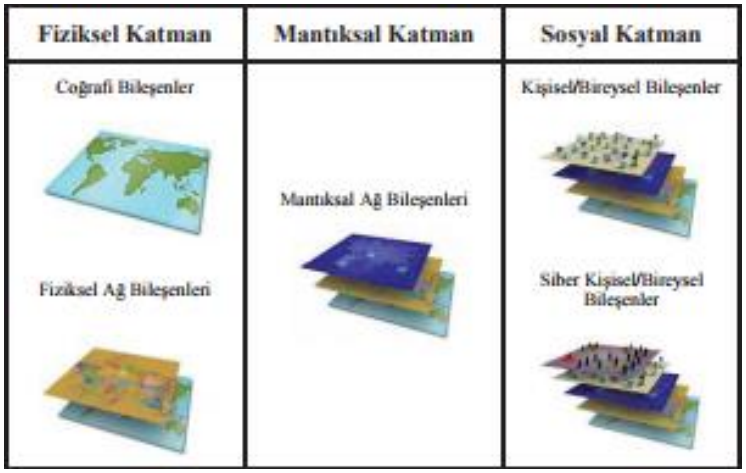
Bir alandaki terminoloji o alanın kavramsallaştırılması ve temel prensiplerinin anlaşılması açısından önemlidir. Bu nedenle siber uzay alanındaki terminolojik ihtiyaç her geçen gün artmaktadır. Çalışmada siber uzay ve insan hakları arasındaki ilişkinin bir uzantısı olarak bu alandaki aktörlerin kendi çıkarları doğrultusunda yapmış oldukları tanımlamaların yaratmış olduğu sorunlar ilerleyen kısımlarda değerlendirilmiştir. İnsan hakları ve siber uzay konusundaki tarihsel arka plan ve gelişim kısaca bu şekilde verilebilir.

2.2. Siber Uzayın Katmanları

Siber uzayın sınırlarını belirlemek oldukça zordur. Ancak siber uzay belirli katmanlardan oluşan boyutlara sahiptir. ABD Kara Kuvvetleri Komutanlığı Siber Uzay Operasyonları Konsept Kabiliyet Planı 2016-2028 isimli bildirisinde siber uzayı çeşitli katmanlara ayırmaktadır. Şekil 1'de görüleceği gibi 3 ana katman bulunmaktadır. Bu katmanlar fiziksel, mantıksal ve sosyal katmanlardır. Bu katmanlarda kendi içinde 5 farklı alt bileşenden

meydana gelmektedir. Fiziksel katman içerisinde coğrafi ve fiziksel ağ bileşenleri yer almaktadır. Ağlara bağlı olarak çalışan bilgi sistemleri coğrafi bileşenler içerisinde bulunmaktadır. Fiziksel ağ bileşenleri ise altyapılara erişimi sağlayan her türlü teknik bileşenleri ifade etmektedir. Mantıksal katman bilgisayar, telefon, modem gibi ağların bağlı bulundukları odak noktalarını ifade etmektedir. Sosyal katman ise kullanıcıların yer aldığı hem gerçek, hem de sanal bireylerden oluşan katmanı ifade etmektedir (US Army Cyberspace Operations Concept Capability Plan, (Erişim Tarihi: 18.07.2018) https://fas.org/irp/doddir/army/pam525-7-8.pdf).

Şekil 1. Siber Uzay'ın Katmanları



Kaynak: https://www.researchgate.net

David Clark'ın siber uzay modellemesinde ise dört katman bulunmaktadır. Bu katmanlar sırasıyla fiziksel iletişim altyapı katmanı, mantıksal katman, bilgi katmanı ve kullanıcıların bulunduğu katmandır. Fiziksel altyapı katmanı siber uzayın bir gerçekliğe dayandığına ve fiziki altyapısına gönderme yapmaktadır. Ancak siber uzayın daha çok sanal bir alan olarak görülmesi onun mantıksal alt bileşenlerinden kaynaklanmaktadır. İkinci katman olan mantıksal katman fiziksel temellerle desteklenmektedir. Hizmetleri oluşturan ve siber alanın temel özelliklerini destekleyen mantıksal katmanda sürekli yeni bileşenler oluşmaktadır. Bilgi katmanı ise siber ortamda saklanan, iletilen ve dönüştürülen bilgileri ifade etmektedir. Sonuncu katman olan kullanıcılar katmanı siber alanda faaliyette bulunan, katılan - iletişim kuran, bilgi alışverişinde bulunan, kararlar alıp planlar yapan, hizmet ve yetenekleriyle siber alanın kendisini dönüştüren kişileri ifade etmektedir (Almeida, 2016: ss.6-8).

2.3. Siber Uzay ve İnsan Haklarının İncelenmesi

Siber uzayda gerçekleştirdiğimiz faaliyetlerin olumlu ve olumsuz olmak üzere iki yönü bulunmaktadır. Bu alanda bilgiye erişim, fatura ödemeleri, bankacılık işlemleri, alışveriş, eğitim, sosyal medya kullanımı, iletişim gibi birçok fırsat bulunmaktadır. Ancak diğer taraftan bu alanda yer alan kullanıcılar açısından hak ihlalleri ortaya çıkmaktadır. Siber uzayda kullanabileceğimiz haklar ve bu hakların ihlallerine yönelik girişimler güvenlik yaklaşımı perspektifinde değerlendirilmektedir.

Teknolojik gelişmelere bağlı olarak değişen bu yeni güvenlik tehditleri siber uzayda karşımıza çıkmaktadır. Temel hak ve özgürlüklerin ihlal edilmesi bu alanda yer alan aktörlerin davranışlarına göre şekillenmektedir. Kimi zaman bireysel ihlaller gerçekleşirken kimi zaman bir grup, şirket, organizasyon ya da devlet tarafından gerçekleştirilen ihlaller söz konusu olmaktadır. Ancak bu noktada daha önemli olarak karşımıza çıkan durum bu ihlalcilerin çoğu zaman tespit edilememesidir. Sorumlular tespit edilse bile gerekli yaptırımları uygulayacak uluslararası mekanizmaların eksikliği göze çarpmaktadır (Ermiş, 2015).

Uluslararası sistemin aktörleri nasıl tarihsel süreç içerisinde değişime ve gelişime uğrayarak günümüze kadar çeşitlilik göstermekte ise siber uzay alanının da kendine has bazı aktörleri bulunmaktadır. Bu aktörler kimi zaman sistemin içindeki bir hatadan kaynaklanan ve durumdan haberi dahi olmayan bireylerden oluşuyorsa kimi zamanda sistematik bir biçimde bilinçli ve yaptıklarının ne gibi sonuçlar doğuracağını bilen kimselerden oluşmaktadır.

Bunlar sırasıyla sıradan kullanıcılar, ulusal menfaatleri göz önünde bulunduran ve politik, ekonomik, askeri, teknik motivasyonlara sahip ve devlet destekli yapılar, daha çok kişisel bilgileri ele geçirmeye ve bundan büyük menfaatler sağlamaya yönelik kurulmuş olan suç örgütleri, çeşitli ideolojilerin ve fikirlerin propagandasını yapma amacı güden haktivistler, daha çok eski çalışan ya da işten çıkarılan kişilerden oluşan ve intikam amacı güdenlerin oluşturduğu kişiler, hackerlar kadar bilgi sahibi olmasalar da sistemdeki açıklardan yararlanarak menfaat elde etme amacı güden script kiddie'ler, sistemde tam olarak nasıl hareket etmesi gerektiğini bilmeyen ve bu nedenle bir takım hatalara neden olanlar olarak ifade edilebilir (İbrahim Korucuoğlu, http://www.siberoloji.com, 15.07.2018)**.**

Dünyada yaklaşık dört milyar internet kullanıcısının olduğu göz önünde bulundurulduğunda ne kadar büyük bir kitlenin etkileşim halinde olduğu ortaya çıkmaktadır (Internet World Stats, https://www.internetworldstats.com/stats.htm, Erişim Tarihi: 15.07.2018). Böyle bir alanda meydana gelen iletişim ve etkileşim sonucunda insan haklarına yönelik ihlallerin de olağanüstü bir boyuta ulaştığı görülmektedir. Siber uzayın sanal olmanın ötesinde artık gündelik yaşamları kontrol eden, düzenleyen ve belirleyen bir işlevi bulunmaktadır. İnsanların büyük çoğunluğu günlük yaşantısının büyük bir kısmını siber alanda geçiriyor. İnsan hakları açısından bakıldığında siber uzayda karşımıza çıkan çok çeşitli hak ihlalleri bulunmaktadır. Kullanıcılar açısından yaşanan bu mağduriyetleri önlemek için siber alanda bir güvenlik ihtiyacı doğmuştur. Çalışmanın sonraki kısımlarında bu ihlaller incelenmiş ve siber güvenliğin sağlanması açısından geliştirilen bilişim hukukunun temel prensipleri ele alınmıştır.

2.4. Siber Uzayda İnsan Hakları İhlalleri

Siber uzayda yaşanan insan hakları ihlalleri çok geniş bir alana yayılmaktadır. İnsan hakları sadece temel hak ve özgürlüklerden oluşmamaktadır. Sosyal, ekonomik ve kültürel haklar ve üçüncül kuşak haklarda insan haklarının içerisinde yer almaktadır. Bu nedenle siber uzayda meydana gelen ihlaller bu çerçevede değerlendirilmelidir. Peki, bu ihlaller nelerdir? Bir ihlalin söz konusu olması için hem ulusal hem de uluslararası anlamda yaptırımları olan sözleşmeler, anlaşmalar, kanunların varlığı ve anayasalarda hukukun üstünlüğü ilkesine dayalı hakların belirlendiği kararların alınmış olması gerekmektedir.

Genel olarak bakıldığında siber uzayda karşımıza çıkan ihlaller şunlardır: Özel hayatın gizliliğini ihlal etmek, haberleşme ve iletişimin gizliliğini ihlal etmek, nitelikli hırsızlık, kredi kartı ve banka dolandırıcılığı, bilgisayar sabotajı, çocuk pornografisi, tehdit ve şantaj, siber zorbalık, siber terörizm, casusluk, insan kaçakçılığı, organ ticareti, fuhuş, kişisel verilere izinsiz erişim sağlamak, başka bir devletin verilerini ele geçirmek, hacking (hackleme), bilişim sistemine izinsiz girmek, sistemi engellemek veya bozmak, verilerin değiştirme ya da yok etmek, ifade, görüş özgürlüğünü ihlal etmek, nefret söylemi vb. olarak sıralanabilir (Bilgi Teknolojileri ve İletişim Kurumu, http://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu-detay-58.html, Erişim Tarihi: 17.07.2018).

Sanal ortamda insan hakları mevzuatının en önemli parçaları, ifade, görüş, kişi özgürlüğü ve mahremiyet hakkıdır. İnternetin de bu hakların kullanımı için vazgeçilmez bir araç haline geldiği görülmektedir. İfade özgürlüğü, kişi güvenliği ve özgürlüğü, özel yaşamın gizliliği ve kişisel verilerin korunması sık sık ihlal edilen hakların başında gelmektedir. İletişim ve bilişim alanındaki teknolojilerin artmasına paralel bir biçimde ortaya çıkan bu güvenlik sorunları geç te olsa bilişim hukukunun doğmasını sağlamıştır. İnsan hakları ve siber uzay alanında ortak bir güvenlik prensibi oluşturulacaksa bu erişilebilirlik, gizlilik ve bütünlük ilkeleri ile mümkün olacaktır (Can ve Akbaş, 2014: ss.17-18).

Bilişim yolları kullanılarak; terör örgütlerinin faaliyetlerini sanal dünyaya taşımaları, interaktif altyapının dolandırıcılık, hırsızlık amacı ile kullanılabilir hale gelmesi, çocuk pornografisinin yaygınlaşması, nefret söylemlerinin artması gibi nedenler bilişim hukukunun doğuşunu hızlandıran gelişmeler olmuştur. Ancak uluslararası bir bilişim hukukunun varlığından söz etmek oldukça zordur. Uluslararası çalışmalarda devletler daha çok çıkar odaklı hareket etmektedir. Bu nedenle bilişim hukuku alanında yapılan çalışmalar ulusal boyutta kalmaktadır. Uluslararası genel geçer bir bilişim hukukuna yönelik çalışmalarda ise devletler bu kararları daha çok tavsiye niteliğinde görmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2018).

Siber uzayda gerçekleşen faaliyetler interneti kullanan herkes açısından olumlu ya da olumsuz sonuçlar doğurabilmektedir. Örneğin bir nükleer tesisi hedef alan terör örgütünün o tesisi hacklemesi, etkileri açısından küresel bir nitelik taşımaktadır. İnternet üzerinden IP bilgilerinize sahip olan birisi illegal faaliyetlerde bu bilgileri kullanabilmektedir. Sosyal medya üzerinden paylaştığınız bir fotoğrafa sizi tanısın veya tanımasın yüz binlerce hakaret gelebilmektedir. Bilgisayarınıza ya da cep telefonunuza gelen bir e-postaya tıkladığınızda siz daha farkında bile olmadan kameranıza, kişisel bilgilerinize, fotoğraflarınıza, mesajlarınıza erişip özel hayatınızın gizliliği ihlal edilebilmektedir. Üstelik bununla kalmayıp bu bilgiler şantaj amaçlı kullanılabilmektedir (Arısoy, 2007: s. 167).

Siber uzayda gerçekleşen suçların, ihlal edilen hak ve özgürlüklerin kapsamı oldukça geniştir. Bu girişimler ise en çok internetin karanlık yüzü olarak adlandırılan DeepWeb'te karşımıza çıkmaktadır. Deep Web internet üzerinde normal web tarayıcılarımızla ulaşılamayan ve arama motorlarında görüntülenmeyen internet sitelerinin genel adıdır. Genelde içeriklerin illegal

olduğu bu ortama giriş yapabilmek için çoğunlukla TOR Browser kullanılmaktadır (Sui vd. 2015: ss. 6-7).

İnternet dünyasının çok geniş olduğu bilinse de bizim anladığımız ve bildiğimiz kısmı tüm internet dünyasının sadece %4'üdür. Kalanı ise Deepweb olarak ifade edilen boyutlardır. Tek bir boyut değil, boyutlar söz konusudur. Yani katman katman daha derine inmek mümkündür. Belli bir noktadan sonrası için özel cihazlar gerekir ve çok az insan bu boyuta erişebilmektedir. Deep Web kavramı için buzdağının görünmeyen yüzü tanımı yapılmaktadır. İllegal faaliyetlerin çoğunluğu ise Deepweb olarak değil Darkweb olarak adlandırılmaktadır. İnsan kaçakçılığı, fuhuş, uyuşturucu ticareti, kiralık katil ve hırsızlık ilanları, sadizm ve mazoşizme yönelik içerikler, çocuk pornografisi, stratejik ve gizli belgelerin yayınlanması veya satılması, sahte kimlik ve pasaport düzenleme faaliyetleri, patlayıcı madde yapımı içerikleri, insanlar ve hayvanlar üzerinde yasal olmayan tıbbi deneyler vs. gibi faaliyetler bulunmaktadır. (Zinnur Yeşilyurt, http://ab.org.tr/ab15/bildiri/249.pdf, Erişim Tarihi: 26.07.2018).

Bu durumun nedenleri arasında, Bilgisayar teknolojilerinin ve sistemlerinin yaygın bir şekilde kullanılması, siber alanda yüksek kazançların daha az riskle elde edilme imkânının bulunması, kanunlarda siber güvenlikle ilgili boşlukların olması, şikâyet bilincinin yaygınlaşmaması, siber alana yönelik yeterince bilgiye sahip olmadan faaliyetlerde bulunulması, suçları gerçekleştiren kişilerin eylemlerinin yaptırımsız kalacağını düşünerek rahat hareket etmesi, suçun işlendiği yer ve zamanın tespit edilmesinin çok zor olması, gerçekleştirilen eylemlerde kimliği gizlemenin kolay olması gibi faktörler sayılabilir (Bilgi Teknolojileri ve İletişim Kurumu, 2018).

Siber uzayda meydana gelen insan hakları ihlalleri ve bu ihlallerin boyutu tüm aktörler açısından değerlendirilmelidir. Örneğin sanal ortamda kişisel verilerin çoğunun özel şirketler tarafından depolanması, alınıp satılması haklarımızın ihlal edildiğini göstermektedir. Örneğin bilmediğimiz veya tanımadığımız firmalardan aldığımız kısa mesajlar, e-postalar, bilgilerimizin üçüncü kişilerle paylaşıldığını kanıtlar niteliktedir. Devletlerin de güvenlik kapsamında kişisel bilgilerimizi kullanması, hesaplarımızı kontrol etmesi, telefonlarımızı dinlemesi, internet üzerinde gerçekleştirmiş olduğumuz faaliyetlere izinsiz ulaşması yine ihlallere örnek olarak gösterilebilir. (International Telecommunication Union- ITU, 2006).

3. Siber Uzayda İnsan Haklarını Koruma Mekanizmaları

Siber uzayda meydana gelen ihlallerin çözüme kavuşturulması insan hakları kavramlarının siber güvenlik ile bütünleştirilmesi ile gerçekleştirilebilir. İnternetin kullanıcıları açısından sadece devletleri değil herkesi kapsayacak ortak bir siber güvenlik anlayışı ile insan hakları korunmalıdır.

Siber uzayda güvenlik açısından yaşanan problemler sadece bireyleri değil şirketleri ve devletleri de endişelendirmektedir. Siber alanda bir insan haklarından ve siber güvenlikten söz edilecekse her şeyden önce ortak ilkeler ve prensiplerin benimsenmesi ve internet etiğinin oluşturulması gerekmektedir. Etik kavramı günümüzde tanımlanması en zor alanlardan birisidir. Bu nedenle siber uzaydaki etik kurallarının oluşturulması son derece zor ve zahmetli bir iştir. Her ne kadar internet etiği ve hukuku alanında yapılan çalışmalar yeni bir süreç olup yavaş ilerlese de hem insan haklarını korunması hem de siber uzayda güvenliğin sağlanmasına yönelik olumlu gelişmeler olarak karşımıza çıkmaktadır (Weber, 2016: ss. 2-3). İnternet etiği kısaca internet vasıtasıyla gerçekleştirilen işlemlerde davranışları belirleyen kurallar olarak tanımlanmaktadır. İnternetin küresel çapta yönetilmesini sağlayacak bir mekanizma kurulması günümüzde oldukça zor olarak görülmektedir. İnternet Etiği, kontrol edilmesi son derece güç olan internet dünyası için uluslararası düzeyde alınacak önlemler ve ilkelerin belirlenmesi, ortaya çıkabilecek sorunların çözülmesine katkı sağlama amacıyla ortaya çıkmıştır. Çalışmanın bundan sonraki kısmında internet ya da diğer bir adıyla bilişim etiğine yönelik atılan adımlar incelenmektedir (Aydın, 2013: s.102).

İnternet olgusu hemen her yere sızmış olduğundan yarattığı risk ve zararlar etik tartışmalarının temelini oluşturmaktadır. Daha önce ifade edilen bu risk ve zararlar insan haklarına yönelik ihlallere neden olmaktadır. Devletlerin bile vatandaşlarının bilgilerine izinsiz erişim sağlayabildiği, verilere erişim yasağı koyduğu bir alanda haklarımız ne kadar güvence altında olabilir? İnternet etiği işte bu ve buna benzer durumlarda ihtiyaç duyduğumuz güvenlik ilkelerinin belirlenmesine katkı sağlayan bir kavram olarak karşımıza çıkmaktadır. Bu tarz sorunların çözülmesine yönelik girişimler gelişmiş ülkelerin, bölgesel ve uluslararası kuruluşların atmış olduğu adımlarla açıklanabilir. Birleşmiş Milletler, Avrupa Konseyi, G8, OECD bu örgütlerin başında gelmektedir.

İnternet Etiği konusundaki adımlardan ilki 1958 yılında Bilgisayar Etik Enstitüsü (Computer Ethics Institute) tarafından yayınlanan 10 ilke ile atılmıştır. Bilgisayar kullanımı konusunda etik prensipler ortaya koyan bu çalışma da başkalarının bilgisayarını izinsiz kullanmamak, bilgisayarı hırsızlık için kullanmamak, bilgisayara zarar vermemek, bedelini ödemediğimiz yazılımı kullanmamak ve kopyalamamak, bilgisayarı saygı duyulacak işlerde kullanmak gerektiği ifade edilmektedir. (Bilgisayar Etik Enstitüsü, http://computerethicsinstitute.org/publications/tencommandments.html, Erişim Tarihi: 29.07.2018).

Çalışmanın bundan sonraki kısmında internet etiği ve siber uzayda insan haklarını korumak için Avrupa Birliği ve Birleşmiş Milletlerin çalışmaları ile birlikte uluslararası örgütlerin çalışmaları ve ulusal eylem planları açısından öne çıkan çalışmalar incelenmektedir.

3.1. Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa Konseyi Siber Suç Sözleşmesi (Council of Europe- Convention on Cybercrime) uluslararası açıdan siber güvenlik ve insan haklarını gözeten en önemli sözleşme olup 23 Kasım 2001 tarihinde imzalanmıştır. 1 Temmuz 2004 yılında yürürlüğe giren sözleşme Türkçe olarak "Sanal Ortamda İşlenen Suçlar Sözleşmesi" şeklinde ifade edilmektedir. Türkiye'de bu sözleşmeyi 22 Nisan 2014 tarihinde TBMM'de kabul ederek yasalaştırmıştır. Sözleşme, özellikle telif hakkı, bilgisayarla ilgili dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlalleri, internet ve diğer bilgisayar ağları yoluyla işlenen suçlarla ilgili konuları ele almaktadır. Ayrıca bilgisayar ağlarının aranması ve durdurulması gibi bir dizi yetkiyi ve prosedürleri içermektedir (European Cybercrime Convention, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, Erişim Tarihi: 24.07.2018).

Sözleşmenin giriş kısmında öngörülen temel amacı, özellikle uygun yasaları benimseyerek ve uluslararası işbirliğini ilerleterek, toplumu siber suçlardan korumayı amaçlayan ortak bir ceza politikası izlemektir. Sözleşme siber güvenliğin sağlanması noktasında ulusal mevzuatların uyumlulaştırılması amacı gütmektedir. Sözleşme, taraf olan devletlere sözleşmede yer alan hukuki düzenlemeleri iç hukuklarına uyarlama yükümlülüğü getirmiştir (Önok, 2013: ss. 1242-1243).

3.2. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı

13 Mart 2004 yılında kurulan Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) Avrupa Birliğine üye olan devletlerin ulusal ağ ve bilgi güvenliğine katkıda bulunmak, siber kültürün geliştirilmesini sağlamak, kritik altyapıların ve bilgi sistemlerinin siber saldırılardan korunmasını sağlamak amacıyla kurulmuştur. Temel hedefi ise bilgi güvenliği ve ağ güvenliğini sağlayarak AB iç pazarının düzenli bir biçimde işleyişine katkıda bulunmaktır (European Union Agency for Network and Information Security, https://www.enisa.europa.eu/about-enisa/mission-and-objectives, Erişim Tarihi: 22.07.2018).

3.3. İnternet Hakları ve İlkeleri Dinamik Koalisyonu

2005 yılında Tunis Zirvesi'nde internetin ve insan haklarının bir arada ele alınması gereken alanlar olduğu fikri ortaya atılmıştır. Bu alanda çalışma yapması için iki birim oluşturulmuştu. Bunlardan birisi olan İnternet Hakları Bildirgesi Dinamik Koalisyonu (Internet Rights and Principles Dynamic Coalition) internet üzerinde oluşturulacak kuralların ve yönetim ilkelerinin belirlenmesi için çalışmalara başlamıştır. 2009 yılına gelindiğinde yapılan çalışmalar sonucunda internette insan hakları ve ilkeleri şartı oluşturulmuştur. Bu şartın pratik bir biçimde kullanılabilmesi ve belirli bir insan hakları standardına ulaşabilmesi için alanında uzman kişiler tarafından ana hatları belirlenmiştir. Bu amaçla çeşitli taslak ve versiyonlar oluşturulmuş bunlar geniş katılımcılardan oluşan tartışmalarla geliştirilmiştir. 2011 yılında ise bu konuda yapılan çalışmalar nihayete erdirilmiş ve "10 Etkili İlke" adıyla yayınlanmıştır(The Charter of Human Rights and Principles for The Internet, https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf, Erişim Tarihi: 22.07.2018).

İnternet ortamında ya da sanal ortamda insan haklarına saygı konusunda temel prensipler ortaya koyan bu ilkeler, hakların eşitliği ve evrensel niteliğine vurgu yapmaktadır. Ayrıca herkes için güvenilir ve erişilebilir internet hakkı, fikir ve ifade özgürlüğü, internet aracılığıyla organize olabilme hakkı, bilgiye erişimin sağlanabilmesi için sansürün ortadan kaldırılması, kişisel verilerin korunması ve özel hayatın gizliliğinin ihlal edilmemesi, kültürel çeşitliliğin teşvik edilmesi, internetin tüm paydaşları için eşit fırsatlar sunması ve hukukun üstünlüğü prensibine dayalı açık ve şeffaf bir niteliğinin olması gibi konuları ifade etmektedir (Internet Rights and Principles Coalition, http://internetrightsandprinciples.org/site/about/, Erişim Tarihi: 26.07.2018).

İnternet Hakları ve İlkeleri Dinamik Koalisyonu, insan hakları standartlarını internet üzerinden yönetmek ve internet yönetimi süreçlerini ve sistemlerini geliştirmek için çalışmaktadır. Koalisyon üyeleri, Internet'te hakların çerçevelendirilmesi ve uygulanmasına yönelik süreçleri ve araçları tanıtmak için bireysel ve ortak olarak çalışmaktadırlar. Yayınlamış oldukları ilkeler farklı dillere çevrilmekte ve BM, Avrupa Birliği gibi organizasyonlarca desteklenmektedir (The Charter of Human Rights and Principles for The Internet, 2014).

3.3. Avrupa Siber Suç Merkezi (EC3)

Europol, Avrupa Siber Suçlar Merkezi'ni (European Cybercrime Center-EC3) 2013 yılında AB'deki siber suçlara karşı kanun uygulama sorumluluğunu güçlendirmek ve böylece Avrupalı vatandaşların, işletmelerin ve hükümetlerin çevrimiçi suçlardan korunmasına yardımcı olmak için kurmuştur. Kurulmasından bu yana, EC3 siber suçlarla mücadelede önemli bir katkı yapmıştır (Europol – European Cybercrime Center, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, Erişim Tarihi: 24.07.2018).

3.5. Birleşmiş Milletlerin Çalışmaları

Birleşmiş Milletler 1980'li yıllardan itibaren siber güvenlik çalışmaları yapmaktadır. BM Genel Kurulu "Küresel Siber Güvenlik Kültürünün Oluşturulması ve Kritik Bilgi Altyapılarının Korunması (Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures)", "Bilgi Teknolojilerinin Suç Amaçlı Kötüye Kullanımı İle Mücadele (Combating the Criminal Misuse of Information Technologies)" kararlarında üye ülkelere alması gereken tedbirleri açıklamıştır (United Nations General Assembly, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf, Erişim Tarihi: 29.07.2018).

Özellikle siber kültürün oluşturulması noktasında belirlemiş olduğu farkındalık, sorumluluk, etik, demokrasi, risk tasarımı, güvenlik yönetimi ilkeleri vs. önemlidir. Söz konusu olan bu ilkeler OECD tarafından da kabul edilmiş "Bilgi Sistemleri ve Ağların Güvenliğine İlişkin

OECD Rehber İlkeleri" (OECD Guidelines for the Security of Information Systems and Networks) olarak adlandırılmıştır (OECD, https://www.oecd.org/sti/ieconomy/15582260.pdf, Erişim Tarihi: 29.07.2018).

BM'ye bağlı Bilgi ve İletişim Teknolojileri Görev Gücü 2002 yılında yayınlamış olduğu "Bilgi Güvenliği- Siber Tehditlerin ve Siber Güvenliğin Keşfedilmemiş Bölgelerinde Hayatta Kalabilme Kılavuzu (Information Security: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security)" ile güvenlik olaylarına müdahale edecek mekanizmalarını, siber güvenlik sorunlarına yönelik çözüm önerilerini ortaya koyması bakımından önemlidir. BM, bilgi güvenliğinin sağlanması açısından Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (IMPACT) adıyla faaliyet gösteren bir platform oluşturmuştur. Ayrıca BM'ye bağlı olarak faaliyet gösteren bir uzmanlık kuruluşu olan Uluslararası Telekomünikasyon Birliği (ITU) de bilgi güvenliği ile ilgili çalışmalar yürütmektedir. Bunların yanı sıra BM Genel Sekreterliği, İnternet Yönetişim Formunun düzenlenmesi görevinde bulunmaktadır (Güngör, 2015: ss.58-59).

Bu forumun amacı internet konusunda ilgili devletlerin altyapılarını geliştirmek, siber güvenlik sorunlarına yönelik tecrübe paylaşımında bulunmak, internetin güvenliğini sağlayacak politikaların hayata geçirilmesini sağlayacak çalışmalar yapmak olarak sıralanabilir. BM uluslararası bir sözleşme ortaya koyamamıştır ancak bu konuda yapılacak çalışmaları desteklemektedir. Özellikle Avrupa Siber Suç Sözleşmesini destekleyen bir tutum takınmaktadır (Ünver, 2011: ss.5-10).

Dünyada siber güvenlik ile ilgili çalışmalar yürüten diğer örgütler ve kurumlar şunlardır: Asya-Pasifik Ekonomik İşbirliği (APEC), Güneydoğu Asya Ülkeleri Birliği (ASEAN), Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST), Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE), Uluslararası Elektroteknik Komisyonu (IEC), Internet Mühendislik Görev Gücü (IETF), INTERPOL, Amerikan Devletleri Örgütü (OAS), Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD). (Network World, https://www.huffingtonpost.com/2010/08/05/most-influential-cybersec_n_671690.html, Erişim Tarihi: 01.08.2018).

Ulusal siber güvenlik stratejisi yayınlayan bazı ülkeler şunlardır: ABD, Almanya, Arnavutluk, Avusturya, Azerbaycan, Birleşik Krallık, Belçika, Çin Halk Cumhuriyeti, Çek Cumhuriyeti,

Danimarka, Estonya, Finlandiya, Fransa, Hırvatistan, Hindistan, Hollanda, İspanya, İsrail, İsviçre, İtalya, İzlanda, Japonya, Kanada, Katar, Letonya, Litvanya, Lüksemburg, Macaristan, Malezya, Norveç, Pakistan, Polonya, Portekiz, Romanya, Rusya, Slovakya, Slovenya, Suudi Arabistan, Türkiye, Ukrayna. (NATO Cooperative Cyber Defence Center of Excellence, https://ccdcoe.org/cyber-security-strategy-documents.html, Erişim Tarihi: 01.08.2018)

Genel olarak bakıldığında siber uzayda insan haklarının korunmasına yönelik yapılan çalışmaların daha çok ulusal ya da bölgesel nitelikli olduğu görülmektedir. Özellikle uluslararası alanda işbirliğinin azlığı ve uluslararası bir koruma mekanizmasının oluşturulamaması devletlerin ulusal çıkarlarına öncelik veren tutumlarından kaynaklanmaktadır. Her devletin siber güvenlik kavramına farklı anlamlar ve tanımlamalar getirmesi, terminolojik ve teknik yetersizlikler bu sorunun derinleşmesine neden olan diğer faktörlerdir. Çalışmanın bu bölümünde siber uzayda insan haklarını korumak, dolayısıyla siber güvenliği sağlamak için yapılan çalışmaların ulusal ve uluslararası boyutları incelenmiştir. Çalışmanın bundan sonraki kısmında genel değerlendirmeler ışığında ulaşılan sonuçlar ve öneriler sunulacaktır.

SONUÇ

Bilgisayar ağlarının artması ve bilgi teknolojilerinin yayılması, dünyayı her zamankinden daha çok birbirine bağlamaktadır. 2030'da İnternet kullanıcılarının 5 milyar civarında olması beklenmektedir. O zamana kadar, dünya nüfusunun % 80'inin mobil bağlantıya sahip olacağı ve % 60'ının geniş bant erişimden yararlanacağı düşünülmektedir. Bu nedenle internet yaşadığımız dünyayı, tüketim hızını ve şeklini daha da geniş bir ölçüde şekillendirecektir (Council of Europe, http://www.consilium.europa.eu/en/policies/cyber-security/ Erişim Tarihi: 28.07.2018). Dijital çağ zenginlik, bilgi ve özgürlük açısından milyarlarca insana büyük fayda sağlamaktadır. Bu nedenle, internetin güvenliği ve istikrarı ve veri akışlarının bütünlüğü, devletler, şirketler, bireyler için giderek önem kazanmaktadır.

Siber uzay ve insan hakları birbirinden farklı alanlar olarak görülebilir. Ancak bu alanlar birbirini kapsamakta ve karşılıklı olarak etkileşim içerisinde bulunmaktadır. Siber alanın gün geçtikçe genişleyen yapısı insan hakları ihlallerinin de artmasına neden olmaktadır. Özellikle bu alana yönelik güvenlik anlayışı her aktör tarafından ayrı değerlendirilmektedir. Siber uzayda güvenlik nasıl sağlanacak? Siber uzayda barış tesis etmek mümkün müdür? Siber

uzayda insan hakları savunulabilir mi? Bu soruların cevabını vermek şu an için mümkün görünmese de yaşanılan gelişmeler ve atılan adımlar bize bazı ipuçları vermektedir. Bunlardan hareketle siber uzayda insan haklarının geliştirilmesi için şu sonuçlara ulaşabiliriz:

* Bilişim etiğinin geliştirilmesi için uluslararası işbirliğine yönelik çalışmalar arttırılmalıdır.
* Siber güvenlik ve türevleri (siber suç, siber zorbalık, siber uzay vs.) ile ilgili tanımlama sorunun çözümü için alanında uzman kişilerden oluşan ve herkes için ortak ilkelerin belirlendiği geniş kapsamlı konferanslar düzenlenmelidir.
* Siber uzay, insan hakları, bilişim etiği konusunda özellikle genç kuşağa yönelik eğitim politikalarının hayata geçirilmesini sağlamak. Bu konuda devletin girişimi olabileceği gibi özel sektöründe teşvik edilmesi önemlidir.
* Ulusal düzeyde alınacak güvenlik politikalarında ihmal ve ihlal edilen boşlukların düzenlenmesi sağlanmalıdır. Bu durum devlet ve yurttaşları arasındaki güven probleminin çözümüne de katkı sağlayacaktır.
* Teknolojik gelişmeler ve dijital çağa uyum sağlamak, toplumsal ve kültürel değerlerin zarar görmesini engellemek için siber kültür politikası oluşturmak,
* Siber uzayda insan haklarını korumak için teknik bilgi, altyapı çalışmaları ve risk analizlerini ölçecek birimlerin kurulmasını sağlamak
* Küresel ölçekte gerçekleştirilecek bu çalışmalar temelde insan haklarına, hukukun üstünlüğüne, uluslararası hukuk ilkelerine sıkı sıkıya bağlı bir şekilde hayata geçirilmelidir. Ayrıca siber politikalar özgürlük ve güvenlik arasında sürdürülebilir bir denge içerisinde hayata geçirilmelidir.

Sonuç olarak insan haklarının, ortaya çıkışından günümüze kadar olan tarihsel süreçte çeşitli aşamalardan geçtiği görülmektedir. Bu nedenle çalışmada insan haklarının dinamik bir kavram olarak değişim ve gelişim süreci ele alınmıştır. Diğer yandan siber uzay kavramının tarihsel arka planı verilerek açıklanmaya çalışılmış, siber uzayın aktörleri ve katmanları incelenmiştir. Siber uzay ve insan hakları arasındaki ilişkinin bağlantıları Soğuk Savaş ve sonrasındaki rekabetçi ortam bağlamında ele alınmıştır.

Teknolojik gelişmeler ve özellikle internetin ortaya çıkması, küreselleşme akımı, bilgi toplumuna geçiş gibi önemli noktalar siber uzayın sınırlarını daha da genişletmiştir. Siber uzay fırsatlar ve faydalarla birlikte, tehditler ve risklerin de yer aldığı bir alan olarak karşımıza çıkmaktadır. Bu durum bireylerin, grupların, şirketlerin, devletlerin güvenliğe bakış

açılarını da değişime uğratmıştır. Siber uzayın korunması temelde siber güvenliğin sağlanması ile mümkündür. Ancak siber uzayın başat aktörü olarak görülen devletlerin ve uluslararası örgütlerin evrensel bir siber güvenlik politikası oluşturmak için atacakları adımlarda ulusal çıkarları ve menfaatleri ön plana çıkarması nedeniyle başarısız bir girişim olarak karşımıza çıkmaktadır. Her geçen gün siber uzayda yeni tehdit türleri ortaya çıkmaktadır. Bu durum sadece bireyleri değil devletleri de zor durumda bırakmaktadır. Örneğin siber uzayda potansiyel tehditler içerisinde yer alan siber terör tehlikesi doğurabileceği sonuçlar düşünüldüğünde bile göz ardı edilmemesi gereken alanlardan biri olarak karşımıza çıkmaktadır. Önemli olan, işbirliği için atılacak olan adımların geç kalınmadan büyük felaketler yaşanmadan atılmasıdır. Büyük felaketlerin yaşanmaması açısından vatandaşlarının can ve mal güvenliğini düşünen devletler aynı hassasiyeti siber uzayda ihlal edilen ve göz ardı edilen diğer hak ve özgürlükler içinde göstermelidir.

KAYNAKÇA

ALGAN, Bülent, (2007) *Ekonomik, Sosyal ve Kültürel Hakların Korunması,* Ankara: Seçkin Yayıncılık.

ALMEIDA Virgilio, Cyberspace Governance Concept and Framework, Harward University,https://cyber.harvard.edu/~valmeida/pdf/Lecture2.pdf (20.12.2017)

ARISOY, Mine, (2007) "Hakaret", *Türkiye Barolar Birliği Dergisi*, Sayı 72.

AVRUPA KONSEYİ VE İNTERNET, https://edoc.coe.int/en/index.php?controller=get-file&freeid=6079 (12.12.2017)

AVRUPA KONSEYİ, https://europa.eu/globalstrategy/en/cyber-security (05.01.2018)

AYDIN, İnayet, Çocuk, İnternet ve Etik, https://www.researchgate.net/publication/316473196_Cocuk_Internet_ve_Etik, (18.12.2017)

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

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, Bilişim Hukuku, http://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu-detay-58.html (17.12.2017).

BİLGİSAYAR ETİK ENSTİTÜSÜ, http://computerethicsinstitute.org/publications/tencommandments.html (22.12.2017)

BRYANT, Rebecca, (2001) "What Kind of Space is Cyberspace?", *Minerva - An Internet Journal of Philosophy*, Vol. 5.

CAN, Özgü ve Fatih Akbaş, (2014) "Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması", *Tübav Bilim Dergisi*, Cilt: 7, Sayı: 2.

CHAPMAN, Garry, (2003) "An Introduction to the Revolution in Military Affairs", http://www.lincei.it (Erişim Tarihi: 24.07.2018).

CINGI, Aydın (2009) *Sora Sora Demokrasi*, İstanbul: Kalkedon Yayınları.

DARICILI, Ali Burak, (2017) "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi", *Uluslararası Çalışmalar Dergisi*, Cilt 1, Sayı 1.

ENGİN, Zeynep Özlem Üskül, (2014) " Birey Kavramının Gelişimi ve İnsan Hakları", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt 72, Sayı 1.

ERENDOR, M.E., "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", *Cyberpolitik Journal*, vol.1, no.1, pp.114-133, 2017.

ERMİŞ, U. (2015) "Siber Caydırıcılık: Teoriği Kolay, Pratiği Zor", https://siberbulten.com/makale-analiz/siber-caydiricilik-teorigi-kolay-pratigi-zor/ (Erişim Tarihi: 28.07.2018).

EUROPOL – EUROPEAN CYBERCRIME CENTER, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (18.12.2017)

GIBSON, William, (1984) *Neuromancer*, Grafton Books - Collins Publishing Group, London, 1984.

GÜNGÖR, Murat, (2015) *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, T.C. Kalkınma Bakanlığı: Bilgi Toplumu Dairesi Başkanlığı, Uzmanlık Tezi, Ankara.

HUFFPOST, Most Influential Cyber Security Organizations in The World, https://www.huffingtonpost.com/2010/08/05/most-influential-cybersec_n_671690.html, (Erişim Tarihi: 01.08.2018)

INTERNET RIGHTS AND PRINCIPLES COALITION, http://internetrightsandprinciples.org/site/wp-content/uploads/2017/03/IRPC_Booklet_Turkish_final.pdf (23.12.2017)

ITU- International Telecommunication Union, (2006), *Research on Legislation in Data Privacy, Security and the Prevention of Cybercrime*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CRIM-2006-PDF-E.pdf, (Erişim Tarihi 26.07.2018).

ITU- International Telecommunication Union, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf (Erişim Tarihi: 29.07.2018).

KABOĞLU, İbrahim Ö., (2011) *Anayasa Hukuku Dersleri*, İstanbul: Legal Yayınları.

KILIÇ, Yavuz, (2015) " Hobbes, Locke ve Rousseau'da Doğa Durumu Düşüncesi", *Temaşa Erciyes Üniversitesi Felsefe Bölümü Dergisi*, Cilt 2, Sayı 2.

KIVILCIM, Fulya, (2013) "Küreselleşme Kavramı ve Küreselleşme Sürecinin Gelişmekte Olan Ülke Türkiye Açısından Değerlendirilmesi", *Sosyal ve Beşeri Bilimler Dergisi*, Cilt 5, Sayı 1.

KORUCUOĞLU, İbrahim, Siber Uzay Tanımı ve Aktörleri, https://siberoloji.github.io/siber-uzay-tanimi-aktorleri/ (16.12.2017).

KÜÇÜKALİ, Rıdvan, Hasibe Akbaş, (2016) "Bir Haklılaştırma Zemini Olarak Doğal Hukuk", *MSKU Eğitim Fakültesi Dergisi*, Sayı 3.

LEINER, M.Berry, *A Brief History of the Internet*, Internet Society, https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf (18.12.2017).

MALHOTRA, Sona, (2016) "Cyber Crime- Its Types, Analysis and Prevention Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6, Issue 5.

NATO Cooperative Cyber Defence Center of Excellence, https://ccdcoe.org/cyber-security-strategy-documents.html, (Erişim Tarihi: 01.08.2018).

OECD, Guidelines for the Security of Information Systems and Networks Towards a Culture of Security, https://www.oecd.org/sti/ieconomy/15582260.pdf, Erişim Tarihi: 29.07.2018).

ÖNOK, Murat, Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadele ve İşbirliği, http://dergipark.gov.tr/download/issue-file/517 (18.12.2017).

RUDE George, (2015) *Fransız Devrimi,* İstanbul: İletişim Yayınları.

SEZGİN, Murat, (2016) "Bilişim Devrimi, Sibernetik İletişim ve Halkla İlişkiler", *Sosyal Bilimler Enstitüsü Dergisi*, Karabük, Cilt: 6, Sayı: 2.

SUI, Daniel, vd., (2015) "The Deepweb and The Darknet: A Look Inside Internet's Massive Black Box", *Wilson Center*, Stip 3.

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI, (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.*

TOKU, N. (2004) Felsefe Yazıları, İstanbul: Yeni Zamanlar Yayınları.

TURHAN, Aydın, (2013) "İnsan Hakkı Kuşakları Arasındaki Tamamlayıcılık İlişkisi", *İstanbul Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 4, Sayı 2.

TURHAN, Oğuz, (2006) *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)*, Devlet Planlama Teşkilatı: Planlama Uzmanlığı Tezi, Ankara.

ÜNAL Şeref, (1994) "İnsan Haklarının Tarihi, Felsefi ve Hukuki Temelleri", *Ankara Barosu Dergisi*, Ankara.

ÜNAL, Yenal, (2009), "Bilgi Toplumunun Tarihçesi", *Tarih Okulu Dergisi*, Sayı: 5.

ÜNAL, A. N., Milli Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü, https://www.researchgate.net/profile/Ahmet_Unal6/publication/321125904_Milli_Guc_Unsur

larinin_Belirlenmesinde_Siber_Uzay_Faktoru/links/5a0e74b00f7e9b7d4dba66fe/Milli-Guec-Unsurlarinin-Belirlenmesinde-Siber-Uzay-Faktoerue.pdf (20.12.2017).

ÜNVER, Mustafa vd., (2011) Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri, Ankara.

WEBER, Rolf H., (2016) "Global Commission on Internet Governance", *Royal Institute of International Affairs*, No 39.

YEŞİLYURT, Zinnur, DeepWeb, Web'in Karanlık Yüzü, http://ab.org.tr/ab15/bildiri/249.pdf (15.12.2017).

OPINIONS / YORUMLAR

THINKING ON THE CHANGING REPRESENTATION OF MUSIC ON CYBERSPACE

Uğur Zeynep GÜVEN[4]

Abstract

This paper addresses the emerging concept of cyberization of music through a particular focus on the changing representation of music. In this context, the first part presents a historical overview on the representation of music for a better understanding of today's digitalization of music. The second part revolves around the intertwining relationship between technology and society and its impact on cultural preferences and taste in music. The last part focuses particularly on the emerging concept of cyberization of music and questions the ways it transformed the musical representation. The evaluations expose an ever-changing musical representation in our contemporary era, with a lack of live interaction where music followers tend to be influenced by the shared view of the others. Since there is no single and absolute correct way of analyzing the cyberspace for it has become an overarching term used to describe a multitude of aspects of the new communication technologies, the evaluations herein wishes to contribute to the interpretation of music on cyberspace.

Keywords: Cyberspace, music, cultural transformation, technology

SİBER ALANDA MÜZİĞİN DEĞİŞEN TEMSİLİ ÜZERİNE DÜŞÜNMEK

Özet

Bu makale literatüre yeni bir kavram olarak giren müziğin siberleşmesi konusunu müziğin temsilinin dönüşümü üzerinden ele almaktadır. Bu doğrultuda, ilk olarak günümüzde müziğin dijitalleşmesini daha iyi kavrayabilmek için müziğin temsil edilme biçimleri üzerine tarihsel bir değerlendirme sunulmaktadır. Makalenin ikinci kısmı teknoloji ve toplum arasındaki karşılıklı ilişkiyi ele alıp, bu ilişkinin kültürel tercihler ve müzik beğenileri üzerindeki etkileri üzerinde durmaktadır. Son bölüm ise, müziğin siberleşmesi kavramına odaklanarak kavramın müziğin temsili üzerindeki dönüştürücü etkisini sorgulamaktadır. Değerlendirmeler, günümüzde müzik takipçilerinin sanal olarak paylaşılanlardan etkilendiği bir ortamda, gerçek

[4] Doç. Dr., İstanbul Medeniyet Üniversitesi, Edebiyat Fakültesi, Sosyoloji Bölümü. E-posta: zeynep.guven@medeniyet.edu.tr

ve canlı bir etkileşimden yoksun ve sürekli dönüşen bir müzik temsili açığa çıkarmaktadır. Yeni iletişim teknolojilerinin farklı boyutlarını tanımlamada başvurulan kapsayıcı bir kavram haline gelen siber alanı analiz etmenin tek ve kesin doğrulukta bir yöntemi bulunmadığından, buradaki değerlendirmelerin siber alanda müziğin temsilinin anlamlandırılmasına katkıda bulunması ümit edilmektedir.

Anahtar Kelimeler: Siber uzay, müzik, kültürel dönüşüm, teknoloji

Introduction

Contrary to the common rhetoric of the new media, technology is not a recent concept. Even though, music and technology have always been closely associated since the first musical instruments were constructed, the impact of technology on music has come to the forefront within the past few decades. The new communication technologies and the Web 2.0 era entirely transformed the ways we experience music. The phenomenon of digitalization of music marked a milestone in the ways music is composed, represented, distributed and consumed. The main aim of this paper is thus to question the emerging concept of cyberization of music and to think critically on the changing nature of its representation.

The history of music that runs parallel with social history serves to identify, verify and classify the methods that make up the body of musical representation. The term musical representation includes both explicitly and implicitly the cooperative links and conventions that contribute to the realization of a music performance. In other words, musical representation corresponds to a specific 'art world', as described by Becker (1997), consisting of all the people whose activities are necessary to the production of a work of art. For the sociologists studying art, who are mainly interested in the process of production and representation of an artistic piece, whether a movie, a novel or a symphony, the political economy of the social environment in which they are produced and represented matter the most, especially from a macro-sociological point of view. From this perspective, this essay aims to shed light onto the recent phenomenon of cyberization of music. The first part of this paper offers a historical overview on the representation of music. Then the second part examines the recent social implications of the problematic relationship between cyberspace and society. The third part questions the mechanism of the circulation of digitalized music within the scope of cyberization of music.

A Historical Overview on the Representation of Music

The theories concerning the history and the theory of music is generally based upon the ways the music is composed and represented. Within almost less than a century, the theories on the social and cultural aspects of music began to focus more and more on newly found phenomena such as the impact of artificial intelligence on music. One of the earliest and systematic theoretical framework developed Weber (1958), concerned the technical, economic, and social interrelations between modern music, its instruments and its wider social surrounding. His successors and many other music sociologists also believed that at relatively early cultural levels of human civilizations, alongside purely personal, emotional or aesthetic enjoyment of music there appears music designed for socially significant and practical requirements.

The trajectory of the Western art music that puts forth the changing social uses and functions of music has a remarkable impact on the cultural study of music. For instance, the music of Antiquity was performed both as entertainment and artistic performance in addition to being an important part of religious ceremonies. The division between religious and secular music of the Roman Empire were enlarged upon different styles during the Middle Ages following the rise of polyphonic music. Music continued to develop and evolve into truly an art form, reflecting the clarity, realism, and awareness of the Renaissance era. The following centuries' social and political changes had more apparent impacts on music. For instance, the first half of the Baroque period was characterized by the domination of the aristocracy, whereas the second half of it was designated by the democratization of music especially with the opening of public opera houses and concert halls. The music showed emotional restraint and refinement during the following Classical era, which coincides with a significant historical period of revolutions and declarations of independence. Then, 19th century Romanticism was marked by a spirit of individuality and personal freedom, during which the emphasis shifted from the restraint and formal discipline of the Classical point of view to the emotionalism and individualism. Subsequent to post romanticism and impressionism, the 20th century contemporary music became a scene of artistic revolution mostly against European over-

refinement, symmetry in art, consonance and tonality, where artists began to emphasize self-expression and art as technique rather than as an expression of feeling. These attitudes led to abstraction in art and music, and to a long period of adjustment to the new styles for artists and their audiences. The same period witnessed simultaneously the rise of popular music sphere. This brief history of Western art music presented above (Yates 1994; Say 2006) propounds both explicitly and implicitly the interdependence between the representation of music and the development of technology.

With the advent of music industry, the 'composition' of music started to be replaced by the 'production' of music where the contribution of numerous social actors mattered and overshadowed the role of gifted and genius musicians. Music industry then gravitates to draw from non-familiar, non-western, local and indigenous styles, and started to present new genres on various different music scenes, such as jazz, rock and roll, pop, hip-hop, techno, etc. The history of music not only proposes an unending dialogue between the present and the past but also manifests the need to change and adapt to the social milieu where the music is produced and represented. The music industry, inevitably and strongly affected by the digital revolution, now collaborates with various different digital platforms and needs what cyberspace has to offer.

Technology, Cultural Preferences and Cyberspace

Communication, as an essential sustenance of a society, is the transfer of information from one individual or group to another, whether in speech or through the mass media. Wright (1959) explains that mass media is directed toward relatively large, heterogeneous, and anonymous audiences where messages are transmitted publicly and the communicator tends to be within a complex organization. Today, the mass media composes of traditional media and the new media. The latter expands continuously in a global system of interconnectedness. In this regard, the term cyberspace refers to an information space in which data is configured in such a way as to give the user the illusion of control, movement and access to information, which links together a large number of users that operates in a feedback loop to the operator (Featherstone and Burrows 1995, p.2). Many scholars agree on the fact that it then offers a 'virtual reality', an artificial environment and forces the social actors to engage in a 'computer-mediated communication'. Cyberspace is also capable of creating a milieu for the expression of the self and manifestation of the identity, where one can choose among tons of

different competences, interests, capacities that s/he has, and combines them in different ways, sometimes by regenerating its components.

In this sense, the term cyberspace becomes an object of study, especially within the scope of sociology of communication. Since cyberspace has become a catchall term of different types of electronic communication, aside from social media tools, online news, virtual reality environments, it includes streaming audio and video. One of its most prominent social implications is the construction of web-based communities depending on similar taste in music and in other cultural preferences. Social-networking sites, music sharing sites, blogs, live Internet broadcasting, are among those new cultural communities that are electronic, networked and interconnected.

Kaplan and Haenlein (2010) highlight certain terms in order to better understand these social and cultural characteristics of cyberspace and the complex social relations it produces. One of those concepts is 'social networking' suggesting the grouping of individuals together into specific groups, using online networking services. 'Social bookmarking' on the other hand, is a way of sharing, organizing, searching and managing web pages on the Internet. Internet signifies new ways of doing it globally through the process of coming together toward a common point. Yet, the social actors of the new media, from different social classes, social strata, with different economic, social and cultural backgrounds, display the characteristics of a 'consumer' who also tries to be a 'producer' because anyone can produce and deliver content to a public audience. Within this framework, people tend to share their musical productions as well as their musical preferences on cyberspace.

Towards a Cyberization of Music

The interlinked relationship between technology and music can be seen through the crystallization of new forms of representation of music on cyberspace. The cyberization of music, as a recent phenomenon and an attempt to make sense of digitalized music, has both social and cultural dimensions. As the growth of the Internet and the progress of multimedia technologies, millions of songs have become omnipresent and accessible in digital multimedia

data format. Concerning the latter, the algorithms for the retrieval of MP3 music objects and the appropriation of this new immaterial format have been subjected to interdisciplinary academic researches (i.e. Lui and Tsai, 2001; Magaudda 2011, Alderman 2008). MP3 as a digital compression technology in the sequel of vinyl, cassette and compact disc, entirely transformed the ways music is represented and distributed. This new storage of music, virtual and intangible, enabled a multifaceted and fragmented musical representation. Music streaming applications using large amounts of music data such as on-line music stores, digital music libraries and Internet radios, among many others, started to provide users a supposedly unlimited power of listening.

Music recording takes part within the main title of digital arts, which also include videos, writings and other crafts. It unavoidably raises questions concerning copyright, privacy and security issues. The problems of sustainability and public awareness engagement with arts on the Internet are among other current issues. The questioning of the aesthetic value in it yields to a critique of new media art rather from the perspective of sociology of art. Yet, all kinds of musical acts within new media have their own set of protocols and rituals that can briefly be wrapped up by two major acts; typing and mouse clicking. These newly adopted and highly performed social actions eventually lead the way to cybernetics. Cybernetics, as defined initially by Norbert Wiener (1954), refers to any self-regulating system that is set up by a stimulus and response through continuous feedback. As part of the representation of music, musical performance forms a cybernetic system in media and promotes an exchange between the musicians' actions and audience responses. However, it can be seen that in the case of music on cyberspace there is a temporal disconnection between performers and the audience, whereas in live concert halls or venues, the audience and stage personae are simultaneously performers making up the body of the musical representation.

Concerning the outcomes of this cyberization process, Lichty (2000, p.352) points out that the absence of live intercommunication results in a simulacrum of performance pieces. In other words, a cybernetic analysis of musical representations and technologically based performances result in the lack of live and real-time interaction between on-stage performers and audience members and of cognitive feedback between audience and performer. Further outcomes with regard to this process concern the change in the ways people listen to music. When we ask to ourselves today, 'why do we like what we like?' the answer might probably

be shaped by the mechanism of cybernetics, which also depends highly on the 'shared' views of the others. Most or least liked songs, music genres, music styles as well as the labeling of subcultural or ethnic sounds illustrate these shared representations. These categories and labels are now being continuously redefined and reconstructed without a need to base upon a solid point of artistic reference.

Some statistics from around the world and from Turkey may help to expose this growing prevalence of musical representation on the Internet. For instance, Spotify[5] is one of the most popular online music streaming websites with its 160 million users and 71 million registered users in 61 different countries in 2017. As a cyber musical platform, it offers more than 2 billions of playlists, composed of different music genres of many different styles, ranging from classical symphonic music to jazz, from rock to pop, to folk or ethnic music. Concomitantly, Turkish Statistical Institutes's Report[6] on cultural life in Turkey points out that almost 54% of online cultural activities are composed of audio files (both uploading and downloading music) and include various different types of musical productions. Another report (2017) points out that, the teenagers and young adults choose to listen to Internet radio, with a percentage of 24% and 25% consecutively. In addition, listening to music from online music streaming websites is very common for young people, 32% for teenagers and 27% for young adults. And finally, sharing one's recorded music and/or musical performance online is highly practiced by young people, 26% for teenagers and 21% for young adults. These numbers demonstrates the increasing rates of cyberspace musical activities. As a result, we can infer that cyberization of music is not only changing the ways the music is represented, but it is also reshaping the musical preferences and cultural tastes.

Conclusion

In our contemporary era, with the means of mass communication and the new media any composed musical piece can be immediately standardized by means of mechanical recording and circulated through a supposedly unlimited nebulous scape of the worldwide web. The already problematic difference between art music, folk music and popular music, implying a

[5] https://press.spotify.com/us/about/
[6] http://www.tuik.gov.tr/PreHaberBultenleri.do?id=24693

distinction between highbrow and lowbrow art forms have now been taken over by a cyber representation of music on an interface, denoting the recognition of a brand new music sphere.

We had been experiencing the end of the modernist metanarratives concerning the sphere of art and culture. Cyberpace has introduced further complications into this discussion in our contemporary era. On one hand, there are many different social actors who wish to preserve the system of music industries of the previous century. Yet, on the other hand, there are others who see the online music streaming and digital performances as a gift of cyberpace.

Today, each minute, thousands of music files, mostly free of charge, are searched for, listened to, liked and shared by billions of users. This has been considered as a convenience for consumers but a hassle for record companies, and the end result reveals an irreversible cultural transformation.

References

Alderman, J. (2008). *Sonic boom: Napster, MP3, and the new pioneers of music*. NY: Basic Books.

Becker, H. (1997). *Art worlds*. Berkeley: University of California Press.

Featherstone, M., Burrows, R. (Eds.). (1996). *Cyberspace, cyberbodies, cyberpunk: Cultures of technological embodiment*. London: Sage.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, 53(1), 59-68.

Lichty, P. (2000). The cybernetics of performance and new media art. *Leonardo*, 33(5), pp.351-354

Liu, C. C., & Tsai, P. J. (2001). Content-based retrieval of mp3 music objects. *Proceedings of the tenth international conference on Information and knowledge management*, 506-511.

Magaudda, P. (2011). When materiality 'bites back': Digital music consumption practices in the age of dematerialization. *Journal of Consumer Culture*, 11(1), 15-36.

Weber, M. (1958). *Social and rational foundations of music*. Illinois: Southern Illinois University Press.

Say, A. (2006). *Müzik tarihi*. İstanbul: Müzik Ansiklopedisi Yayınları.

Spotify Verileri (2017). Erişim 3 Şubat 2017, https://press.spotify.com/us/about/

TÜİK Hanehalkı Bilişim Teknolojileri Kullanım Verisi (2017). Erişim 6 Mart 2017, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=24862

Wiener, N. (1954). Cybernetics in history. In Craig, R & Muller, H. (Eds.), *Theorizing in communication: Readings across traditions* (pp. 267-273), London: Sage Publications.

Wright, C. R. (1959). *Mass communication: A sociological perspective*. New York : Random House.

Yates, C. D. (1994). *Overview: An introduction to music history*. MA: Simon & Schuster Custom Publishing.

SİBER DÜNYA RİSKLERİ VE ALINABİLECEK ÖNLEMLER

Ayşegül Güler[♣]

Özet

Dünyayı örümcek ağı gibi saran sanal ağların oluşturduğu siber alan insanlara büyük kolaylıklar sağlamasının yanında ciddi riskleri de bünyesinde barındırmaktadır. İnsanların teknolojiden yararlanması onların hayatlarını kolaylaştırmanın yanında, belli merkezlerce kontrollerine imkân da tanımaktadır. İnternet üzerinden yapılan her işlem, kullanıcılar hakkında yapılan analizlere veri tabanı oluşturmaktadır. Teknolojiyi elinde bulunduran devletler uluslararası hukuki boşluktan yararlanarak devlet dışı aktörler üzerinden hasımlarına zarar verebilmektedir. Kötü niyetli hackerler ahlaki sorumluluk duymadan insanların bilgilerini kendi amaçları doğrultusunda kullanabilmektedir. Sanal dünyada yapılan bilgi devşirme ve manipüle davranışlarına karşı ise insanların savunma mekanizmaları yetersiz kalmaktadır.

Devletlerarası rekabet de sanal alana kaymış ve rakip görülen tarafın ekonomisinden sağlığa, siyasete ve askeri alanlara kadar bilgileri kısa sürede toplanabilirken zorlayıcı önlemler hayata geçirilebilmektedir. Sanal tehlikelerden korunmanın en garanti yolu, onu kullanmamaktır. Ancak kişiler interneti kullanmasa bile devletler kamu hizmetlerinin büyük bir bölümünü bilişim sistemleri üzerinden yapmakta ve vatandaşlarının bilgilerini bazen koruyamamaktadır. Uluslararası yasaların yetersiz olması ise etkin güçlerce sanal saldırıların baskı unsuru olarak kullanılmasına zemin hazırlamaktadır. Saldırıya uğrayan tarafın meşru müdafaa hakkının bulunup bulunmadığı ise tartışmalıdır. Klasik Birleşmiş Milletler (BM) sisteminin sanal mağdurlara yönelik alacağı önlemlerin yetersiz olacağı düşünüldüğünde, siber suçlarla ilgili uluslararası toplumun ortak bir kavram oluşturması, insanların mahremiyetlerinin korunması ve suçluların cezasız kalmaması için ortak aklın hayata geçirilmesi gerekmektedir. Bu çalışmada kişilerin, kurumların ve devletlerin karşı karşıya kaldığı sanal tehditlerin neler olduğu üzerinde durulacaktır. Sanal alanı kötü niyetle kullananlara karşı, ulusal ve uluslararası alanda alınabilecek önlemler ve devletleri hedef alan saldırılarda meşru müdafaa hakkının kullanılıp kullanılamayacağı incelenecektir.

Anahtar Kelimeler: Siber Alan, Güvenlik, Riskler, BM, Müdahale.

[♣] Dr., Kazım Karabekir Meslek Yüksek Oklu, Karamanoğlu Mehmetbey Üniversitesi. aseguler@gmail.com

*Ayşegül Güler, Öğr. Gör. Dr. Karamanoğlu Mehmetbey Üniversitesi.

Cyber World Risks, Precautions To Be Taken Of People And States

Abstract

The cyber space created by virtual nets that surround the world like a spider web provides great convenience to people and also contains serious risks. Also making their lives easier, people benefit from technology, and they also have the opportunity to control certain centers. Every transaction made on the internet creates a database for the analyzes made about the users. States that have the technology can take advantage of the international legal gaps and damage their opponents over non-state actors. Malicious hackers can use people's knowledge for their own purposes without moral responsibility. The defense mechanisms of people are inadequate against the manipulation and manipulation of information made in the virtual world. The interstate competition has also shifted to the virtual space. The competing side of the economy, health, politics and military information can be gathered in a short time, the compulsory measures can be passed on to the imagination.

The safest way to protect yourself from virtual threats is not to use it. However, even if people do not use the internet, the state sometimes does not protect the information of their citizens when they make a large part of the public services through the information systems. The inadequacy of international laws paves the way for the effective use of virtual attacks as pressure elements. Whether the attacking party has the right to self-defense is controversial. When the classical United Nations system was deemed inadequate for virtual victims, the international community on cybercrime to form a common concept, protection of people's privacy and common mistakes must be made to prevent the criminals from going unpunished. This study will focus on the virtual threats facing people, institutions and governments. Measures that could be taken in the national and international arena against malicious users of the virtual space, and whether the right to self-defense can be used in attacks targeting states will be examined.

Keywords: Cyber Field, Security, Risks, UN, Intervention.

Giriş

Gerçek hayatın gölgesi olmaya başlayan siber uzay gelişmeye açık, hayatımızın her noktasına giren kaçamadığımız bir dünyadır. Dünyada milyonlarca insan bilgisayarın sağladığı kolaylıklardan yararlanmaktadır. Sanal ağ dünyayı örümcek ağı gibi sarmıştır. İnsan eliyle

oluşturulan sistemler insanı dışlama boyutuna gelmiş ve avantajları yanında ciddi riskleri bünyesinde barındıran siber dünya iki yüzü keskin bir kılıca benzetilmektedir.

İletişim teknolojisi ile bilgisayar teknolojisini birbirinden ayırmak imkânsızlaşmıştır. 1957 yılında uzaya yerleştirilen ilk uydu o tarihlerde büyük heyecan uyandırmış insanlık tarihinde önemli bir gelişme olarak değerlendirilmiştir. Günümüzde bu teknoloji sıradanlaşmış uzay, değişik amaçlarla gönderilen sayısız uydularla dolmuştur. Uydular aracılığıyla yapılan işlemler sabit telefonları dinlemekten daha kolay hale gelmiştir. Uydular, bilgisayar komutlarına göre iş görmekte, bilgisayar sistemleri üzerinden her konuda istenilen bilgileri toplayabilmektedir. Bilgisayarlar yapay zeka olarak insanlara büyük hizmetlerde bulunmasına rağmen kendisine hizmet edecek programları yeğlemektedir. Herhangi bir merkezdeki bir bilgisayar ülkenin en ücra köşesindeki bir evin elektrik harcamasını görebilmektedir. Toplumun büyük bir bölümünün yanında taşıdığı cep telefonları, uydu teknolojisi ile çalışmakla birlikte analiz ve taramayı yapan bilgisayarlardır. Ses özellikleri kaydedilen bir şahsın cep telefonu ile yaptığı görüşme neticesinde yeri tespit edilebilmektedir. Konuşulmayan hatta kapalı durumdaki cep telefonlarını izleme imkânı olması elektronik perdeleme sistemlerini de zaman zaman yetersiz kılmaktadır. Telefon firmaları ise insanların para vererek izlenmek istemeyeceklerinden bu gerçeği reddetmektedir.

Tüm bilişim sistemlerini içine alan kişilerin, kurumların ve devletlerin bilgi işlemlerinin hedeflerine güvenilir bir şekilde ulaşmasını sağlayan kaynakları ifade eden siber güvenlik kavramı günümüz dünyasında sıklıkla kullanılan bir kavram olmuştur. Teknik bir konu olan bilgi güvenliği konunun detayını ifade ederken, sosyal bir tanım olan siber güvenlik ise yazılım güvenliği, web güvenliği donanım ve ağ güvenliği gibi farklı alanları içine alan geniş kapsamlı bir kavramdır. Toplumda internet kullanımının yaygınlaşması ile sanal dünyadaki tehlikelere karşı insanlar daha duyarlı olmaya başlamıştır. Kullanıcıların kaydedilen verileri artıkça bilgi güvenliği daha da önemli hale gelmektedir.

Bilişim teknolojisinin tehlikeli olmasının nedeni, onun kötü amaçlar için kullanılmasıdır. Temel görevi bilgiyi işlemek olan bilgisayarlar ne yapmaları gerektiğini söyleyen yazılımlara bağlı olarak işlem yapmakta ancak üreteni kadar performans gösterdiğinden mutlaka bir açığını bulmak mümkün olabilmektedir. İnternete bağlanabilen veya sinyal gönderebilen her cihaz, potansiyel bir tehdit kaynağı olabilmektedir. Virüsler, Truva atları içine gizlenen kurtlar, tuzak kapıları, elektronik sıkışıklık siber saldırılar için alt yapı oluşturmaktadır. Siber

saldırı denildiğinde akla ilk gelen hack kavramı yazılım açıklarını bularak kendisine yarayacak şekilde kullanma davranışıdır. Dijital sistemde bir kapı varsa her iki tarafa da açılma imkânı vardır. Bu da siber alanda ahlaki sorumluluk duymayan saldırganlara, teröristlere ve kötü niyetli kişilere yeni ufuklar açarak yok etme imkânı sunmaktadır. Belli bir konu hakkında dikkat çekmek ve kamuoyu oluşturmak amacıyla faaliyet yürüten hacktivistlik kavramı ise bilişimin iyi amaçlarla kullanılıp kısa sürede geniş kitlelere ulaşma imkânı vermesi, olumlu bir yararlanma şeklidir. Burada üzerinde duracağımız konu ise iletişimi kötü niyetli kullanan sanal dünyanın korsanları, hackerlerdir. Hackerler, siber sistemlere şifre kırma işlemi ile izinsiz sızma işlemlerini gerçekleştirebilen kişi veya kişilerdir ve özel hayatın gizliliğine büyük tehdit oluşturmaktadır. Diğer bir ifadeyle yazılımlara açık bulma mantığı ile yaklaşan kişilerce sistem gerektiğinde içeri girmek için kapı kırılmakta "hack" lenmektedir. Güvenlik önlemleri ise karşılaşılan olgular dikkate alınarak oluşturulmaktadır. Ancak gelişmiş tehditlerin standart güvenlik duvarlarını aşma, kendini gizleme, değerli bilgileri alma konusunda sınır tanımadıkları görülmüştür. Güvenlik altyapısının güçlü olması saldırganlarla mücadele imkânlarını artıracak olmakla birlikte siber suçlarla mücadelenin maliyeti de giderek artmaktadır.

İnternetin sivil alanda kullanılması sanal bir hayatın oluşmasını gündeme getirmiştir. Sosyal medya, vahşi kapitalizm mantığı içinde çok hızlı gelişmekte, etkisinden kaçılamayacak bir ağ oluşmakta ve şahıslar siber dünyadan yararlanırken zararları çoğu kez göz ardı edilebilmektedir. Elektronik haberleşmenin hızı ve ucuzluğu onun yaygınlaşmasını sağlarken, haberleşmeye, güvenliği tehdit eden virüslerin gölgesi düşmektedir. İnternette tıklanan şeyler her bir saniyede 1500-2000 merkezle paylaşılmakta, profilinize yeni sayfalar eklenmektedir. Bu belirsizlik de insanlarda özellerinin ifşa edileceği endişesini artırmakta ve depresyona neden olabilmektedir. Hayatımız hakkında birçok bilgi dijital ortamda saklanmakta, bilgiler sürekli bilgisayarlar arasında gidip gelmektedir. İnterneti kullanan e-posta, haber ve web sayfaları ve sohbet odalarının her biri ardında iz bırakmaktadır. Yapılan aramaların bazı çevreler tarafından takip edildiği düşünülmekte ve insanlar bu veriler kullanılarak yönlendirilebilmektedir. Örneğin Facebook gibi sosyal medya platformlarında kişilerin aramaları yönünde reklamlar çıkmaktadır.

Alınan ve gönderilen bilgilerin şifresinin çözülüp çözülmediğini bilmek her zaman mümkün değildir. Bilgisayar sistemine sızma paranoyası giderek büyümektedir. 2005 yılında ortaya çıkan Facebook kısa sürede neredeyse dünyanın tüm kişisel bilgilerini kendinde toplamayı

başarmıştır. İnsanlar aslında görünür olmak için Facebook kullanmakla birlikte yapay zekâyla şahısların mahremiyeti azalmaktadır. Arka kapı kullanılarak zayıflıklardan yararlanılıp standart güvenlik tedbirlerinin algılamadığı küçük hamlelerle kötü amaçlı yazılımlar marifetiyle kimlik bilgileri çalınıp kötü amaçlarla kullanılabilmektedir. Sıradan insanların vakit geçirmek, eğlenmek, haberdar olmak için kullandığı sosyal ağlar büyük bir silaha dönüşebilmektedir. İnsanlar, verilerin nasıl bir sistem tarafından paylaşıldığının ve öneminin farkında değildir. Ücretsiz e-posta adresi veren bir siteye kaydolurken verilen bilgiler sadece o şirketin eline geçmez çünkü siteler topladıkları bilgileri başka firmalara satabilmektedir. Böylece verilerden eğilimleri belirlenmekte, ticari amaçlar dışında siyaset ve kamuoyu oluşturma faaliyetlerinde kullanılabilmektedir. İnsanlar inanmak istediklerine meyilli olduğundan sosyal medya ağlarıyla duygular manipüle edilerek insanların davranışları etkilenmekte ve yönlendirilebilmektedir. Örneğin 2016'daki Amerika Birleşik Devletleri (ABD) seçimlerine müdahale konusu gizemini korumaktadır. Facebook iddialara göre 50 milyon kullanıcısının bilgilerini satarak 2016 seçim kampanyalarında verilerin kullanılmasına aracılık etmiştir (Sabah Gazetesi, 2018). Yine bir görüşe göre de elde edilen veriler kullanılarak Rusya kontrolündeki 300 trol ordusu ABD seçimlerini etkilemeyi başarmış, Meksikalılar Trump'a yönlendirilirken, siyasiler Clinton yanlısı olarak görüldüğünden sandıktan uzak tutulmaya çalışılmıştır.

Kullandığımız e-devlet sistemi bürokrasiyi azaltıp kişilere çeşitli faydalar sağlamaktaysa da bireyleri saldırıya açık hale getirebilmektedir. Çünkü e-devlet sisteminin yaygınlaştırılması kişilerin izlenmesini kolaylaştırmaktadır. Devletin kişiler hakkında ne kadar bilgi sahibi olması kişilerin zararına olabilir? Bu soruya geniş kapsamlı bir cevap vermek gerekmektedir. Çünkü kişilerin haberi olmadan siyasi eğilimleri gibi kişisel eğilimleri belirlenmekte bu gelişme temel insan haklarından olan özel hayatın gizliliği ve kişisel verilerin korunması haklarını yerle bir edebilmektedir. Bu sebepten sitelerin her seferde bilgileri ne amaçla aldığını belirtmesi ve onaylatması gerekmektedir. Çünkü kişisel bilgilerimizin hangi alanlarda kullanıldığını bilmek hakkımız olsa gerekir.

Konuşulanları çözümleme boyutuna ulaşan bilgisayarlardan doğabilecek kâbus senaryoları ise Türkiye'de henüz görülmek istenmemektedir. 14 Aralık'tan itibaren Türkiye'de bankalara yönelik başlatılan siber saldırıların arkasında Rusya'nın olduğu şüphesi ciddi idi. Ancak böyle bir şüpheye suç isnat edilebilmesi için saldırının devletin talimatı, yönlendirmesi veya kontrolü altında yapıldığının tespiti gerekmektedir (Gümüşbaş, 2016).

Bireyler yaşadığı veya şahit olduğu olaylar nedeniyle tecrübe kazandıysa da sosyal medya insanlığın geleceğini tehdit etmektedir. Şahısların bilgisayarda sakladığı bilgiler üzerindeki kontrolleri sınırlıdır. Yanlış bilgileri düzeltmek kolay değildir. Kişiler, kendilerini güvende hissetmek ve bilgilerinin gizliliğinin korunmasını isterler. Peki, sıradan insanlar siber tehlikelerden korunabilir mi? Korunursa ne kadar korunabilir? Sorularına verebileceğimiz cevap sıradan kullanıcıların tehlikeleri engelleme imkânlarının oldukça sınırlı olduğudur. Tedbirlere rağmen geleneksel yöntemlerle bilgileri korumak mümkün gözükmemektedir. Lisanslı koruma programları bile ancak % 85 koruma sağlayabilmektedir. Dünyada Wikileaks örneği varken siber dünyanın sağladığı özgürlük zaman içinde özel hayat kavramını da yok edecektir.

Şahıslar, bireysel güvenliklerini sağlamak amacıyla ortak ağlardan mümkün olduğunca uzak durmalı, karşılaşılan her linke okuyup incelemeden tıklamamalı, web sayfalarındaki "https" ifadesini kontrol etmelidir. Güvenli erişim kanalları (VPN) kullanılmasına gayret edilmelidir. Kolay kırılamayan şifreler kullanılmalı ve 3-5 ayda bir şifreler değiştirilmelidir. Bilgiler sık sık yedeklenmeli, aynı şifreler değişik platformlarda kullanılmamalıdır. Ortak wi-fi kullanımından kaçınılmalıdır. Toplum medya okuryazarlığı konusunda eğitilmeli ve siteler üzerinde kamuoyu baskısı oluşturulmalıdır. Çünkü verilerin korunması hakkı aslında evrensel bir insan hakkıdır. Ayrıca unutma hakkı, verilerin hangi amaçlarla toplandığını bilme hakkı ve verileri alma hakkı etkin halde hayata geçirilmelidir.

İşlevleri aktif tutması gereken kurumlar açısından konuya yaklaşıldığında, gizli bilgilerin korunması kritik bir öneme sahiptir. Elektronik ağları en çok kullanan ülkeler, siber saldırılara daha fazla maruz kalma riskini taşımaktadır. Her geçen gün virüs bulaşma riski ve güvenlik olayı artmaktadır. Virüs ve saldırılara karşı alınan önlemler aciz kalmaktadır. 21. yüzyılda bilişim teknolojisindeki hızlı değişimler sonucu devletlerarasında yaşanan rekabette savaş yöntemleri değişmiştir. Savaş ağlar üzerinden bilgi alma, zarar verme, kontrol etme gibi yöntemlere yönelmiştir. Teknolojinin gelişmesi saldırıların şahıslar tarafından da yapılmasına imkân sağlamıştır. Saldırının kaynağının tespitinin zor olması devlet destekli de olsa yaptırım uygulanmasını zorlaştırmaktadır (Kaymak, 2017:1).

Siber saldırılar henüz klasik askeri hareketlerin yerini almak için yeterli değildir. Ancak askeri faaliyetleri destekleme kabiliyeti çok yüksektir. Bilgi sistemlerine daha bağımlı olan devletler

ekonomisi daha zayıf bir devlet tarafından büyük zarara uğratılabilir. Konvansiyonel veya nükleer silahların kullanıldığı büyük bir savaş muhtemelen son savaş olacağından devletler devlet dışı aktörler üzerinden yürüttükleri saldırıları siber uzayda tutma isteğindedir (Dikbıyık, 2014:8-10). Kısacası günümüz saldırıları denizden veya havadan yapılmamakta kablolar üzerinden gerçekleşmektedir, yani savaşlar bilgisayarlaşmıştır. Post-modern savaş olgusu kitleleri etkilemek amacıyla sahaya sürülmüştür. Savaş günümüzde silahlı kuvvetlere karşı yürütülen bir eylem olmaktan çıkmış toplumun bütün kesimlerini ilgilendiren her türlü araç kullanılarak yapılan sızma girişimleri ile yürütülmektedir Körfez Savaşı'nda bilgisayarlar etkin olarak kullanılmış, savaş alanından canlı yayınlar yapılarak kuvvetler sevk ve idare edilirken hasım tarafın psikolojisinin yıpratılması amaçlanmıştır. Özetle bilgisayarlar savaş alanında komuta, kontrol, istihbarat ve iletişim amacıyla kullanılmıştır.

Tek kurşun atmadan, kan akıtmadan ülkeleri zaafa uğratmak imkânına sahip olunabileceği mümkün gözükmektedir. Dünya artık bilim temelli bir savaş yaşamakta, ekonomik, siyasi, askeri gibi alanlarda ciddi bir siber mücadele yürütülmekte, korsan fonlar kullanılarak ülkelerin borsaları çökertilebilmektedir. Zaman zaman ülkemizde de karşılaştığımız gibi bir ülkenin kritik merkezlerine, örneğin elektrik santrali veya iletim hatlarına yapılacak bir müdahale ülkelerin ekonomisini bir anda felç edebilmektedir. Finans kuruluşları, hastaneler, enerji kaynakları ilk hedefler arasındadır. Hava ulaşımında kullanılan kontrol kuleleri, borsa bilgisayarları, ATM'ler ve hastaneler sıkça hedef olmaktadır. Firmaların kendilerini siber güvenlik açısından kontrol etmek amacıyla yaptırdıkları sızma testleri birçok kez yetersizlikleri ortaya koymaktadır. Kötü amaçlı kullanımları önlemenin yolu yine siber güvenlikçilerin yazışmaları izlemesinden geçmektedir. Verilere ulaşmak inanılmaz zaman ve para tasarrufu sağlamaktadır. Devletler yazılımlarda açık kapı bırakılmasında ısrarcı davranmaktadır. Bilgisayar sistemleri ABD kaynaklıdır ve tüm dünyadaki bilgileri denetleme imkânı vardır. Microsoft'un ABD çıkarlarını korumak adına yazılımlarda arka kapı bıraktığı yaygın bir kanaattir. Terör faaliyetleri siber alanda yapılırken bazı devletler siber terör gerekçesiyle dünyayı kontrol etme gayretindedir. Dünya üzerinde çıkacak muhtemel bir savaşta ilk mermiyi kimin atacağı bilinmemekle birlikte saldırıların internet üzerinden yapılacağını ifade etmek kehanet olmasa gerekir. Hükümetler, ülkelerindeki internet trafiğini güvenlik gerekçesiyle izlese de bu alan istismara açık bir alandır. Her halükarda özel hayat denetim altındadır.

Siber tehdit ortamı değiştikçe tedbirler de değişmek zorundadır. Bilgi ve iletişim teknolojisindeki gelişmeler yakından takip edilmelidir. Tecrübeler ışığında üst bir güvenlik ağı oluşturulmalı ve sürekli güncellenmelidir. Personelin siber saldırılara karşı gerekli bilgilerle donatılması gerekmektedir. Stratejik alt yapı (enerji, eğitim, ulaştırma vb.) alanlarında zaaflar belirlenip tedbirler alınmalıdır.
Siber saldırılarda bir devlet diğer devletlere karşı bilgi sistemleri üzerinde oluşturacağı etki ile üstünlük sağlamayı amaçlamaktadır (Dikbıyık, 2014:8-10).Örneğin ABD'de birçok bilgisayarın Kosova müdahalesi sırasında Çin kaynaklı saldırıya uğraması engellenememiş ve Çin'in Belgrad büyükelçiliği 9 Mayıs 1999'da ABD hava kuvvetlerince vurularak uyarılmıştır.

Devletler siber saldırılara ne kadar hazırlıklıdır? Bu soruya net bir cevap verebilmek mümkün gözükmemektedir. Çünkü tedbirler tehdidin tanınmasından sonra oluşturulduğu için siber korsanlar devletleri de aciz bırakabilmektedir. Elde edilen bilgiler illegal amaçlarla kullanılabilmektedir. Bu yüzden modern ülkelerin savunma sistemleri bilgisayar ağını zorunlu kılmaktadır. Siber mücadeleye karşı ülkeler kendi siber ordularını oluşturmakta ve kendi yazılımlarını üretmeye çalışmaktadır.

Devletleri tehdit etmeye başlayınca bilinir hale gelmeye başlayan siber saldırıların doğrudan devletleri ve insanlığı hedef alması doğacak sonuçların vahameti, konunun uluslararası hukuk açısından ciddi şekilde ele alınmasını gerektirmektedir (Kaymak, 2017:1). Siber saldırı: düşman olarak kabul edilen merkezlerin bilgisayar sistemlerini ve buradan geçen bilgileri bozmak, yanıltmak ortadan kaldırmak için yapılan hareketler olmasına rağmen uluslararası alanda bir metin üzerinde uzlaşma sağlanan bir kavram değildir. Birleşmiş Milletler (BM) 3814 sayılı kararın 1. maddesi saldırıyı "Saldırı, bir devletin diğer bir devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya işbu tanımda belirtildiği üzere, Birleşmiş Milletler Antlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılması" (3814 sayılı karar BM Enformasyon Merkezi) olarak tanımlanmaktadır. Bu tanım siber saldırıların silahlı saldırı kabul edilip edilemeyeceğine açıklık getirmemektedir. Silahlı saldırı, kuvvet kullanımıdır. Ancak her kuvvet kullanımı silahlı saldırı değildir. Uluslararası sistem devletleri esas aldığından siber saldırıların BM Antlaşmasının 2/4. maddesinde açıklanan saldırmazlık ilkesini ihlal edip etmediği tartışmalı hale gelmektedir. 2/4. maddesi "Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Miletlerin amaçları ile

bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar" ifadesini taşımaktadır. Bu hükümler saldırıya uğrayan tarafa müdahale için bir meşruiyet sağlar mı? 51. maddede belirtilen meşru müdafaa veya BM Güvenlik Konseyi kararı ile kuvvet kullanma istisnası, silahlı saldırı olması durumunda meşru müdafaa hakkını vermektedir (BM Antlaşması). Siber saldırılar insan kayıpları ve büyük maddi kayıplar oluşturmuşsa meşru müdafaa hakkı doğabilmekte, can kaybı olmadığı durumda siber saldırılar kuvvet kullanımı olarak değerlendirilmemekte ve meşru müdafaa hakkı doğmamaktadır.

Siber saldırılar bu kapsamda değerlendirilebilir mi konusu tartışmalıdır. Saldırıya uğrayan tarafın konuyu Güvenlik Konseyine götürmesi halinde alınacak tedbirleri içeren 41 ve 42. maddelerin siber saldırıları engellemeyeceği de aşikârdır. Siber saldırılar konusunda en ciddi çalışma NATO'nun ortaya koyduğu Tallinn Siber Saldırı Kılavuzu'nda devletlerin iç işlerine müdahale, seçim sonuçların manipüle etme, bir hacker grubunun desteklenmesi, bu türden suçlardır (Gümüşbaş, 2016). Bir devletin siber saldırıya uğraması halinde saldırının bir devlet tarafından yapıldığının ve saldırıya uğrayanın devlet olması şartı oluşursa meşru müdafaa hakkının doğacağı Tallinn uzmanlarınca ileri sürülmektedir. Ancak siber saldırıların kaynağını bulmak ve misillemenin caydırıcılığını önceden bilmek kolay değildir (Dikbıyık, 2014:7). Günümüze kadar devletlerarasında gerçekleşen siber operasyonlar siber saldırı boyutuna ulaşmamış kabul edildiğinden meşru müdafaa hakkı da doğurmamıştır (Gümüşbaş, 2016). 11 Eylül sonrası yürürlüğe konulan Bush Doktrini olarak bilinen ABD strateji belgesi meşru müdafaaya yeni bir boyut getirdiyse de henüz siber saldırılar açısından hayata geçirilmemiştir.

Siber saldırılar kontrollü yapılma imkânı vermektedir. Hedef sistemlere küçük hamlelerle zarar verilebileceği gibi hedefin bütün kritik altyapı sistemlerini bir anda felce uğratması da mümkündür. Ancak küçük seviyede yapılan saldırılar, açıkların görülüp kapatılması konusunda yardımcı da olabilir (Dikbıyık, 2014:11-32). Devletlerin altyapıları ve desteği olmadan büyük saldırılar gerçekleştirilemeyeceği bilinmesine rağmen saldırıları kimse üstlenmemekte, bir grup kendisini ifşa ederek konu kapanmaktadır. Ayrıca İran nükleer tesislerine karşı kullanılan Stuxnet virüsü dışında devletlerin saldırı amaçlı kullandığı bir yazılım da literatüre girmemiştir (Kaymak, 2017:4). NATO uzmanları, zararın ciddi boyutta olmadığı için bunların "silahlı saldırı" sayılamayacağı görüşünü açıklamıştır. Yine de Stuxnet

adlı siber saldırı, bunun devletler seviyesinde hukuki boyutunun belirlenmesinin gerekliliğini ortaya koymaktadır (Tuğal, 2016).

Kısacası siber suçlarla ilgili yasal altyapılar yetersiz kalmaktadır. Bilgisayar ağları ve donanımları üzerinden işlenen suçlar siber suç olarak kabul görmekle birlikte uluslararası hukukta hangi eylemlerin siber saldırı suçu olarak kabul edileceği açıkça belirlenmemiştir. Avrupa Konseyince siber suçlarla ilgili 2001 yılında hazırlanan sözleşme 2003 yılında tarafların onayıyla yürürlüğe giren Siber Suç Sözleşmesinde "yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemi aracılığıyla sahtekârlık veya dolandırıcılık" suçlarıyla sınırlı tutulmuştur (Tuğal, 2016). Günümüz hukuk ilkeleri, devleti esas almaktadır. Yani uluslararası kişi ve kurumlar sorumlu tutulamamaktadır. Sorumlular tespit edilemediği için saldırılar cezasız kalmaktadır. Bu yüzden ulusal ve uluslararası hukukun düzenlenmesi ve güncellenmesi gerekmektedir. Siber suçlara karşı oluşturulan kişisel verilerin korunmasına yönelik düzenlemeler sık sık güncellenmediğinden yetersiz kalmaktadır. Siber suç, saldırı, casusluk gibi terminolojinin gelişmesine paralel olarak değişen eylemlere karşı ulusal ve uluslararası hukukun gerekli düzenlemeleri yapması ve sık sık güncellenmesi gerekmektedir.

Kaynakça

Birleşmiş Milletler Antlaşması, https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf, (Erişim Tarihi: 10.03.*2018*).

BM Enformasyon Merkezi UNIC-Ankara Saldırı'nın (Tecavüzün) Tanımı: Birleşmiş Milletler Genel Kurulu'nun 3814 (XXIX) Sayılı ve 1974 Tarihli Kararı, http://www.unicankara.org.tr/doc_pdf/3814.pdf, (Erişim Tarihi: 09.04.2018).

Dikbıyık, F. (2014). "Stratejik ve Operasyonel Siber Savaş" s:1-35 Siber Caydırıcılık. SG507SiberSavaşlarGüz2014, http://docplayer.biz.tr/14265180-Siber-caydiricilik-sg-507siber-savaslar-guz-2014-yrd-doc-dr-ferhat-dikbiyik.html, (Erişim Tarihi: 12.03.2018).

Gümüşbaş, A. (2016). Uluslararası Hukuk Açısından Türkiye Siber Saldırılara Karşı Ne Yapabilir? https://siberbulten.com/makale-analiz/uluslararasi-hukuk-acisindan-turkiye-siber-saldirilara-karsi-ne-yapabilir/, (Erişim Tarihi: 23.04.2018).

Kaymak, O. (2017). Siber Harekâtlar Ve Uluslararası Hukukta Meşru Müdafaa Hakkı, http://www.ilimvemedeniyet.com/siber-harekatlar-ve-uluslararasi-hukukta-mesru-mudafaa-hakki.html, (Erişim Tarihi:13.03.2018).

Sabah Gazetesi, 21.03.2018, "Yine Facebook (/haberleri/facebook) Yine Skandal!.

Tuğal T., Ş., (2016). Siber Güvenlik Savaş Casusluğun Hukuki Boyutu, http://www.itnetwork.com.tr/siber-guvenlik-savas-casuslugun-hukuki-boyutu/, (Erişim Tarihi: 23.04.2018).

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

GELECEĞİN ENDÜSTRİLERİ

Ross, A.(2017). Geleceğin Endüstrileri (Murat Buğan (Çev.). Ankara: Orion Yayınevi. pp.286. ISBN: 6055145972 (paperback). ₺ 26.46

Reviewed by Nezir Akyeşilmen*

Hayatın her alanını kuşatmaya başlayan dijital dünya günlük hayatımızın ayrılmaz bir parçası haline gelmiştir. Bugün milyarlarca araç ve gereç otomasyon ve interleşerek hayatımıza konfor katmaktadır. Nesnelerin interneti(IoTs), Büyük Veri, Bulut teknolojisi ve Block Chain gibi yenilikler gelecekte siber teknolojinin hayatımızı daha da derinden etkileyebileceği ve değiştireceğinin en somut örnekleri arasında yer almaktadır.

Bugün yaşadıklarımızı 30 yıl önce internetin kurucu babaları dahi hayal edemezlerdi. Peki 30 yıl sonra nasıl bir dünya ile karşılaşacağız? Yenilikler ve yeni teknolojiler bizleri nereye taşıyacak? *Geleceğin Teknolojiler* bir dizi konunun yanı sıra şu sorulara da cevap aramaktadır. 10 yıl sonra bizi nasıl bir dünya bekliyor? ; Kansere çare bulunacak mı? ; Robotlar işimizi elimizden alacak mı? Ya da robotlarla rekabette başarılı olmak için neler yapmamız gerekiyor? ; Geleceğin meslekleri hangileri olacak? ; Çocuğumu geleceğe nasıl hazırlamalıyım? ; Geleceğin yatırım alanları hangileri? ; Büyük veri ve analitik hayatımız nasıl değiştirecek?(Arka kapak).

Geleceği tahmin etmek her zaman zor ve riskli bir girişimdir. Zira, mevcut veri üzerinden neler olabileceğini kestirmek zordur. Bu arada ne tür yenilik ve gelişmelerin meydana geleceğini tahmin etmeyi de içeren böyle bir girişim ciddi bir bilgi, tecrübe ve açık bir vizyon gerektirmektedir. Alec Ross bu özellikleri önemli oranda karşılamaktadır.

Ross, Amerika'nın önde gelen inovasyon uzmanlarından biridir. ABD Başkanı Obama'nın her iki seçim kampanyasında yaptığı danışmanlığın yanı sıra dört yıl boyunca ABD Dışişleri Bakanı Hillary Clinton'ın İnovasyon Danışmanı olarak görev yaptı ve Dışişleri Bakanlığı Onur Ödülü'ne layık görüldü. Halen Johns Hopkins Üniversitesi'nde ders vermekte, yatırımcılara, şirketlere ve hükümet liderlerine danışman olarak hizmet vermektedir.

* Assoc.Prof.Dr., Departmen of International Relations, Selçuk University, can be contacted on twitter @nezmen or E-mail: nezmen@yahoo.com.

Geleceğin endüstrileri kitabı sekiz bölümden oluşmaktadır. Giriş ve sonuç bölümlerinin yanında "Ve Robotlar Sahnede"; "İnsan Makinesinin Geleceği"; "Para, Güven ve Piyasaların Kodlaştırılması"; "Kodların Silahlaştırılması"; "Veri,"; ve Gelecekteki Piyasaların Coğrafyası" bölümleri bulunmaktadır. Bu incelemede üzerinde durulacak gereken konular; "robotik, ileri yaşam bilimleri, paranın kodlaşması, siber güvenlik ve büyük veri gibi geleceğin kilit endüstrileri ile bunların ortaya çıktıkları jeopolitik, kültürel ve kuşaksal bağlamlardır. Bu endüstriler yalnızca kendi başlarına önemli oldukları için değil, aynı zamanda daha büyük küresel eğilimlerin sembolleri olması ve birbirleriyle olan ilişkileri nedeniyle seçtim" diyor, Ross(s.19).

Her yeni değişim ve dönüşümün kazanları ve kaybedenleri olduğunu ileri süren Ross, şu tespitlerde bulunmaktadır(s.10);

> *İnovasyon ve küreselleşmenin son dalgası kendi kazananlarını ve kaybedenlerini üretti. Kazananlar tarafında yer alan birinci grup; yatırımcılar, girişimciler ile yeni buluşlar ve hızlı büyüyen piyasalar etrafında bir araya gelen yüksek vasıflı işçilerdi. Kazanan ikinci grup ise, ülkelerinin dışa açılıp küresel ekonominin bir parçası olmasıyla oluşan ucuz iş gücü avantajını kullanıp fakirlikten orta sınıfa terfi eden 1 milyardan fazla insan. Kaybedenler ise, Amerika ve Avrupa gibi yüksek maliyetli işgücü piyasalarında yaşayan, becerileri, küreselleşen piyasaların ve teknolojinin hızına yetişemeyen insanlardı.*

Robotlaşmanın gelecekte hayatın her alanında yer alacağını iddia eden *Geleceğin Endüstrileri,* yaşlı ve hasta bakıcılığından sanayideki işçiliğe kadar her alanın robotlarla dolacağından emin. "Yeni meslek sahiplerine ve bakıcılarınıza merhaba deyin. Önümüzdeki on yıl, insanlar robotlarla birlikte yaşamayı öğrendikçe dönüşen toplumları görecek" gibi net bir öngörüde bulunmaktadır.

Kişiye özel ilaçların üretileceği tıbbi devrimden, insan beyninin heclenebileceği djitalleşmeye geniş yelpazede argümanlar geliştirmektedir. Dijital para ve kodların silahlaştırılmasından, siber güven(siz)liğe, büyük veriden yeni pazarlara her alanda meydana gelecek yenilik ve değişikliklere güzel örnekler vermektedir.

Ross'a göre, "Dünya, Soğuk Savaş'ı (Cold War) geride bıraktı ancak Kod Savaşı (Code War) başlamak üzere"(s.125). İşin doğrusu bu savaş başlamış durumda. Ve dünya çapında her gün milyonlarca siber saldırı ve çatışma meydana gelmektedir. Bunların büyük bir kısmı zararsız olsa bile, %1'lik bir kısmı bile binlerle ifade edilmektedir. Tehlike büyük ve geleceğin savaşları hiç kuşkusuz siber savaşlar olacaktır.

Giderek dijitalleşen hayatımız, dünyanın değişik yerlerinde bilmediğimiz dijital dehlizlerde bizimle ve küreyle ilgili muazzam veri biriktirilmektedir. Bu veriler gelecek endüstrilerinin hammaddesi olacaktır. Veriyi kontrol eden dünyayı kontrol eder. Ross bu konuda "Tarım çağının hammaddesi topraktı. Demir, endüstriyel çağın hammaddesiydi. Veri ise bilgi çağının ham maddesidir"(s.155) demektedir.

*Ross kitabın önemini anlatırken şunları söylemektedir: "*ailemin veya büyükanne ve büyükbabamın 1960'larda keşke okusaydık diyebilecekleri kitap, küreselleşmenin dünyaya ne getireceğini açıklayan bir kitap olurdu. 20 yıl önce üniversiteyi bitirirken keşke okusaydım diyebileceğim kitap, internetin ve sayısallaştırmanın dünyaya ne getireceğini anlatan bir kitap olurdu. Bu kitap, ekonomilerimize ve toplumlarımıza gelecek 20 yıllık değişim sürecinde yön verecek endüstrilere göz atıyor"(s.19).

Geleceğin Endüstrileri, Murat Buğan tarafından aslına uygun ve dil farklılıklarını ortadan kaldırmaya çalışan bir hassasiyetle, oldukça akıcı ve tutarlı bir dille çevrilmiştir. Kitap okuyucuya büyük bir ufuk penceresi açmaktadır. Okundukça teknolojinin toplum üzerindeki etkilerini ve geleceğimize vereceği yön hakkında sağlıklı bir bilgiye sahip oluyorsunuz. Teknoloji hem korkulan hem de sevilen bir şeydir. Toplumda bugünlerde Aşk ve nefret arasında bir teknoloji algısı var. Fakat Geleceğin Endüstrilerini okuduğunuzda onun basit bir araç olduğunu ve insanların onu istedikleri yere çekebileceğini anlıyorsunuz.

Kitabın bu pozitif yanlarına karşın, bazı eksikliklerinin olduğunu da vurgulamakta yarar var. Konu ve tahmin açısından oldukça zengin olmasına rağmen, kendisinin önem verdiği veri yönüyle biraz zayıf kalmıştır. Hikayelerle kitap zenginleştirilmiş, fakat gelecek tecrübeleri biraz daha göz ardı edilmiştir. Gelecekte insan hayatının tam olarak nasıl şekilleneceği konusuna biraz daha fazla ağırlık verilebilirdi. Diğer önemli bir husus teknolojiyi biraz fazla abartmış gibi görünüyor ki gelecek onu haklı çıkarabilir. Fakat bu tür anlatı bile insanın

geleceği karanlık görmesi sürecine bir zemin hazırlamaktadır. Bilgi ve örneklerin çok, fakat araştırmanın kısmen zayıf kaldığı bir çalışma.

Sonuç olarak, *Geleceğin Endüstrileri* teknolojiyi, dijitalleşmenin geleceğini ve insanın karşılaşacağı durumları anlamak için herkese uygun bir dil kullanmaktadır. Fazla teknik olmayan ve fakat herkesin bilmesi gereken konuları işlemiştir. Politikacılar, karar alıcılar, sosyal ve fen bilimleri öğrencilerinin kısacası bütün dijital vatandaşların okuması gereken bir kitap.

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.