Yönetim Bilimleri Dergisi/Journal of Administrative Sciences
Cilt/Volume: 22, Sayı/No: 53, ss./pp.: 852-875
DOI: https://doi.org/10.35408/comuybd.1360459

-RESEARCH ARTICLE-

NATIONAL SECURITY AND THE TOOLS OF CYBER POWER: THE AREAS OF STATES' HEGEMONIA

Gülşah ÖZDEMİR[1] & Soner KARAGÜL[2]

Abstract

In the post-Cold War era, in terms of international relations, 'cyber security' emerges as a significant security issue for the spheres of state sovereignty beyond the personal sphere. In addition to the harmful effects of cyber threats on the functioning of public institutions and organizations, it also raises a problem for states, such as managing perception operations by creating a society more open to manipulative influences.
In our globalizing world, the States' dependence on each other has increased. At the same time, there has been a period in which the fundamental security issues are intertwined for the States. In such a situation where the States cannot define themselves outside the system, classical realist approaches are insufficient to explain the changing -and increasingly abstracted-security areas. Nation-states must develop more complex skills and prioritize cooperation to deal with these new security threats. In our study, which focuses on the national cyber security perceptions of states, the measures taken by the States in the cyber world on priority issues, such as institutional functioning and survival problems, are analyzed in terms of national security strategies. On the theme of 'new security' the main focus is the necessity for actors to develop new defense capabilities within the 'quick response and easy adaptation' framework in the face of increasing and diversifying cyber threats. In our study, which deals with the efforts of digital Nation-states to increase their effectiveness in cyberspace in determining the 21st-century sovereignty areas and the increase in their tendency towards cyber warfare tools, the active/passive defense methods followed by the States in the perspective of cyber security strategies have been evaluated. In this context, it is the most acceptable method for the States to prefer the 'active defense model' to avoid cyber-attacks against vital institutions such as education and health.

Keywords: *Cyber security, Nation-state, Hegemony.*

JEL Codes: *F50, H56. N40*

Başvuru: *14.09.2023* **Kabul:** *10.07.2024*

[1] Assis. Prof. Dr.,Balikesir University, Burhaniye Applied Sciences Faculty, Balikesir, Turkiye, gulsah.ozdemir@balikesir.edu.tr, 0000-0001-8900-2560
[2] Prof. Dr., Canakkale Onsekiz Mart University, Biga Faculty of Economics and Administrative Sciences, Canakkale, Turkiye, sonerkaragul@comu.edu.tr, 0000-0003-2842-0691

SİBER GÜÇ ARAÇLARI VE ULUSAL GÜVENLİK: DEVLETLERİN HEGEMONYA ALANLARI [3]

Öz

Soğuk savaş sonrası dönemde uluslararası ilişkiler açısından 'siber güvenlik' kişisel alanın ötesinde devlet egemenlik alanlarına yönelik de oldukça önemli bir güvenlik meselesi olarak karşımıza çıkmaktadır.
Siber tehditlerin kamu kurum ve kuruluşlarının işleyişine yönelik olumsuz etkilerinin yanı sıra, manipülatif etkilere daha açık bir toplum yaratmak suretiyle devletler için algı operasyonlarını yönetmek gibi bir sorunsalı da ortaya çıkardığı bilinmektedir.
Küreselleşen dünyamızda sistemin en önemli aktörü olarak devletlerin birbirlerine olan bağımlılığının arttığı ve aynı zamanda devletler açısından temel güvenlik konularının da iç içe girdiği bir dönemi beraberinde getirmektedir. Devletler nezdinde kendini sistemin dışında görme durumunun mümkün olamayacağı böylesi bir ortamda klasik realist yaklaşımlar değişen –ve gitgide soyutlaşan- güvenlik alanlarını açıklamada yeteriz kalmaktadır. Ulus devletlerin bu yeni güvenlik tehditleriyle baş edebilmek için artık daha komplike beceriler geliştirmeleri ve işbirliğini ön planda tutmaları gerekmektedir.
Devletlerin ulusal boyuttaki siber güvenlik algılamaları üzerine odaklanan çalışmamızda, kurumsal işleyiş ve beka sorunları gibi öncelikli konularda devletlerin siber düzlemde almış oldukları önlemler, ulusal güvenlik stratejileri nezdinde incelenmektedir. 'Yeni güvenlik' temasında aktörlerin günden güne artan ve çeşitlenen siber tehditler karşısında 'hızlı cevap ve kolay adaptasyon' mantığı ile yeni savunma yetenekleri geliştirmelerinin gerekliliği üzerine odaklanılmaktadır. 21. yüzyıl egemenlik alanlarını belirlemede dijital ulus devletlerin siber uzayda etkinliğini artırma çabaları ile siber savaş araçlarına yönelme eğilimlerindeki artışın ele alındığı çalışmamızda devletlerin siber güvenlik stratejileri perspektifinde izledikleri aktif/pasif savunma yöntemleri değerlendirilmiştir. Bu bağlamda bilhassa devletler için –eğitim ve sağlık gibi- hayati kurumlara yönelik gerçekleşebilecek siber saldırılardan kaçınmak amacıyla 'aktif savunma modelini' tercih ediyor olmaları en kabul edilebilir yöntem olarak karşımıza çıkmaktadır.

Anahtar Kelimeler: *Ana Siber güvenlik, Ulus devlet, Hegemonya.*

JEL Kodları: *F50, H56. N40*

"Bu çalışma Araştırma ve Yayın Etiğine uygun olarak hazırlanmıştır."

1. INTRODUCTION

Hegemony refers to the relationship between dominant classes and classes subject to the dominant since Ancient Greece. In political, economic, cultural, and military fields, hegemonic relations can be experienced between individuals, classes, groups,

[3] Genişletilmiş Türkçe Özet, makalenin sonunda yer almaktadır.

or states. Today, there is no doubt that technological capacity can create a hegemonic relationship.

In the modern sense, Antonio Gramsci's approach to hegemony is widely referenced. Grasmci, who introduced hegemony to political philosophy, sought an answer to the question of "how the elite minority can control the majority without resorting to violence" with the concept of consent. The situation, also referred to as forced consent, occurs due to both the subject's power and respect for the hegemon.

In the International Relations literature, hegemony has been used since the early 1970s, adapted from Gramsci by Robert Cox (Özçelik, 2005:95). The distinctive aspect of hegemony in international relations is that the dominant international actor/actors exert influence on international politics by consent when necessary and coercion when necessary. International actors that create influence can be powerful states and various international organizations, political communities, economic organizations, and NGOs. On the other hand, as Cox states, the international hegemonic class, which exists outside the states, imposes its ideology, strategy and joint actions on other actors, especially its followers (Cox, 1993:49).

Realist, liberal, critical and system analysis approaches in the International Relations literature have each offered their unique perspectives on hegemony. This diversity of views underscores the complexity of the international hegemonic structure, which is not simple enough to be explained by a single theory. Among these approaches, the Hegemonic Stability Theory stands out, offering a thought-provoking argument that the international system will remain stable in the presence of a single hegemonic power. This approach has raised intriguing questions about the stability of the world economy after the Second World War and the role of the USA in this stability (Körpe, 2022, 267).

The Neoliberal (Liberal Institutionalist) Approach, which argues that international cooperation is possible with the contribution of international institutions and regimes, is based on neoliberal economic principles, namely that the international system can remain stable in the absence of a hegemon. Nevertheless, the hegemonic actor is the founder of the system and has weight in determining its rules, encouraging participation in the system, and maintaining stability. Due to this role, stability can continue even if the hegemonic actor declines.

According to the neo-Gramscian hegemony approach, there are shifts in the system's center due to the expansion of the spheres of influence of non-state actors within the international system. On the other hand, a new hegemonic world order is being established. The main point that the representatives of the World Systems Approach agree on regarding hegemony is that it is a cyclical process in which actors with hegemony experience power accumulation and loss in various areas. It is a recurring cyclical process, with states gradually weakening after reaching their maximum capacity for exerting hegemonic power, and another state becoming a hegemonic power. In a sense, the Cold War ended when one of the two competitive hegemonic powers broke away from the race and the other became the sole hegemonic power. The developments after the September 11 trauma of the USA and the hegemonic

tendencies of states such as Russia and China can be considered signs of a new cyclicality.

The areas of hegemony for states are determined by a variety of factors, including economy, military power, cultural influence, and science and technology. In today's world, technological capacity plays a crucial role in creating hegemonic relations. A state's success, particularly in the field of science and technology, can significantly enhance its hegemony capacity. States can establish technological superiority and hegemony through their high-tech products, patents, and research and development activities.

The issue of cyber security, which has recently been mentioned in international relations in terms of both its scope and impact, emerges as a new conflict area with the effect of technological developments and space studies. Cyber threats increase the problems of international security exponentially, in terms of the involvement of various actors in the global system and suddenly creating a perceptible effect all over the world. In the new environment, where the boundaries of sovereignty drawn by the traditional hegemonic understanding have become unclear, it has become necessary for all international actors to adapt to the new security environment.

According to the international relations literature, it is seen that new approaches to security emerged in the post-Cold War era (Baylis, 2008:71). The Cold War period, in which national security concerns were the main determining factor in interstate relations, brought cyber security to the forefront with the use of various technological tools related to intelligence, such as space races and spy planes developed between the two main actors of the system and data transfer methods. The shift of attack and defense to the digital environment makes the cyber world an essential field of study for international relations.

For the countries under the NATO security umbrella, which was shaped by a symmetrical threat perception during the Cold War period, the security dimension has changed with the disintegration of the USSR, and cyber attack and threat dimensions have been added to conventional and nuclear threats in the changing world. Globalization and technological developments have not only made all the actors in the international system more connected to each other but also changed the direction of the threats. Multi-actor threats have replaced threat perceptions developed only among states, and the necessity of creating a defense and deterrence mechanism beyond conventional defense has emerged to combat such formations.

Classical security definitions of the Westphalian order, in which security is defined in proportion to the military capacity and power of the states, are insufficient in today's world, where the threat is diversified. Especially in today's world, epidemic diseases, environmental and climate problems, migration, and famine problems have greatly expanded the scope of security. Thus, threats in the cyber world are another critical area faced by the actors in the new security theme shaped by these variable dynamics.

In addition to armed conflicts in the fields of land, sea, air, and space, encounters between different actors in the international system have started to take place in

cyberspace for the last two decades. The cyber world, which has begun to be accepted as the fifth-dimension hegemony area with the increasing effect of technological developments, appears as a new artificial conflict area (Worth, 2015:177-178). Since it is an asymmetrical attack method that has the capacity to affect various fields such as communication networks, information, and information systems, energy, and transportation sectors, cyber-attacks are occurring in quite ordinary, complex, and damaging dimensions today. In the face of these asymmetrical attacks, where the defense capability of foresight, disarmament, and deterrence is complicated, Nation-States have become obligated to include cyber security policies in national security issues and take deterrent proactive measures.

Every passing day, in the face of the States' efforts to draw their borders in the cyber world and to define their space races, it is considered necessary to examine the national security strategies of countries that reveal their goals and purposes in the cyber world within the framework of the securitization of cyberspace. As a study carried out for this purpose, the examples discussed were preferred in terms of population density, internet structures, and security concepts; the evaluations of the actors in our study were analyzed in the light of national security strategy documents.

2. SECURITY AND THE CYBERNETIC TRANSFORMATION

Due to the undeniable increase in the place of computers and the internet in today's world, it has become common to encounter 'cyberization' tendencies and technological variations of each phenomenon in many subjects, from education to health. Contrary to what is thought, a clear definition of cyberspace, which offers a virtual reality outside the physical world in many fields such as communication, services, and finance, cannot be made far beyond just computer and internet relations (Fang, 2018: 12-15).

It is seen that the word cyberspace, which was first mentioned in William Gibson's short story 'Burning Chrome', appeared as an imaginary and futuristic concept describing an urban area with problems such as crime, social exclusion, and poverty (Kneale, 2004: 218). The meaning of cyberspace as the definition of a new world has been discussed in institutions and organizations such as the Central Intelligence Agency-CIA, the National Security Agency-NSA, and the Russian-American Cyber Security Summit.

As a matter of fact, according to the definition in the Draft Cyber Security Strategies of the Russian Federation (CCDCOE, 2014) which is closely interested in the field of cyber domination after the area of space domination, the concept of cyberspace as "a global space where information technology infrastructures including computer systems and the internet are located", means "the ability of people to be connected to each other without any limitations through telecommunications". According to the US Department of Defense, cyberspace is defined as the electronic environment in which information is created, transmitted, received, stored, processed, and deleted (DOD, 2021). According to both definitions, cyberspace means the combination of internet

and telecommunications technologies that allow information to be recorded, stored, received, and transmitted.

The concept of cyberspace, which defines a new world full of uncertainties, includes opportunities and innovations as well as vulnerabilities, threats, and risks and also expands the digital divide and virtual inequality between developed and developing countries beyond the effect of interpersonal communication (Crowther, 2017: 66).

According to prominent geopolitical writer Colin Gray, creator of the Modern Strategy book, "In common with the land, sea, air, and space environments, the electronic realm of cyberspace is a[designated combat zone...' Cyberspace' is another 'geographical' zone for…strategy to be considered"(Gray, 1999: 268). Accordingly, cyberspace is thought to have conflict areas just like the other four hegemony approaches. The only difference is that the hegemony area of cyberspace is the electronic world, and the borders of this world are pretty comprehensive.

Air and space domination approaches, which have been added to the land and sea regions, which have been seen as the most basic domination area in the history of humanity, have been the determining physical areas for the hegemony borders of the states in the military and commercial sense for years. A new generation fifth dimension has been added to these four 'domain areas', which offer approaches based on the dominance of the physical areas covered by the Cosmos: Cyberspace (Clarke and Knake, 2019: 237-240).

In the cyber world, which is accepted as a new battlefield in the fifth dimension after land, air, sea, and space dominance, states should take precautions against terrorist groups that want to carry their illegal activities into this environment, as well as prevent negative situations such as theft and fraud that can only occur against their citizens (Orend, 2014: 15). At this very point, we have another question about the States' response to cyber-attacks: 'How, when and how is an active defense against cyber-attacks an appropriate solution?' So much so that protection-oriented/passive cyber attacks such as antivirus software for individuals and companies. It is seen that the defense methods need to be more sufficient for the cyber threats, that the states need to take vital precautions, especially the survival problems. Considering this situation, the necessity of States to focus on developing their cyber defense capacities for proactive measures targeting the source of the attack emerges.

Considering that wars in today's world are not only fought by military means, the existence of software and computer programs that disrupt all public functions, from health to education, causes states to perceive the cyber world in the dimension of sovereignty on a political plane. Cyber attacks, which have become the main agenda items for the security of countries and individuals, are becoming a widespread threat to State sovereignty in the 21st century. All of the actions and technologies applied against the risk of malicious attacks against the cyber assets of people, institutions, or users operating in the cyber environment can also be interpreted under 'cyber security'.

For the definition of cyber security;

• Defense methods used to detect and prevent possible intruders (Kemmerer, 2003: 710),

• The necessity of protecting computer networks and their contents (Lewis, 2006),

• Reducing the risk of malicious attacks on software, computers, and networks (Amoroso, 2006: 165),

• All of the tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, training, good practices, and technologies used to protect the cyber environment (ITU,2009),

• The ability of cyberspace to protect or defend against cyber attacks (CNNS,2010),

• The art of ensuring the existence and continuity of a nation's information society (Canongia,and Mandarino, 2014: 65),

• Ways and means to prevent and prevent unauthorized use of electronic data (Oxford Online Dictionary, 2014),

• Protection and restoration of electronic communication systems and services, communication networks, and computers against threats (NIST, 2020),

• Actions to prevent damage, unauthorized use, and abuse of electronic information and communication systems and the information they contain are currently used (Hogan & Newton, 2016).

In line with these expressions, in addition to seeing that the definition of cyber security is focused on electronic databases and communication, the problem of how effectively the operational activities to ensure security against electronic-based threats can be used by the States continues.

For these types of cyber threats, whose borders and perpetrators are often seen as unclear to state sovereignty areas, in today's conflicts, in which cyber weapons come into play beyond traditional military operations, the transitivity between a regular military operation and a cyber military operation also draws attention. For example, while the Iraq War takes its place in the literature as a conventional war, Georgia (2008) and Ukraine (2014-2022) appear as a hybrid conflict area in which both traditional vehicles and the cyber world are included. In addition, Stuxnet (2010) and Aramco (2012) can be defined as complete cyber operations.

Computer networks in the world and everything they control are within the scope of cyberspace, and the Cyber world, as a new domination area created by human beings, differs from the other four domination areas. This new and man-made domain of domination cannot be made politically clear regarding its natural and geographical

boundaries. Due to the lack of borders and fast communication, threats and risks in the cyber environment are equally unlimited and immediate.

In terms of being able to exist simultaneously in different geographies in various countries, elements of cyberspace have brought problems for new security perspectives in the context of national borders. Cyberspace, which means a virtual computer world, offers opportunities to users in a wide variety of areas, such as information sharing, communication, playing games, socializing, doing business, and creative visual designs. While the development in the information world and the rapid increase in internet use offer people various freedoms, they can also make personal data or system equipment vulnerable to threats from time to time.

The new perception of security in the cyber world occurs at the level of national borders and sovereignty on the basis of nation-states. The nation-state in the Westphalian order could define and access any external actor entering its borders when necessary. However, being aware of the attacks on banks, hospitals, vehicles, and public services on the virtual platform and predicting the potential losses due to these attacks are among the factors that increase the cyber security concerns of nation-states. So much so that it has become a necessity to be able to respond to cyber-attacks, especially for states such as the USA, which are likely to be the target of cyber threats (Stoffer, 2022). Increasing its own institutional and technological capacities means creating a barrier against attacks and drawing nation-state borders in cyberspace.

3. HEGEMONIC SECURITY OF STATES AND THE CYBER ENVIRONMENT

In the historical process, within the framework of new security understandings after the Cold War, there have been changes in security perceptions as well as the main problems of countries in international relations. Gaining the ability to access and control energy resources within the scope of gaining power emerges as the main theme of the struggle in the 21st century. The new geopolitical equations that have arisen due to the gradual erosion of the world's geopolitical codes and equations have made it necessary to reconsider the interstate role, partnership, opposition, and interests. These emerging new definitions of security can be reshaped within the framework of the same aims of establishing hegemony in different fields of struggle (Özçelik, 2018: 8).

Hegemonic security, underpinned by a robust international economic order, is upheld by a hegemonic state, ensuring international order, security, peace, and freedom. The Cold War era saw the emergence of a stable hegemonic structure, largely maintained by the interaction of hegemonic states like the USA and the USSR, and the subordinate states that consented to it. The post-Cold War era, marked by significant events such as the 1991 Iraq War, saw the USA redefine the hegemonic understanding of security, bringing a fresh perspective to global issues (Körpe, 2022: 274). The international system, which began to be reshaped with the millennium, has made inevitable changes in the hegemony areas and security approaches of international

actors, especially states. Although the main basis for the USA to be a hegemonic power since the second half of the 20th century is its military superiority, the importance of technological capacity is undeniable. One result of the USA's hegemonic understanding of security being exposed to cyclical effects is the hegemonic decline experienced after September 11 (Körpe, 2022:277). The September 11 attack necessitated a change in the US's hegemonic understanding of security. Although the USA's sole hegemonic power position as the winner of the East-West struggle has been shaken, its undisputed superiority in military terms continues.

Air dominance approaches based on air power, which emerged after the Second World War and provided greater ease of transportation, led to radical changes in the defense strategies of countries. In particular, the development of aircraft systems and the emergence of new combat systems have led to the discussion of the concepts of space domination in addition to the air domination approach. Today, the fact that technology is an integral part of our daily lives and the development of information technologies have made people dependent on this technology in many respects. IT products such as computers, the internet, mobile phones, and satellites are among the indispensables of daily life. When we look at the distribution of internet usage in the world over the years, it is seen that the figure, which was 5.18 billion according to 2023 data, has increased rapidly compared to previous years. We can talk about the number of users, which was 4.9 billion in 2020, 3 billion 753 million people in 2018, and 2 billion 831 million people in 2015, just three years ago. The increase in numbers in such a short time shows how fast the spread of the internet is in the world (Statista, n.d.).

While digital transformation, which has accelerated in almost every field with the effect of the Covid-19 pandemic, offers many opportunities for us, it also brings various risks. At a time when information and data are more important than anything else, cyber-attacks emerge as one of the biggest threats the world faces. Cyber-attacks target not only states and government institutions but also aviation, scientific research organizations, oil and petrochemical industries, internet infrastructures, and large companies. States with strong intelligence networks, such as the USA, are claimed to have transformed the espionage activities of the Cold War period into today's cyber hegemony activities through various tactical actions.

Technology not only makes our lives easier, but also opens up new areas for us to learn and pay attention to. Cyber security is one of these issues. It should be noted that today, there are many institutions that have transferred their data to the internet under the influence of digitalization, as well as many cyber attackers infiltrating networks to obtain this data.

The increasing use of internet-connected devices in human life increases the risk of being exposed to security breaches at the same rate. Ensuring the confidentiality, integrity, and accessibility of information is essential for the cyber world's security. Situations such as using information only by persons with access authorization, being

aware of sensitive information, and the fact that the original data has not been lost or changed can be counted as the basic requirements of cyber security.

In today's world, where digital security is as important as physical security, cyber-attacks carried out by illegal individuals or groups with malicious software now directly target institutions that host the data of thousands or even millions of people.

Cyber-attacks, which develop as "planned and coordinated attacks on the information and transmission systems and critical infrastructures of targeted individuals, companies, institutions, organizations, and the state", can have methods such as infiltrating computer systems, stealing information from systems, and putting false information into systems (National Institute of Standart Technology, n.d.). Cyber-attacks, which can be commercial, political, or military purposes, are made to the extent that they damage a country's critical institutions, communication and computer systems, energy and transportation networks, and military command and control systems, and it is a form of asymmetric warfare and is called cyber warfare (Clarke and Knaake, 2019: 182-183).

Internet technology, which has penetrated many areas, is the greatest reality of the 21st century. Artificial intelligence, hypersonic technologies, and autonomous vehicles… Digital tools create elements that will affect the nation-state structures of the future not only in the context of citizens in social life but also in the context of state institutions. The new generation of digital nation-states, on the one hand, accelerates their tendency to increase digital literacy; on the other hand, they try to develop digital protection methods against cyber-attacks against their institutions. In today's international system, it is seen that the main actors who can develop various satellite technologies add to their national cyber security strategies to have cyber warfare tools instead of conventional weapons.

We see that the foundations of cyber wars, which we discuss with technological advances, were laid during the Cold War. With the production of the first personal computers in the 1980s, the demilitarization of the internet, which started after the Cold War, brought commercialization. The unstoppable trend of mobile phone technology in the 2000s has included the internet in every aspect of life. In addition to this development, the internet-based restructuring of systems that we call some critical infrastructures such as health, education, and defense in terms of nation-states has brought about differentiation in the security dimension.

Considering that today's countries are actively using technological weapons to shape the future, it is known that nation-states such as the USA, Russia, China, Israel, and the UK not only use national defense against cyber-attacks but also use hackers for active defense. It is known that the USA continues to host large companies that are information and technology giants. However, China has recently been making progress that challenges the leadership of the United States, thanks to the high technology companies that are developing and growing stronger in its country. This

poses a significant threat to the USA's technological leadership, especially in the fields of robotics, space exploration, and artificial intelligence (Slawotsky, 2017:121).

When we look at the wars of Estonia (2007) and Georgia (2008), which are called the first cyber wars, the cyber-attacks carried out by Russia against these two countries in order to prove its cyber power resulted in the interruption of the services, financial transactions and communication of the official institutions in the countries for three weeks (AFCEA, 2012). In addition to these two countries in the Russian sphere of influence, the US Department of Defense has recognized cyber-attacks as a cause of war, with the leak in the US command center where the Iraq and Afghanistan wars were waged in 2008.

The response to Russia's cyber-attacks by the USA expanded the field of cyber warfare, and this time, a cyber-attack was carried out with spyware called Stuxnet (Chen, 2014: 5), targeting Iran's nuclear facilities, which is a country of symbolic importance for Russia. In return for this incident, Iran confirmed that the USA carried out cyber-attacks against Ghost Aircraft Technology, Unmanned Aircraft Communications and Missile Targeting Technologies, Electromagnetic Pulse Dam and Missile Attacks, and the US and Israel Military Bases.

As can be seen, cyber-attacks that overgrow like a spark and can envelop an entire country in its sphere of influence also clearly allow the parties to retaliate due to the ambiguity of where and by whom.

Computer technologies, which became civilian and commercialized after the Cold War, allowed states to develop their military capacities with the possibilities of cyberspace and paved the way for states, organizations, and institutions to produce security strategies to increase their cyber-attack/defense capabilities. Naturally, to improve the functionality of cyber defense mechanisms and build a sustainable defense mechanism, nation-states have created facilities and structures for cyber defense, which they have entered into various institutionalizations. In this context, in terms of cyber defense, the USA, Russia, China, Iran, Israel, and the UK are among the countries that rapidly increase their security capacities. They present examples of the rapid transition from terrestrial borders to cyber borders in the world of the future with their national cyber security strategies.

The USA, which evaluated its cyber security strategy as a continuation of its hegemony until the early 2000s, has tended to expand its military and intelligence targets in order to provide cyber security. The basis of this trend is Russia, which tends to increase its military capacity with the increase of threats originating from China in the context of cyber espionage capacity and the possibilities of cyberspace. Due to its federal structure, the US cyber security strategy has been shaped by the influence of the Presidency's directives as well as the documents of the relevant institutions and organizations.

In this context, if we look at the US cyber security strategy, it is possible to increase the private sector-public cooperation in order to protect critical public infrastructures, to establish a federal system in order to reveal common tactics and plans, to raise awareness of the entire society against cyber-attacks, to take technical and administrative measures from Russia and China at the global level (MacGibbon, 2009: 2-3). It is seen that it draws a framework in the form of struggle. There is now a cyber security strategy shaped by the US decision-makers, who are united in the view that having a good army equipped with conventional weapons is not enough. Considering that 12 million dollars are spent to fight cyber wars in the USA-according to the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the idea that future security doctrines will be built on cyber armies can now be considered beyond possibility. In addition, it is known that the USA, which allocates $10.9 billion to cyber security institutions in its 2023 fiscal budget, is tending to form an army in this field (Office of Management and Budget, 2023). Since the term of President Clinton, the USA has taken several initiatives to maintain its hegemony in the cyber environment:

- Developing aggressive strategies against non-allied countries,
- Launching cyber missions
- Keeping the cyber-space left in instability under control in a position that determines the rules by following an aggressive security strategy.

While the US's intention to become a hegemonic cyber power is evident from the comprehensive and aggressive cyber security strategies it pursues, countries such as China and Russia are disturbed by this situation (Nan, 2024).

After the Afghanistan War between 1979-89, the Russian cyber strategy, which aimed to develop the armed forces with network technologies, was started as a security-based initiative in the areas of close domination. The cyberization tendencies in this security and military bureaucracy emerged with the intense use of network technologies in the Chechen War of 1994-1996 (Pernik, 2018: 53). Russia, which has developed its aim of expanding its military power, especially after the 2000s, by taking advantage of the technological infrastructure features of the Soviet period, has made investments in cyber-attack/defense, intelligence, network technologies, and social media. In this way, it aimed to develop its broad information war capability to become a global cyber power. Russia, which tends to use the innovations and opportunities provided by cyberspace to achieve its foreign policy goals, has carried out cyber-attacks against the regions where it has problems in foreign policy. It is known that based on the 'Information Security Doctrine' adopted by President Putin in 2000, it carried out hybrid attacks in Estonia in 2007, Georgia and Lithuania in 2008, and Kyrgyzstan in 2009, using new technologies intensively through its cyber power (Pernik, 2018: 54-56).

Especially nowadays, Russia, which is making a serious effort to have a comprehensive information warfare capability covering activities and plans such as cyber espionage, cyber contraception, disinformation, electronic warfare,

psychological warfare and propaganda, and cyber-attack, follows the path of using non-military methods in hot conflict areas. Another important goal for Russia, which focuses on internet control/management issues to steer conflicts with less conventional power and less construction loss, has been to break the global hegemony of the USA in this area. It has developed its national software and hardware for this purpose, offered domestic social media applications to young people, and set up domestic antivirus programs by increasing internet controls (Jasper, 2020: 52).

It is seen that Russia, which has sought to expand its cyber dominance to solve its foreign policy problems, has been carrying out an active cyber war strategy during the annexation of Crimea in 2014 and the Donbas War, which has lasted until today. In the process leading up to the main war, the blockades against the infrastructure/system of the target country and the disinformation activities that wear out its soldiers, it was ensured that the cyber-attacks in Ukraine were carried out effectively in favor of Russia (Pernik, 2018: 60-64). It is known that Russia, which uses the opportunities offered by new technologies as a strategic foreign policy tool, has turned the region into a testing ground to establish a cyber weapon arsenal[4] in addition to the conventional attacks it has carried out in Ukraine since February 24, 2022. Following Russia's 2014 annexation of Crimea, there was a significant increase in cyber attacks against Ukraine. Almost a quarter of a million Ukrainians were left without electricity in a series of cyber attacks on the main distributor power plant in Ukraine in 2015-2016 (EPRS, 2022). In June 2017, Ukraine's government, financial and energy systems were first targeted with the NotPedya malware attack.

Russia, which sees this rapprochement between NATO and Ukraine as a major threat to itself, was accused of rendering dysfunctional many public institutions and organizations, such as Ukraine's Ministry of Foreign Affairs and the Ministry of Education, with a series of cyber attacks in the 2022 war.

The Russian Main Intelligence Directorate (GRU) and Russian state-backed hackers are turning the region into an active cyber warfare area with malware to render Ukraine's information communication networks and infrastructure equipment dysfunctional (Kolbe, 2022). It can also be seen from the examples given that the Russian Federation, which heavily refers to cyber security in its current strategy documents, intensively uses its capacity-building activities in cyberspace, especially in its relations with its neighbors.

When we look at China, an essential power in terms of its population and area, it can be said that it is a country that other states have closely followed in recent years with its rapidly developing military and economic infrastructure. Considering that 988 million of the 4.9 billion internet users worldwide are in China (Statista, n.d.), the impact of China's national cyber security strategy, as a nation-state capable of dominating cyberspace space, is globally significant.

[4] Arsenal is a space for developers to showcase the latest open source tools and products. Here, this situation can be described as the area where the equipment of cyber forces is put into practice.

The basis of China's cyber security strategy is to protect its economic, political, and military institutions. In terms of internal security, China, which tends to develop its cyber capacity in the field of defense, has to create and redesign this capacity in terms of cyber espionage. It is stated that the acquisition of new-generation technologies is considered necessary by the Chinese authorities in terms of the adequate power of such technologies in espionage operations (Volz and Viswanatha, 2018).

The importance of the country's administration to maintain internet control and control against information wars and espionage activities that may be directed against them from other countries, as well as social control, should be discussed. It is possible to state the new generation technological opportunities for the infrastructures of critical institutions and organizations in the target regions, as well as counter-espionage and cyber-attack planning as other important sub-headings in national cyber security strategies. It is seen that China, which is on the same level as Russia, with its national software, hardware, and smart phones in the face of a US-based global hegemony in the cyber world, draws the arrows of criticism from Western states with its strict internet controls and censorship. China's oppression and censorship policies, which prevent its citizens from communicating with the outside world in the virtual world, are carried out to control opposition groups and maintain their national hegemony in the virtual world.

It can be said that the document titled "National Cyber Security Strategy 2016-2021" reveals the basic cyber security policies for the UK, which sees the most prominent threat source in terms of its economic interests and national security as risks originating from cyberspace. In this direction, the UK is locked into three objectives that offer a series of action plans for cyber threats on the basis of Defense-Deterrence and Development. Instead, this action plan envisages public-private sector cooperation in terms of strengthening the information infrastructure and defending against threats (Bird, 2020: 4). Supporting the development of the cyber security industry can be considered within the scope of meeting the development-oriented target for the British government, which sees strengthening the existing active-passive resistance elements in the cyber field as an effective deterrent.

In addition to strengthening the infrastructures of areas that are most exposed to cyber threats, such as financial institutions, banks, insurance companies, telecommunications companies, and tourism agencies, starting international cooperation processes in this field, especially NATO and the EU, are considered important targets for UK cyber defense policies.

For Israel preferred to develop effective defense methods due to the security conditions and threat perceptions of its region, the basis of the defense strategy adopted by the then Prime Minister David Ben-Gurion in 1953 was to create deterrence. When we evaluate the issue in terms of cyber security, it is seen that Israel, which finds the public-private sector partnership and cooperation of academic circles critical, focuses on early warning systems by focusing on R&D studies in the name of cyber security.

For Iran, another country in the same geography with similar security problems, the Stuxnet attack targeting its nuclear facilities in 2010 was a significant turning point regarding cyber defense. Iran, which wants to take advantage of the asymmetrical advantages provided by cyberspace against powers such as the USA, Saudi Arabia, and Israel in its region, has followed a national security strategy to increase its cyber-attack capacity in the first place. With its retaliatory operations, the Iranian Cyber Army emerges as the central umbrella organization for determining cyber policies (Anderson and Sadjadpour, 2018: 9).

It is a fact that the threat levels increase faster than the defense capabilities, as well as the extensive resources allocated from their own budgets by the states to provide cyber security, not only in terms of the States covered in this study but also around the world. Considering that cyber continental shelf and cyber integration models will be discussed frequently in terms of nation-states in the coming days and the concept of cyber homeland will be on the agenda more, the necessity of expanding the security concept to include national cyber security emerges. The actions of states, such as predicting possible attacks on their own cyber borders, intervening simultaneously, and creating protection programs to control cyber-attacks, can be effective methods to stop potential attacks against them in the cyber world.

CONCLUSION

E-commerce, E-export, E-government, E-diplomacy, and E-war, within the 'future' international system, which is completely dependent on the infrastructure of internet technology, puts states and their citizens in an 'e' state. Information systems, consisting of data formation, storage, and protection, are at the center of cyberspace. Smartphones, smart homes, smart cities… In an era where everything is interconnected, we are 'connected' in every aspect of our lives. Considering that 7.33 billion of the world population of more than 8 billion are mobile phone users and 5.18 billion of them are internet users (Statista, n.d.), it is seen that we are surrounded by cyber networks that are indispensable in every moment of our social life, from education to defense, from communication to commerce. Various manipulations on social media reveal the most current state of cyber warfare. New conflict areas are no longer cities or extensive lands, but the increasingly digitalized cyber world can be defined as the most up-to-date conflict area whose borders cannot be determined. Establishing hegemony in such an environment is complex, and states must cooperate and update their strategies.

The increased use of technology and the high dependence on information technologies in developed countries with globalization reveals that they are heavily affected by all kinds of disruptions in the cyber world. Especially today, attacks on states and organizations such as Estonia, Georgia, and NATO, as well as leading companies, have resulted in states' immediate perception of security towards cyberspace. It has emerged as a new field that has been securitized due to the dedications such as 'new terrorism' and 'postmodern terrorism' that occurred in this field. The fact that the region was turned into a cyber warfare area by Kremlin hackers during the Ukraine

war in the last period is also included in the literature as the most recent example of postmodern warfare.

At a time when cyber-attacks against states, businesses, and individuals are increasing day by day, the legal responsibility of states to respond to such cyber-attacks is an influential agenda. At this stage, the discussions focused on the scope of legal obligation mostly question the choice of states to respond to attacks on the grounds of 'prohibited' use of force or 'self-defense' (Majuca and Kesan, 2009: 2-3). Considering that the actions are mainly carried out by a group of hackers, not by a state, the question of how much a state can use its right of self-defense against illegal activities in the cyber world remains one of the more controversial issues.

When we look at the cyber security strategies of the states, it is seen that; It has become the primary goal of the states to monitor an active defense by predicting the attacks that may occur against them in cyberspace and taking precautions against them. Vigorous defense requires organizations to predict seizures before they happen, detect and respond in real time, set traps and alarms to contain attacks and take a layered approach to protect critical assets.

In addition to forecasting and precautionary headings, states that want to increase deterrence with legal security sanctions also wish to realize their development-oriented cyber security goals by supporting cyber security industries. Increasing internet use and cyber activities are widely used for states as well as individuals. We live in an environment where the possibility of States encountering cyber threats beyond classical risks has become a reality beyond being a possibility. In this case, we also have to face the fact that the issue of cyber security often goes beyond the borders of the nation-state, necessitating international cooperation.

Considering that these attacks are not carried out directly by States but indirectly, it reflects a situation beyond the assumption that such cyber-attacks will increase in the future. At this point, in the coming days, states should be ready to cooperate in ensuring cyber security and to draw the limits of cyber sovereignty/freedom. As governments get better against cybersecurity threats both nationally and internationally, the key to cyber solid defense is nations working together against threats.

The issue of cyber security, which has become an essential problem of developed and developing countries, makes it necessary to collaborate in the globalizing world. Cyber threats can operate in every field where they can strike the states economically and politically, as well as the theft of intellectual rights and information against companies, the destruction of functioning public mechanisms, and the creation of grievances among citizens. Individuals or groups can create these threats, or States can support them. While cyber espionage activities may be aimed at improving the military capacity of countries or gaining technological superiority from time to time, disinformation and propaganda activities aimed at other states or groups and using cyber tools to create a sphere of influence in the international arena draw attention. It

is seen that the problem has turned into a global security issue beyond being evaluated only by a single state (Kesan and Carol, 2010). Therefore, the solution will likely be overcome on an inter-state platform beyond a single state authority. On the other hand, the absence of a hegemonic power that can solve security threats in cyberspace causes problems in preventing conflict of interests both nationally and globally. For example, due to the changes in the hegemonic understanding of security after September 11, the USA has turned to initiatives to prevent the questionability of its hegemony in the real world from occurring in cyberspace. These initiatives make cyberspace not a more stable environment but an environment full of competition and conflict of interest.

Although the extent to which states can use force in the face of cyber-attacks against their functioning mechanisms is still a controversial issue, the desire of states to use their self-defense rights against possible attacks in the cyber world is predominant. The cyber security strategy documents they have published nationally for this purpose, the various protection measures they carry out in this direction, and the efforts for nationalization in the cyber world can be considered as efforts to draw the areas of cyber sovereignty. The tensions will inevitably be much higher in such a situation, assuming that states may prefer defense methods that are sometimes inappropriate or that tend to use excessive force. Considering this situation, having an internationally acceptable definition of cyber-attacks and determining who can respond to it in case of a possible attack within the framework of an international consensus will provide a global solution platform for states' sovereignty concerns. However, establishing national and international cyber defense centers, where the source is often difficult to find, will be another point to be considered for states in terms of cyber security.

SİBER GÜÇ ARAÇLARI VE ULUSAL GÜVENLİK: DEVLETLERİN HEGEMONYA ALANLARI

1. GİRİŞ

Kapsam ve etkileri bakımından uluslararası ilişkilerde son zamanlarda adından oldukça söz ettiren siber güvenlik, teknolojik gelişmelerin ve uzay çalışmalarının etkisiyle yeni bir çatışma alanı olarak gün yüzüne çıkmaktadır. Siber tehditler, uluslararası sistem içerisindeki çeşitli aktörlerin müdahil oluşu ve aniden tüm dünyada hissedilebilir etkiler yaratıyor olması nedenlerinden ötürü uluslararası güvenlik sorunlarını katlayarak artırmaktadır. Her geçen gün devletlerin siber dünyadaki sınırlarını çizme gayretleri ve kendi siber ortamlarını tanımlama çabaları, siber uzayın güvenlikleştirilmesine yol açmaktadır. Bu çerçevede birçok ülke, siber dünyadaki hedef ve maksatlarını ortaya koyan ulusal güvenlik stratejilerini güncellemektedir. Devletlerin hegemonya alanlarındaki genişlemenin sonucu olarak bu çalışmada ele alınan örnekler, nüfus yoğunluğu, internet yapıları ve güvenlik konseptleri bakımından tercih edilmiş olup, aktörlerin sadece ulusal güvenlik stratejileri değil

aynı zamanda sınırları çizilemeyen siber ortamın denetimine ilişkin uygulamalar de ele alınmaktadır.

2. GÜVENLİK VE SİBERNETİK DÖNÜŞÜM

Bilgisayar ve internetin günümüz dünyasındaki yerinin yadsınamayacak ölçüde artmış olması, eğitimden sağlığa pek çok konuda 'siberleşme' eğilimleri ve her olgunun teknolojik varyasyonlarına rastlamak olağan bir durum haline gelmiştir. Zannedilenin aksine yalnızca bilgisayar ve internet ilişkileri anlamına gelmenin çok ötesinde iletişim, hizmetler ve finans gibi pek çok alanda fiziksel dünyanın dışında sanal bir gerçeklik sunan siber uzayın net bir tanımı yapılamamaktadır.

Belirsizliklerle dolu yeni bir dünyanın kapısının aralandığı siber uzay, fırsatlar ve yeniliklerin yanı sıra güvenlik açığı, tehdit ve riskleri de bünyesinde barındırmaktadır. Bu ortamda bireyler arası iletişim etkisinin ötesinde gelişmiş ve gelişmekte olan ülkeler arasındaki dijital bölünme ve sanal eşitsizlik de genişlemektedir.

İnsanlık tarihinin en temel hakimiyet alanı olarak görülen kara ve deniz bölgelerine hava ve uzay hakimiyet alanları eklenerek devletler bu fiziki alanları siyasi, askeri ve ekonomik anlamda hegemonya sınırları haline getirmişlerdir. Kozmos'un kapsadığı fiziki alanların hakimiyetine dayalı yaklaşımlar sunan bu dört 'domain area'ya yeni nesil bir beşinci boyut eklenmiştir: Siber uzay.

Günümüz dünyasında savaşların yalnız konvansiyonel askeri araçlarla gerçekleşmediği göz önünde bulundurulduğunda eğitim, sağlık, ekonomi, finans ve daha birçok kamusal ve özel aktiviteyi aksatan çeşitli yazılımlar ve bilgisayar programlarının varlığı, devletlerin egemenlik boyutunda siber dünyayı politik düzlemde algılamasına neden olmaktadır.

3. DEVLETLERİN HEGEMONİK GÜVENLİĞİ VE SİBER ORTAM

İkinci Dünya Savaşı sonrası ortaya çıkan ve kara ve deniz hakimiyet teorilerine göre daha fazla ulaşım kolaylığı sağlamış olan hava gücüne dayalı hava hakimiyet yaklaşımları ülkelerin savunma stratejilerinde köklü değişimlere yol açmıştır. Özellikle hava araç sistemlerinin gelişmesi ve yeni savaş sistemleri ortaya çıkışı hava hakimiyet yaklaşımına ek olarak bir de uzay hakimiyetinin tartışılmasına neden olmuştur. Günümüzde ise teknolojinin gündelik hayatımızın ayrılmaz bir parçası oluşu ve bilişim teknolojilerinin gelişimi insanları pek çok bakımdan bu teknolojiye bağımlı hale getirmiş durumdadır. Öyle ki internet ve uydu araçları, bilgisayar ve cep telefonu gibi bilişim ürünleri günlük hayatın vazgeçilmezleri arasındadır.

Birçok alana nüfuz etmiş durumda olan internet teknolojisi 21. Yüzyılın en büyük gerçeği olarak karşımızda durmaktadır. Yapay zeka, hipersonik teknolojiler ve otonom araçlar dahil pek çok dijital araç yalnız sosyal hayatta vatandaş bağlamında değil devlet kurumları bağlamında da geleceğin ulus devlet yapılanmalarını etkileyecek değişiklikler meydana getirmektedir. Yeni nesil dijital ulus devletler bir yandan dijital okuryazarlığı artırma şeklindeki eğilimlerini hızlandırmakta diğer

yandan kurumlarına yönelik gerçekleşecek siber tehditlere karşı dijital korunma yöntemlerini geliştirmeye çalışmaktadırlar. Günümüz uluslararası sisteminde çeşitli uydu teknolojilerini geliştirme yetisine sahip başat aktörlerin konvansiyonel silahlar yerine siber savaş araçlarına sahip olmayı ulusal siber güvenlik stratejilerine ekledikleri görülmektedir.

Yeni milenyumun başlangıcında dönüşüm yörüngesine başlayan uluslararası sistemin evrimi, ağırlıklı olarak ulus-devletler olmak üzere çok sayıda uluslararası aktör tarafından uygulanan hegemonik alanların ve güvenlik stratejilerinin kapsamlı bir şekilde yeniden değerlendirilmesini gerektirmiştir. Küresel güç yapılarının dinamikleriyle derinden iç içe bir kavram olan hegemonik güvenlik, uluslararası ilişkiler alanında geçmişte çok sayıda perspektiften kapsamlı bir inceleme ve analiz konusu olmuştu. Tek bir egemen gücün küresel istikrarı koruma kapasitesine sahip olduğu fikrini öne süren hegemonik istikrar teorisi, özellikle Soğuk Savaş döneminde iki kutuplu yapıyı, Soğuk Savaş sonrasında ise ABD hegemonyasını meşrulaştıran bir bakış açısıydı. ABD'nin 20. yüzyılın ikinci yarısı boyunca devam eden hegemonik etkisinin temelindeki birincil etken askeri güç idi. Bununla birlikte, milenyum güç dinamiklerini şekillendirmede teknolojik yeteneklerin oynadığı rol vazgeçilmez hale geldi. Hegemonik paradigmadaki evrimin sonucu olarak ABD'nin geleneksel hegemonyasını siber ortamda da sürdürme refleksleri, yükselen bölgesel teknolojik güçlerle karşı karşıya getirmektedir.

Günümüzde ülkelerin geleceğe şekil vermek adına teknolojik silahları aktif bir biçimde kullandığı göz önünde bulundurulduğunda, ABD, Rusya, Çin, İsrail ve İngiltere gibi ulus devletlerin siber saldırılara karşı ulusal savunmaya geçmekle kalmayıp aktif savunma adına hackerları da kullanmakta oldukları bilinmektedir.

Küresel düzen ve istikrarı odaklanan Hegemonik istikrar teorisi, tek bir ulus-devlet veya bir devletler koalisyonunun baskın güce sahip olduğunda potansiyel saldırganları caydırdığını ve bir güç dengesi sağladığını öne sürmektedir. Ancak bu anlamda, siber tehditlerin hızla yükselişi bu paradigmaya yepyeni karmaşıklıklar getirmektedir. Siber uzaya yönelen dünyamızda ortaya çıkan dijital güvenlik açıklarının ulusal güvenliği daha da güvencesiz hale getirdiği gerçeği düşünüldüğünde devletlerin istikrar sağlama yönündeki tedbir arayışları sağlam siber savunma altyapısını gerektirmektedir.

Sadece bu çalışma kapsamında ele alınan devletler açısından değil dünya genelinde siber güvenliği sağlamaya yönelik devletlerin kendi bütçelerinden ayırdıkları geniş kaynakların yanında tehdit seviyelerinin savunma yeteneklerinden daha hızlı arttığı şeklinde bir gerçek söz konusudur. Yakın gelecekte ulus devletler açısından siber kıta sahanlığı ve siber entegrasyon modellerinin sıklıkla konuşulacağı ve siber vatan kavramının daha çok gündemde olacağı düşünüldüğünde, güvenlik konseptinin ulusal siber güvenliği kapsayacak şekilde genişletmesi gereksinimi ortaya çıkmaktadır. Devletlerin kendi siber sınırlarına yönelik olası saldırıları tahmin etme, onlara gerçek zamanlı olarak müdahale etme ve siber saldırıları kontrol altına alabilme maksatlarıyla çeşitli koruma programları oluşturmak şeklindeki eylemleri, siber

dünyada kendilerine yönelik gelebilecek saldırıları durdurma konusunda etkili yöntemler olabilmektedir.

SONUÇ

Tamamen internet teknolojisinin altyapısına bağlı bir şekilde kurulan 'gelecek' uluslararası sistem içerisinde E-ticaret, E-ihracat, E-devlet, E-diplomasi, E-savaş şeklinde devletleri ve vatandaşlarını bir 'E' hali durumuna sokmaktadır. Bilginin oluşumu, saklanması ve korunmasından oluşan bilgi sistemleri siber uzayın merkezinde yer almaktadır. Akıllı telefonlar, akıllı evler, akıllı şehirler… Her şeyin birbiriyle bağlantılı olduğu bugünün dijital ortamında hayatın her alanında her özne 'connected' durumdadır. Bugün 8 milyarı aşkın dünya nüfusunun 7.33 milyarının cep telefonu ve 5.18 milyarının internet kullanıcısı olduğu düşünüldüğünde eğitimden sağlığa, iletişimden ticarete, güvenlik ve savunmadan diplomasiye siber ağlarla çevirili bir atmosfer mevcuttur. Halen fiziksel çatışma alanları mevcudiyetini koruyor olsa da gitgide dijitalleşen siber dünya, sınırları belirlenemeyen çatışma alanına dönüşmektedir.

Devletlerin işleyen mekanizmalarına yönelik gerçekleşen siber saldırılar karşısında ne dereceye kadar güç kullanabilecekleri halen tartışmalı bir konu olarak güncelliğini koruyor olsa da devletlerin meşru müdafaa haklarını olası saldırılara karşı siber dünyada kullanma istekleri baskın gelmektedir. Buna yönelik ulusal çapta yayınladıkları siber güvenlik strateji belgeleri, bu doğrultuda yürütmekte oldukları çeşitli koruma önlemleri ve siber dünyada millileşme çabaları siber egemenlik alanlarını çizmeye yönelik adımlar olarak düşünülebilmektedir. Devletlerin zaman zaman uygun olmayan ya da aşırı güç kullanımına kayan savunma yöntemleri tercih edebileceği varsayımıyla böylesi bir durumda tansiyonun çok daha yüksek olması ihtimali kaçınılmazdır. Bu durum dikkate alındığında siber saldırı ve tehditlere ilişkin uluslararası mecrada kabul edilebilir kriterlerin oluşması ve olası bir saldırı durumunda kimlerin buna karşı cevap verebileceğinin ülkeler arası bir konsensus çerçevesinde belirlenmesi devletlerin egemenlik kaygılarına yönelik uluslararası çözüm platformu oluşturacaktır. Çoğunlukla kaynağını bulmakta güçlük çekilen siber tehditlere yönelik ulusal veya uluslararası siber savunma merkezlerinin kurulması ise devletler açısından dikkate alma zorunluluğu bulunan siber güvenlik önlemi olacaktır.

REFERENCES

AFCEA (Armed Forces Communications and Electronics Association) (2012). The Russo- Georgian War 2008: The role of the cyber attacks in the conflict, Fairfax, VA: AFCEA, Access:07.07.2023, http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

Amoroso, E. (2006). *Cyber Security*. New Jersey: Silicon Press.

Anderson, C. and Sadjadpour, K. (2018). *Iran's Cyber Threat: Espionage, Sabotage,*

and Revenge, Massachusetts: Carnegie Endowment for International Peace Pub.

Baylis, J. (2008). Uluslararası İlişkilerde Güvenlik Kavramı, *Uluslararası İlişkiler,* 5(18), 69-85.

Bird, D. A. (2020). *Real-Time and Retrospective Analyses of Cyber Security*, IGI Global. DOI:10.4018/978-1-7998-3979-8

Canongia, C. and Mandarino, R. (2014). Cybersecurity: The New Challenge of the Information Society. I. Management Association (Ed.), In *Crisis Management: Concepts, Methodologies, Tools, and Applications* (pp. 60-80). IGI Global. DOI: 10.4018/978-1-4666-4707-7.ch003

Chen, T. M. (2014). *Cyberterrorism After Stuxnet*, Strategic Studies Institute, Monographs, Books, and Publications. Carlisle Barracks, PA: US Army War College Press.

Clarke, R. A. and Robert E. K. (2019). *The Fifth Domain Area: Defending Our Country, Our Companies, Ourselves in the Age of Cyber Threats*, NewYork: Penguin Press.

Committee on National Security Systems (CNSS) (2022). Committee on National Security Systems (CNSS) Glossary, Committee on National Security Systems (CNSS) Instruction No. 4009 Access:14.06.2023,https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf

Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2014). Concept of Russia's Cyber Security Strategy – draft underway. NATO. Access:14.06.2023, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

Cox, Robert W. (1993). *Gramsci, Hegemony and International Relations. An Essay in Method*, (eds.), Stephen Gill, Gramsci, Historical materialism and International Relations, Cambridge University Press, Cambridge, 49-66.

Crowther, G. A. (2017). Cyber Domain, *The Cyber Defense Review,* 2(3), 63-79.

Department of Defence (DOD) Dictionary of Military and Associated Terms (2021). Joint Publicstion. Access:15.06.2023, https://irp.fas.org/doddir/dod/dictionary.pdf

EPRS | European Parliamentary Research Service (2022). Russia's war on Ukraine: Timeline of cyber-attacks, (by Jakub Przetacznik and Simona Tarpova) Members' Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Fang, B. (2018). *Cyberspace Sovereignty, Reflexions on Building a Community of Common Future in Cyberspace*, Beijing: Science Press.

Gray, C. S. (1999). *Modern Strategy*, Oxford: Oxford University Press.

Hogan, M. and Newton E. (2015). *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, U.S. Department of Commerce, NISTIR 8074. Access: 20.08.2023, https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

International Telecommunication Union, ITU (2009). Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva. Access:30.08.2023, http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Jasper, S. (2020). Russian Cyber Operations: Coding the Boundaries of Conflict, Georgetown University Press. https://doi.org/10.2307/j.ctv2k88t3d

Kemmerer, R. A. (2003). Cybersecurity. Proceedings of the 25th International Conference on Software Engineering, Portland, USA. 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257

Kesan J. P. and Hayes, C. M. (2010). Thinking Through Active Defense in Cyberspace, Illinois Public Law and Legal Theory Research Papers Series No. 10-11.

Kneale, J. (2004). The Virtual Realities of Technology and Fiction: William Gibson's Cyberspace, Crang, Mike, Phil Crang, Jon May (Ed.) in Virtual Geographies: Bodies, Space and Relations, (pp.319-330), London: Routledge.

Kolbe, P. R. (2022). The cybersecurity risks of an escalating Russia-Ukraine conflict. Harvard Business Review. Access:11.07.2023, hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict.

Körpe, Ö. (2022). "Reading the USA through Strategy Documents: An Analysis on the Change of Hegemonic Security Understanding". Güvenlik Stratejileri Dergisi 18, 265-93. https://doi.org/10.17752/guvenlikstrtj.1104894.

Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. Washington, DC: Center for Strategic and International Studies. Access: 20.08.2023, https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection

MacGibbon, A. (2009). Cyber security: threats and responses in the information age, *Australian Strategic Policy Institute Specia Report*, Issue 26.

Majuca, R. P. and Kesan, J. P. (2009). Hacking Back: Optimal Use of Self-Defense in Cyberspace, *Chicago-Kent Law Review*, Vol. 84, No. 3, 1-69.

National Institute of Standards and Technology, NIST (2020). Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations, Joint Task Force. Access:10.09.2023, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Nan, Y.(2024) " American cyber hegemony: Science fiction turned into reality", https://news.cgtn.com/news/2021-12-23/American-cyber-hegemony-Science-fiction-turned-into-reality-16cvlPiBg9W/index.html

National Institute of Standards Technology NIST (n.d.). Glossary: Cyber Attack, U.S. Department of Commerce. Access: 06.09.2023, https://csrc.nist.gov/glossary/term/cyber_attack#:~:text=Definition(s)%3A,data%20or%20stealing%20controlled%20information.

OECD (n.d.). Gross domestic spending on R&D. Access:02.09.2023, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

Office of Management and Budget, Budget of the U.S. Government FISCAL YEAR 2023, Te White House, Washington, https://www.whitehouse.gov/wp-content/uploads/2022/03/budget_fy2023.pdf

Orend, B.(2014). Fog in the Fifth Dimension: The Ethics of Cyber-War, *The Ethics of Information Warfare*, 2014, Volume 14, 3-23.

Oxford Online Dictionary (2014). Oxford: Oxford University Press. Access: 10.08.2023, http://www.oxforddictionaries.com/definition/english/Cybersecurity

Özçelik, S. (2005). Neorealist and Neo-gramscian hegemony in international relations and conflict resolution during the 1990s. Ekonomik ve Sosyal Araştırmalar Dergisi.

Özçelik, S. (2018). II Soğuk Savaş ve Kırım'daki Jeostratejik Gambit: Rusya'nın Stratejik derinliği Bağlamında Kırım'ın işgali ve Kırım Tatarlar, Osman Orhan (Ed.), *Karadeniz ve Kafkaslar, Riskler ve Fırsatlar: Ekonomi, Enerji ve Güvenlik* içinde, (57-77). İstanbul: TASAM Yayınları.

Pernik, P. (2018). The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine, in Hacks, Leaks And Disruptions-Russian Cyber Strategies, *European Union Institute for Security Studies* (EUISS), Chaillot Papers no:148, 53-64.

Slawotsky, J. (2017). The Clash of Architects: Impending Developments and Transformations in International Law. The Chinese Journal of Global Governance, 3(2), 120-122. https://doi.org/10.1163/23525207-12340025

Statista (n.d.). Forecast number of mobile users worldwide 2020-2025 Access:07.09.2023, https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

Statista (n.d.). Internet usage worldwide - Statistics & Facts Access: 23.08.2023, https://www.statista.com/topics/1145/internet-usage-worldwide/#dossierKeyfigures

Statista (n.d.). Demographics and Use of the Internet, Access:07.09.2023, https://www.statista.com/markets/424/topic/537/demographics-use/#overview

Stoffer, C. (2022). 115 cybersecurity statistics + trends to know in 2023, Norton. Access: 23.08.2023, https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

Volz, D. and Viswanatha, A. (2018). FBI says Chinese espionage poses 'most severe' threat to American security, Access:08.09.2023, https://www.wsj.com/articles/senate-sifts-evidence-of-chinese-cyberespionage-11544635251

Worth, O (2015). *Rethinking Hegemony*, New York: Palgrave Macmillan.

KATKI ORANI / *CONTRIBUTION RATE*	**AÇIKLAMA / *EXPLANATION***	**KATKIDA BULUNANLAR / *CONTRIBUTORS***
Fikir veya Kavram / *Idea or Notion*	Araştırma hipotezini veya fikrini oluşturmak / *Form the research hypothesis or idea*	Gülşah ÖZDEMİR, Soner KARAGÜL
Tasarım / *Design*	Yöntemi, ölçeği ve deseni tasarlamak / *Designing method, scale and pattern*	Gülşah ÖZDEMİR, Soner KARAGÜL
Veri Toplama ve İşleme / *Data Collecting and Processing*	Verileri toplamak, düzenlenmek ve raporlamak / *Collecting, organizing and reporting data*	Gülşah ÖZDEMİR, Soner KARAGÜL
Tartışma ve Yorum / *Discussion and Interpretation*	Bulguların değerlendirilmesinde ve sonuçlandırılmasında sorumluluk almak / *Taking responsibility in evaluating and finalizing the findings*	Gülşah ÖZDEMİR, Soner KARAGÜL
Literatür Taraması / *Literature Review*	Çalışma için gerekli literatürü taramak / *Review the literature required for the study*	Gülşah ÖZDEMİR, Soner KARAGÜL