International Journal of Social Inquiry
Cilt / Volume 12 Sayı / Issue 2 2019 ss./pp. 545-566

THE NEW FRONT IN GLOBAL INSECURITY: CYBERSPACE*

Soner ÇELİK**, Muharrem GÜRKAYNAK*

Makale Geliş Tarihi-Received: 15.02.2019
Makale Kabul Tarihi-Accepted: 20.11.2019
DOI: 10.37093/ijsi.659014

ABSTRACT

The term of security, has been consistently discussed as a case of human beings until today. Especially with the formation of nation-state structures, the concept of security has undergone a constant change.At the same time, the issue of security is one of the main factors determining the international relations.

Especially in the post-Cold War period, the concept of "threat" became more important than the concept of the enemy.In today's popular issues,

---

* *This article is produced from the unpublished PhD thesis titled "The Changing Security Perception in the Globalization Scenario: Case of Cybersecurity" in the International Relations Department of the Institute of Social Sciences. And also paper has been accepted for an oral presentation at the Turkish Foreign Policy and International Relations Congress on 15-17 November 2018. (http://www.alkusam.org)*

** *Süleyman Demirel University, Institute of Social Sciences, Department of International Relations, PhD. Candidate, Isparta / Turkey. ORCID: https://orcid.org/0000-0001-7554-5628. sonercelik85@gmail.com*

*** *Assoc. Prof. Dr., Süleyman Demirel University, Faculty of Economics and Administrative Sciences, Department of International Relations, Isparta / Turkey. ORCID: https://orcid.org/0000-0002-5371-0474. muharremgurkaynak@sdu.edu.tr*

cybersecurity carries the cyber-space beyond the perceptions of the individual and the security of the state and poses an uncertainty and instability in the global security environment.For this purpose, the scope of the study is limited as cyber threats, which are one of the types of threats towards the new security concept.In this study, the effects of the developments and events in the field of cyber-space on the national and international security problems are explained.In this context, in the face of cyber threatening areas and types of cyberspace, it is argued that all kinds of security measures, co-operation and coordination mechanisms that can be taken by the actors in national and international / supranational analysis level can be used.

Keywords: Globalization, Security, Threats, Cyberspace, Cybersecurity.

KÜRESEL GÜVENSİZLİĞİN YENİ CEPHESİ: SİBER UZAY

ÖZ

Güvenlik olgusu, geçmişten günümüze kadar üzerinde sürekli tartışılan bir kavram olmuştur. Özellikle ulus devlet yapılarının meydana çıkması ile güvenlik kavramı sürekli bir değişim içerisine girmiştir. Aynı zamanda güvenlik konusu günümüzde uluslararası düzeydeki ilişkileri belirleyen temel unsurların başında gelmektedir.

Özellikle Soğuk Savaş sonrası dönemde, "tehdit" tanımlaması, düşman tanımlamasından çok daha önemli hale gelmiştir. Günümüzün popüler konularından siber güvenlik, siber-uzayı birey ve devletin güvenliğine ilişkin tehdit algılamalarından öteye taşımakta, küresel güvenlik ortamındaki belirsizlik ve istikrarsızlığı ortaya çıkarabilecek bir mesele olarak karşımıza çıkmaktadır. Bu amaçla çalışmanın kapsamı, konu bağlamında yeni güvenlik anlayışına yönelik tehdit türlerinden biri olan siber tehditler olarak sınırlandırılmıştır. Çalışmada siber-uzay alanındaki gelişmelerin ve olayların günümüzde eriştiği noktadan yola çıkarak ulusal ve uluslararası güvenlik sorunlarına etkisi vakalar üzerinden açıklanmaktadır. Bu kapsamda gelişen siber tehdit alanları ve türleri karşısında siber uzayda ulusal ve uluslararası/uluslarüstü analiz seviyesinde aktörlerin alabileceği her türlü güvenlik önlemleri, işbirliği ve koordinasyon mekanizmalarıyla caydırıcı uygulamaların neler olabileceği tartışılmaktadır.

Anahtar Kelimeler: Küreselleşme, Güvenlik, Tehdit, Siber Uzay, Siber Güvenlik.

INTRODUCTION

The area of global insecurity is changing and transforming among the actors and factors with an unbelievable speed. In this context, various attacks against the asymmetric threats directed by the non-state actors as well as the occupations that compel the conventional response by the state are witnessed. For example, the war in South Ossetia, which broke out in August 2008, was perceived as a short-term war between Russia, Georgia, South Ossetia and Abkhazia, but in fact pointed to a profound change affecting the future of the Caucasus region. In the first week of April 2016, violent armed conflicts between the Azerbaijani and Armenian military forces should be taken into account because of the Nagorno-Karabakh issue, which cannot be resolved despite the cease-fire in 1994, in order to reflect the environment of insecurity in the Caucasus. We can make some inferences about the existence and future of global security.

First of all, after the Second World War, the United Nations (UN) and the permanent peace and stability that is desired to be established in the international system by the end of the World War II, is the violation or abuse of the members of the UN Security Council.In this respect, the validity of the international and regional alliances, such as the UN and NATO, and its binding on the signatory parties are highly controversial. Therefore, it should be questioned how the signatures put on multilateral international conventions as much as the harmony and complementarity between the international and domestic law and beyond the rhetoric are imposed in practice. In this context, it is controversial whether member states comply with the rules of the UN in Yugoslavia, Bosnia and Herzegovina, Afghanistan, Iraq, Yemen, Syria, Georgia and Ukraine. In addition, the functioning and functionality of the common defense mechanism promised by NATO to its allies is open to doubt and criticism.

Secondly, all the debates on international law and the assurances offered by regional/international alliances, on the one hand, global peace and stability are realistic utopia. However, by looking at the current civil war and conflict areas, the cause of this truth should not be sought in the fate of the geography.In other words, the perpetrators and those responsible for the global insecurity environment are not African countries such as Angola, Nigeria, Somalia and Sudan, nor the states in the Middle East such as Iraq, Syria and Yemen. There

should be some factors triggering the conflict, not the parties that should be taken into consideration. Clearly, it is the desire to seize the underground and overland resources as the most important thing for human beings and as countries. Considering factors such as the reduction of available natural resources in the world such as water, energy, oil, decreasing efficiency, and increasing the cost of use, it is clear that wars will not end due to access and sharing of resources.

The third is that in the future, conventional wars will not lose their validity. The role of state and non-state actors because of existing rural, local and regional conflicts, and the structure and course of civil wars have arisen. In the field of today's struggle, similar methods such as intense use of Unmanned Aerial Vehicles (UAV) for intelligence and assault purposes, shooting of military targets with remote controlled hand-made explosive bombs, and suicide attacks aimed at mass murder of civilians are more in the forefront. Although low-intensity conflicts or proxy wars are often voiced today, we cannot say that the regular armies of two or more states are in combat.

How important is the role of conflict, the place and structure of the operation area, the role and responsibility of the state and non-state actors in terms of establishing security, peace and stability on a global scale? In other words, in modern times, when technological innovation changes and transforms the tactics and strategies of war, how and at what level does it threaten national and global security to acquire new talents and take over initiatives in the cyber-space field, defined as the fifth dimension of the war?

In the light of current events at the global and regional level, there is not only rising instability and insecurity, but also a blurred uncertainty. In fact, the increasing and deepening uncertainty has become more prominent in cyberspace space due to its characteristic features. Therefore, a few issues should be underlined about cybersecurity and cyber threats and the nature and cost of cyber warfare, which has the power and character to be present and not exist anywhere at the same time.

1. FINDINGS AND DISCUSSION ABOUT CYBERSECURITY

Since times immemorial, the principal domains of warfare were land and sea. Kings and rulers built armies and navies, fortresses and castles, and sent scouts and spies to find out what their potential adversaries were up to. If properly organized, one would normally have some kind of early warning that an attack was in the making before it actually took place, so that countermeasures could be taken. The fortress gave a sense of security, at least until the advent of modern artillery.

As the technology of flight developed, air evolved as a new domain. There was simply no opting out; if your adversary developed an air force, you needed air defences, or your armies and navies would prove of little avail. Military strategy evolved: why spend resources on attacking a well-protected border when you could strike deep behind enemy lines, at population centres or even at the very centre of decision-making. The combination of technology and military strategy led to the shift from World War I trench warfare to World War II blitzkrieg.

Today, cyberspace has emerged as a domain of its own, in many ways like land, sea and air. Indeed, it might be the domain of choice: We can safely postulate that any future conflict between reasonably advanced actors will be a cyber-conflict. No modern attacker would resist the temptation to destroy, disrupt or confuse enemy sensors, communications and decision-making loops. What will vary is whether the conflict will take place in the physical domains as well. This insight will change the nature of conflict in fundamental ways, and possibly, lower the threshold of war and confuse the very distinction between war and peace.In addition, just as with the advent of human flight, opting out is not an option. Modern societies have become existentially dependent on cyberspace. In the words of Beckstrom, the former head of ICANN: anything networked can be hacked; everything is being networked so everything is vulnerable (Kaspersen 2018).

The global security environment is becoming increasingly ambiguous and unstable due to state and non-state actors using a combination of

tactics and techniques of conventional and asymmetrical warfare. In this context, cyberspace indicates a critical area for states in terms of both attack and defense capabilities. In fact, this area contains a wide range of substructures and superstructures ranging from individual safety to state security. Hence, cybersecurity has a very different and alarming nature than the threat posed by independent hackers who often settle into minds.

In today's research, there is a serious distinction between the "technical dimension" of cybersecurity, which emphasizes mostly computer-oriented information technologies and applications, and the "social dimension" that emphasizes political and legal practices over national security concerns. In this context, the top level security decision makers responsible for providing a national security of a country are; If it is not expected to have a technical depth at the level of expertise in the scope of asymmetrical conflict or implicit operations in the context of the fight against terrorism, it is unthinkable to have a similar level of expertise in the field of computer and information technologies (Çelik, 2018: 2).

As the world becomes increasingly digital, the importance of understanding threats in cyberspace cannot be overstated. Terrorists use cyberspace tools for propaganda, recruitment and fundraising with such ease that intelligence agencies are really struggling to keep pace. The common response from decision-makers has been to enact legislation and institute regulations, but these efforts have been largely reactive and uninformed, evidenced by their failure to mitigate the evolution of cyber threats – and even contributing to increased reliance on the dark net. Decision-makers must be given more information about cyberspace and its security, and the private sector is better positioned than the intelligence community to do this is.

Today, the security of states is directly dependent on technological developments. In this context, the states that do not have the technology in cyberspace face serious security weaknesses. In the same way, states need to reorganize all of their organizations and strategies, which are planned according to the classical security approach, to create an effective cyber attack and cyber defense capacity (Darıcılı, Özdal, 2017: 34).

With the democratization of information and communication technologies, it is observed that states use e-government, internet banking and internet technologies widely and encourage the use of these technologies by citizens.With the undisputed ties of critical infrastructures such as energy, transportation and the expansion of cyberspace, it is understood that only computer, software or network engineers cannot solve the problems that will arise in cyberspace. (Bıçakcı, 2014: 103).Cyberspace, the driving force of which is based on internet and network technologies, is now seen as a new area of struggle by the states.

Advances in science and technology in the 21st century have led to the emergence of new dimensions of security.Uncertainties in the international arena due to the effects of the globalization which gained momentum after the Cold War period, when the enemy was certain, the threats were open, and the appropriate response could be predicted, necessitated a series of changes in the security perception (Erendor, 2017: 114). Along with the process of change, it has become increasingly difficult to make an understandable, reliable and sustainable definition of the concept of security, or to put forward the limits and the framework that everyone can agree on.(Yorulmaz, 2014: 104)

In the same way, it is witnessed that people and technology come together and meet more quickly and unexpectedly than ever before. Tesla's integration of radar into cars, Delta Airlines's trace of luggage with microchips is an example. Cyber life zones emerge in line with the intersection and intensity of cybersecurity and human activities in daily life, which leads to the necessity to examine cybersecurity from a public security perspective. For example, in April 2016, Joshua Corman, Director of the Cyber Statecraft Initiative (CSI), which carries out studies focused on conflict, competition and international cooperation issues within the Atlantic Council, mentions three key features that help to separate cyber life zones;

The first is that cybersecurity weakness / failure can cause loss of life. For example, in February 2016, the Hollywood Presbyterian Medical Center was a victim of ransomware, and hackers / pirates were accidentally stuck in an electronic health record system.

The second is that cybersecurity errors can lead to loss of confidence in basic systems. Cyber habitats have greatly expanded the attack surface for cyber criminals, so that the simplest security researchers have proven their ability to penetrate into modern automotive systems. For example, the fact that drivers do not know who controls the wheels of the car means that they will be lost in the first place.

Thirdly, the failure of cybersecurity can seriously damage the financial markets, as well as the confidence in the government in terms of its ability to protect its citizens. For this reason, an approach that includes national-level strategies and best industry practices designed specifically for all systems, including aerospace, automotive, health, energy, etc., must be adopted beyond the protection of nuclear power plants, federal banks and electricity networks (Fairchild 2016)

In this context, the study of the impact of cybersecurity on national and international security has an important place in understanding the cyber attacks experienced in today's world.The answers of some basic questions should be sought by social scientists.

- Who are the actors?
- Are states new players in cyberspace? (New comers)
- What is the scope of cyberspace? Is cyberspace anarchic structure?
- What is the impact of the governance problem of cyberspace on the international-national security dimension? (Chochri, 2016:15).

Today, the importance of the approaches that evaluate the concepts of cyberspace and cybersecurity within the scope of international relations discipline is increasing. The main reason for this is that states see cyberspace as a new opportunity for the development of hard power. For this reason, the struggle between states on the cyberspace area is increasing and cybersecurity issues are considered as the subject of analysis of international relations discipline and security studies as never before.

In the context of international relations, cybersecurity, cyberspace, and cyber-power have been considered as “low policies”, especially in the context of international relations, in the past twenty years, in particular from a realist point of view. However, the Wikileaks

scandal, which has silently revealed the world through some of the secret documents, has proved that cyberspace is an inseparable part of national security and has pushed decision-makers to take a position against this new area (Clark, Choucri, 2013: 21).

In other words, large actors with dominant power in the land and sea cannot have enough capacity in cyberspace, and smaller or non-state actors can use the cyberspace much more effectively with an asymmetric dimension. The biggest advantage that the cyber world provides to small actors is that cyber weapons are much cheaper than conventional weapons, that criminals cannot be easily identified, and that an action in cyberspace can have devastating effects in the real world. However, in terms of traditional defense, the host is in favor of the defender in the struggle, in contrast to the conditions of cyberspace that we are in, the hackers and cyber criminals. For this reason, it has become invaluable for good cowboys, white hat hackers, states, armies and institutions operating in strategic sectors.

In recent years, cyber defense has been a concept that has come to the fore in defense strategies of great powers and last time at the Lisbon NATO Summit. Cyberspace and its components, such as traditional combat vehicles, can be a means of regulating state mechanisms, financial institutions, national energy and transport infrastructures and social morale.

Cyber warfare can also be defined as an asymmetric warfare. While one side is weak in terms of traditional facilities, it can be intelligent and wasteful and the other is cumbersome and rigid. The most important feature of cyber war and threat is its rapid development. The threat can develop so quickly that the action / response in the traditional strategy may be delayed. While cyber war is an inter-state dispute, non-state actors may also be involved in different ways. In cyber warfare, it is extremely difficult to activate the apparent and proportional power. The target may be a chamber serving only military, industrial, and civilian or various sectors, or only one of them, for example.

Today, when informatics is transformed into a large weapon, states also attach great importance to virtual weapons production. Informatics experts combine to prevent this new threat from the virtual realm. An unidentified instigator, a silent weapon, and an

unknown shooter. The last advanced continuous threat attack named "Stuxnet" has once again shown how hard it is to combat this abstract enemy, which leaves almost no trace in the back, letting the perpetrator and instigator disappear in the depths of the cyber world (Hein, 2010).

The third millennium shows that cyber wars are not a dream, but that in the near future states will be inevitably a battlefield where they will be dragged. In a 2012 speech, then-Secretary of Defense Leon Panetta warned Americans they could face a "cyber Pearl Harbor" someday at the hands of a terrorist group or enemy state. However, for the most part, cyberwar has not yet turned out that very—at least so far. The world has not yet seen nations use computers to launch surprise attacks on factories or refineries, set tanks on fire, bring down aircraft, or shut down an adversary's military. Nor have we seen terrorists use computers to wreak much destruction at all. Although cybersecurity expert Winn Schwartau introduced the concept of Electronic Pearl Harbor in 1991 and made early warnings, it is evident that the cyber threat can no longer be confined to WikiLeaks borders, even though Panetta's prediction has not yet taken place (Pollard, Devost 2016).

In short, one of the dominant elements in the operational environment of today and the future is cyber-space and its capabilities in this area are becoming more and more critical. However, as the cyber war is completely different from the conventional war, it is more complicated to acquire defense and attack capabilities in this area. At this stage, the five characteristics of cyber war are highlighted;

First, the weapons used in cyberspace space are a real war because they are equipped to turn a country into a ruin.

Second, the speed of the attack between the beginnings of the time interval does not allow measuring the speed of the time.

Third, any concealed attack on computers or servers is global because it can quickly and rapidly expose many countries to battle.

Fourth, the defense system and the critical infrastructure of the enemy country, which is located at any point in the world without going to the traditional battlefield, can be easily destroyed from cyberspace.

Fifth, uncertainty and thus instability are much more dangerous, as the time of war and the time of peace are all intertwined (Clarke, K.Knake, 2010: 31).

As can be seen, when the states that are considered to be an enemy are harmed in political, military and economic ways, the stock market and banking systems, electricity and water networks, military facilities or critical infrastructures can be the targets of cyber attacks. Moreover, the states can be directly or indirectly involved in industrial, economic, commercial and so on. They can also apply to cyber espionage activities through the hackers they employ for their needs, interests and purposes. The types of cyber warfare between Russia, the United States, and China and in part North Korea are exemplary.

In 2014, Hollywood had its share of cyber attacks, and Korean hackers who were violent against North Korean leader Kim Jongun and the satirical comedy The Interview, who hacked into Sony Pictures' computer systems. Hackers, Sony's five new films, scenarios, e-mail traffic, etc. While they shared important data on the internet, Sony decided to cancel the New York premiere of the film, and even the film's decision to restrict the screenplay was interpreted as hackers won the war and achieved absolute success and victory. (BBC News 2014)

Another example of the recent past, the DDoS attacks, which are considered the biggest and most powerful cyber attack in the history of the US launched in 21 October 2016, have once again revealed the importance of cybersecurity issues and the size of the damages caused by cyber attacks. It has been announced that all companies affected by the cyber attack are customers of DynDNS, which provides services that make it easier for users to find a site on the Internet. The attack began with dumping DynDNS into DDoS data. This has created an effect that makes it difficult for Internet users who use the service to reach the sites they are looking for and has reduced the internet speed throughout the country. The first impact of the attack was to make it more difficult for users to access more than 80 popular sites, including Twitter, Amazon, Reddit, Pinterest, Etsy, Github, Soundcloud, Spotify, Netflix, PayPal. In addition, the use of DynDNS by a large number of companies as a global address guide for worldwide users has made the attack much more effective and widespread (Lovelace, 2016).

Hillary Clinton's Republican rival Donald Trump's support of the annexation of Crimea following the cyber attacks on the computer systems of the Democratic National Committee (DNC), while controversies over the secret correspondence and documents leaked to the public's open access to the public's public access before the US Presidential elections in November 2016. The fact that he was accused of cooperating with Russian state hackers is quite striking. In fact, the Kremlin, which supported Trump's rope in the US presidential election on 8 November and first congratulated the win, was accused of succeeding in detaining Clinton's credibility with the national public opinion through a number of secret data he had acquired through Russian hackers during the 18-month election marathon (Crowley, Louis, 2018).

Even if we accept that the cyberspace is a new area of conflict, some fundamental questions about this new kind of war must be answered and a consensus should be reached. The questions that need to be answered in the first stage are as follows;

- Who and how will the time, space and borderless cyber attacks be detected before and after? How will the legal relationship between action and perpetrator be established, evidenced and proved?
- How will the process in this area work temporally and methodologically? Furthermore, how will the relationship between the person who leads the attack or the group and their governing relationship be established?
- If the person or organization is related to any state, how will it be connected to the government of that country? Under what circumstances will the government of the country be held accountable?
- How will the potential risk of damaging the security interests of potential attacks be measured and how the damage will be calculated after the attack?
- What kind of a weapon or technology system will be needed to respond to the attacks?
- Will states, which dramatically reduce defense budgets, be willing to meet the cost of cyber warfare and invest in that?

- In what ways do some of the undeveloped states of cyber-defense capabilities and capabilities have an effective deterrence against the threat of war or how much will they be able to carry out the necessary preventive actions?
- How will retaliation against cyber war be required? How will the use of military force or political and economic sanctions be connected to international law? How, when and in what proportion will the cyber attack detected be responded to by force?
- How will the shape and limits of the response to these attacks be drawn? How will the practice of resorting to the use of the provision for damages requiring the use of military force in international law be avoided?

Undoubtedly, it is difficult to answer the above questions clearly. Likewise, at the Warsaw Summit, which took place between July 8, and 9 2016, the Allies officially accepted the cyberspace as NATO's new domain of military operations. Subsequently, they also committed to developing their own national networks and infrastructures for the purpose of cyber-defense, and fulfilling their obligation to increase their ability and ability to rapidly respond to cyber attacks.In the same way, Alliance members negotiated to increase their cyber defense capacity and to integrate cyber-war policies in order to make new decisions. Given the cyber dimension of current crises and conflicts, it is foreseen that this decision will enable NATO to carry out its missions and operations more strongly (NATO 2016)

CONCLUSION

The impact of changes in threat assessments based on changes after the Cold War has a great effect. The threat assessments of states differ depending on different variables such as total power, intention perception, defense-attack balance and geographical proximity. When the security and strategy documents and threat assessments of the states are examined, it is seen that nuclear threats, asymmetric war, transboundary migrations and crimes, international terrorism and cybersecurity issues have come to the fore.

However, it is observed that the post-Cold War armies are changing their usage areas. When the usage of the armies of the states is examined, besides the protection of the country, areas such as the implementation of mobilization, peace support operation and humanitarian aid, defense diplomacy, domestic and foreign military assistance and internal security duties are seen. The fact that the armies can be used in different tasks and regions brings together different countries to operate together, and the use of different forces together, in other words, the need for unified and joint operations.

In the future studies of world vision; The National Defense area will gain importance in the second quarter of the 21st century and the countries that have improved in this area will have a say in the world. When we look at the studies in this field, we see six basic factors, especially the human factor that shapes the National Defense field. These are; asymmetric warfare, national security and counter-terrorism, advanced weapons systems, nuclear threats, cybersecurity, cyberspace and information systems.

Technological changes are seen in the other important factor that accelerates the changes experienced recently. The fact that many information is found on computers, servers with internet access, especially on the Internet, which has very fast propagation, increased connection speeds, and confidentiality information, has made the virtual environments unsafe. As a result, countries such as the USA, China, England, and Russia have created a structure of military cyber forces by adding the cyber environment as a dimension to the war environment. The reflection of this situation on the war was evident in the occupation of Georgia by Russia, and before the Russian ground operation, cyber attacks were carried out and Georgia's official and civilian Internet infrastructure collapsed.

In parallel with the Internet, the connection speeds between the electronic workstations have increased. With these concepts, it is envisaged that the army will collect, process, analyze and share information / intelligence from a single soldier to the decision makers at all levels.

Another aspect of developing technology is the developments in nanotechnology. Nanotechnological developments have begun to affect the security field in terms of electronics, cyber environments,

conventional weapons, self-serving robots, unmanned aerial vehicles and nuclear-chemical-biological weapons. In particular, the emergence of these new weapons and vehicles has brought an asymmetric threat. Because the armies that have these technologies can have advanced systems such as robots using artificial intelligence instead of human, cyber weapons that can be commanded remotely and micro robots that can self-destruct.

There is no managerial theory that can solve the problems and defense approaches of the armies in the modern world and in the future. The structure of today's world is more complex than yesterday. Successfully managing this structure is to have the work force that can accommodate both technical and human ability at the same time. Since the battlefield of the future will be a technology-human-based structure, it will not be wrong to state that the socio-technical approach is the basis of the solution. In this context, only human-based or only technical-based education design will not bring success in order to have armies in the cyber environment. The design of a well-designed teaching system is essential for a deterrent, strong and reputable army in the battlefield of the future as a structure capable of responding to social and technical requirements.

Because of the developments and changes mentioned above, the battle and the battlefield became more complicated. Within this complexity, the human factor of the level of cyber-war within the scope of the defense field is critical in the selection and training of human resources according to the roles and duties of the armed forces in the battlefield of the future. When this process of change and development is evaluated in terms of work force; it is foreseen that the armies will need cyber warfare, use unmanned aerial vehicles, understand and use network structures and will be able to use them in the future. In addition, there is a need for leaders who are able to manage these personnel, who have a common / unified vision and operational mentality and who understand the concept of network-centered operations.

At this point, it is possible to explain the shortcomings of countries, institutions and organizations in terms of cybersecurity, the weakness of communication between different parties (eg an engineer and social scientist) and the lack of sharing of knowledge and experience among

stakeholders (academia, industry and business). Multidisciplinary approach is needed to solve problems.

On the other hand, if we approach the subject with a historical perspective, it can be argued that the innovations in the military competition and space race experienced during the Cold War between the United States (US) and the Soviet Union constitute the foundations of cyberspace-based technologies. Nevertheless, the competition continued in the 1990s with a lower profile between the Russian Federation (RF) and the United States. However, along with the technological progress and economic development, including the People's Republic of China (PRC) in the 2000s, it has been involved in this competition. In this context, it can be claimed that cyberspace space based developments and USA, RF and PRC dominate technologies. The main motivation of this dominating process is that the states in question read the cyberspace as a new opportunity for power struggles in the international system.

In addition, while a global consensus on definitions such as cyber warfare, cyber terrorism and cyber weapons is difficult, there is still no question of international cooperation, global standards and norms for the peaceful use of cyberspace. The main reason for this is the competition processes mentioned in the cyberspace space of these global powers. It is clear that such a compromise would not be possible in the short and medium term, although the provision of such a compromise was essential for a peaceful administration of the international system. The use of an improved dictionary specific to the inter-state cyberspace or the use of a common and technical language can be presented as a recommendation. Such a consensus could also be instrumental in creating other areas of consensus for cyberspace space for future periods.

As a result, cyber-space has become an indispensable phenomenon with its great opportunities and facilities, and it has the potential to be a doomsday weapon with its threats and risks. In this respect, it has now gone beyond the fantastic scenarios of science fiction films and has become a reality of daily life through experiences. It seems that the new competition and battlefields of our age will be on this complex and unparalleled front.

REFERENCES

BBC News. "The Interview: A guide to the cyber attack on Hollywood", https://www.bbc.com/news/entertainment-arts-30512032 (Erişim: 04.08.2018)

Bıçakcı, Salih (2014). "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik". *Uluslararası İlişkiler,* 10(40), 101-130.

Chochri, Nazli (2016). "Explorations in Cyber International Relations: A Research Collaboration with MIT and Harward University". *Research Paper*, 2016(1), 15-16, Available at SSRN: https://ssrn.com/abstract=2727414 or http://dx.doi.org/10.2139/ssrn.2727414 .

Clark, David and Nazli Choucri (2013). "Who Controls the Cyberspace?". *Bulltein of the Atomic Scientists*, 69(5), 21-31.

Clarke , Richard and Robert Knake (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins.

Crowley, Michael and Nelson Louis (2018). "*Trump congratulates Putin after election branded a 'sham'*". Politico: https://www.politico.com/story/2018/03/20/trump-congratulates-putin-election-win-473604 (Erişim: 12.09.2018)

Çelik, Soner (2018). "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım". *Academic Review of Humanities and Social Sciences,* 1(2), 11-20.

Darıcılı, Ali Burak; Barış Özdal (2017)."Enformasyon Savaşı Bağlamında Rusya Federasyonu ve Türkiye İlişkilerinin Analizi". *İGÜ Sosyal Bilimler Dergisi*, 4(1), 19-40.

Erendor, Mehmet Emin (2017). "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu". *Cyberpolitik Journal*, 1(1), 114-133.

Fairchild, Ian (2016). "*Protecting Cyber Life Zones*". http://www.atlanticcouncil.org/blogs/new-atlanticist/protecting-cyber-life-zones (Erişim: 15.06.2018)

Hein, Matthias von (2010). "Siber savaş tehdidi artıyor". *Deutsche Welle Türkçe*. https://www.dw.com/tr/siber-savaş-tehdidi-artıyor/a-6058903 (Erişim: 01.07.2018)

Kaspersen, Anja (2015). "Cyberspace: the new frontier in warfare". *Geopolitics and International Security, World Economic Forum*. https://www.weforum.org/agenda/2015/09/cyberspace-the-new-frontier-in-warfare/ (Erişim: 12.09.2018)

Lovelace, Berkeley (2016). "Friday's third cyberattack on Dyn 'has been resolved,' company says." *CNBC News.* https://finance.yahoo.com/news/major-websites-across-east-coast-140324702.html (Erişim: 11.08.2018)

North Atlantic Treaty Organization (2016). "Cyber Defence Pledge" *Official texts*. https://www.nato.int/cps/en/natohq/official_texts_133177.htm (Erişim: 23.07.2018)

Pollard, Neal and Matthew G. Devost. (2016). "Is Cyberwar Turning Out to Be Very Different From What We Thought?". *Politicio.* https://www.politico.com/magazine/story/2016/08/is-cyberwar-turning-out-to-be-very-different-from-what-we-thought-214136 (Erişim: 12.06.2018)

Yorulmaz, Murat (2014). "Değişen Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde Değişmeyen Güvenlik Paradoksu". *Balkan Araştırma Enstitüsü Dergisi*, 3(1), 103-135.

ÖZET

Günümüz araştırmalarında siber güvenlik ve siber uzay olgusunun çalışma kapsamında ele alınış biçiminde, siber güvenliğin çoğunlukla bilgisayar odaklı enformasyon teknolojilerine ve uygulamalarına vurgu yapan "teknik boyutu" ile ulusal güvenlik kaygıları üzerinden siyasal ve hukuksal uygulamalara vurgu yapan "sosyal boyutu" arasında ciddi bir ayrım bulunmaktadır. Bu çerçevede, bir ülkenin ulusal güvenliğini bütüncül bir şekilde sağlamakla sorumlu olan üst seviye güvenlik karar alıcılarının; nasıl ki terörle mücadele kapsamında başvurulabilecek asimetrik çatışma ya da örtülü operasyon biçimleri konusunda uzmanlık seviyesinde teknik derinliğe sahip olmaları beklenilemez ise, bilgisayar ve enformasyon teknolojileri alanında da benzeri bir uzmanlık beklentisi içerisinde bulunulmaması gerekmektedir.

Günümüzde "siber uzay", kara, deniz ve havadan sonra birçok yönden kendine münhasır bir alan olarak ortaya çıkmıştır. Örneğin, İkinci Dünya Savaşı sırasında, Almanya'nın Enigma makinesinin şifrelerinin çözülmesiyle, Alman ordusuna yanlış bilgi akışı sağlanmış, savaşın kaderi Almanya'nın aleyhine dönmüş ve dünya tarihinin akışı değişmiştir. Bilginin kadim gücüne rağmen, "siber güç" ve "siber uzay" kavramlarının görece yeni birer güç unsuru olarak karşımıza çıktığı söylenebilir.

Ayrıca günümüzde devletlerin güvenliği teknolojik gelişmelere doğrudan bağlıdır. Bu kapsamda, siber uzay alanındaki teknolojilere sahip olamayan devletler ciddi güvenlik zafiyetleri ile karşı karşıyadırlar. Aynı şekilde devletlerin güvenliklerini sağlama noktasında, klasik güvenlik anlayışına göre planlanmış tüm kurum ve stratejilerini etkili bir siber saldırı ve siber savunma kapasitesi yaratmak adına yeniden organize etmesi de gerekmektedir.

Bir başka deyişle, kara, hava ve denizde baskın güce sahip olan büyük aktörler, benzer şekilde siber uzayda yeterli kapasiteye sahip olamamakta ve bunun aksine daha küçük veya devlet dışı aktörler siber alanı asimetrik bir boyutla çok daha etkin şekilde kullanabilmektedir. Siber dünyanın, küçük aktörlere sağladığı en büyük avantaj siber silahların konvansiyonel silahlara göre çok daha ucuz olması, suçlunun kolayca tespit edilememesi ve siber uzayda yapılan bir eylemin gerçek dünyada yıkıcı etkiler doğurabilmesidir. Bununla beraber, geleneksel savunma anlayışında, ev sahibinin yani savunma yapanın mücadelede avantajlı konumda bulunmasının aksine, içinde bulunduğumuz siber uzayın şartları hackerlar ve siber suçlulardan yana olmaktadır.

Son dönemde güvenlik anlayışında yaşanan değişikliklere hız kazandıran diğer ve önemli bir faktörde teknolojik değişimlerdir. Özellikle internetin çok hızlı yayılımı, bağlantı hızlarının artması ve gizlilik dereceli bilgiler dâhil

birçok bilginin internet erişimli bilgisayarlar ve sunucular üzerinde bulunması, sanal ortamları da güvensiz hale getirmiştir. Bunun bir sonucu olarak ABD, Çin, İngiltere, Rusya gibi ülkeler savaş ortamına siber ortamı da bir boyut olarak ekleyerek askeri siber kuvvetler yapılanmaları oluşturmuşlardır. Bu durumunun savaşa yansıması Rusya'nın Gürcistan'ı işgalinde açıkça görülmüş olup Rusya kara harekâtı öncesinde siber saldırılarda bulunmuş ve Gürcistan'ın hem resmi hem de sivil internet altyapısını çökertmiştir.

Modern dünyada ve gelecekte orduların problemlerini ve savunma yaklaşımlarını tek başına çözebilecek yönetsel bir kuram bulunmamaktadır. Günümüz dünyasının yapısı düne göre daha karmaşıktır. Bu yapıyı başarı ile yönetmek teknik ve beşeri yeteneği aynı anda bünyesinde barındırabilecek insan gücüne sahip olmaktan geçmektedir. Bu kapsamda siber ortamda orduların söz sahibi olabilmesi için sadece beşeri veya sadece teknik temelli eğitim tasarımı başarı getirmeyecektir. Uygun dizayn edilmiş öğretim sistemi tasarımı sosyal ve teknik gereksinimlere cevap verebilecek multidisipliner bir yapı olarak geleceğin muharebe sahasında caydırıcı, güçlü ve saygın bir ordu için elzemdir.

Yukarıda kısaca değinilen gelişmeler ve değişimler neticesinde güvenlik, savunma ve savaş kavramları karmaşıklaşmıştır. Bu karmaşıklık içerisinde, savunma alanı kapsamında siber savaş düzeyinde insan faktörü geleceğin muharebe sahasında silahlı kuvvetlerin üstleneceği rol ve görevler göre insan kaynağının seçilmesi ve eğitilmesi kritiklik önem arz etmektedir. Bu değişim ve gelişim süreci insan gücü açısından değerlendirildiğinde; orduların siber savaşı gerçekleştirebilecek, insansız hava araçlarını kullanabilecek, ağ yapılarını anlayıp kullanabilecek personele ihtiyaç duyduğu ve gelecekte de duyacağı öngörülmektedir. İlaveten bu personeli yönetebilecek, hem müşterek/birleşik görüş ve harekât zihniyetine sahip hem de ağ merkezli harekât konseptini kavramış liderlere de ihtiyaç bulunmaktadır.

Buna ek olarak, siber savaş, siber terörizm ve siber silahlar gibi tanımlamalar konusunda küresel bir fikir birliği yapmak zor olsa da, siber uzayın barışçıl kullanımı için hala uluslararası işbirliği, küresel standartlar ve normlar söz konusu değildir. Bunun başlıca nedeni, bu küresel güçlerin siber uzayda sözü edilen rekabet süreçleridir. Bu tür bir uzlaşmanın, uluslararası sistemin barışçıl bir şekilde yönetilmesi için gerekli olmasına rağmen, kısa ve orta vadede böyle bir uzlaşmanın mümkün olamayacağı açıktır.

Sonuç olarak, siber uzay büyük fırsatları ve olanakları ile vazgeçilmez bir olgu haline gelmiştir. Ayrıca tehditleri ve riskleri ile kıyamet günü silahı olma potansiyeline sahiptir. Bu bakımdan bilim kurgu filmlerinin fantastik senaryolarının ötesine geçmiş ve deneyimler yoluyla günlük yaşamın bir

gerçekliği haline gelmiştir. Görünüşe göre, çağımızın yeni rekabet ve savaş alanları bu karmaşık ve eşsiz cephede olacaktır.