Araştırma Makalesi

CYBERWARFARE DYNAMICS: ECONOMIC, POLITICAL AND SOCIAL PERSPECTIVES

Melih ENGİN[*]
Hakan KÖR[**]
Muhammet Fatih AYKURT[***]

Abstract

With the rise and proliferation of the Internet, there has been a significant increase in the utilization of digital technologies. Both governments and private entities are extensively shifting their operations to electronic platforms, marking digitalization as an imperative. These advancements streamline various processes in our daily lives. However, as the quantity of data generated in digital realms surges, so does the interest of malicious individuals or factions in virtual domains. Consequently, the internet has facilitated the emergence of a novel battleground, presenting both advantages and challenges. Within this domain, concepts such as cyber-attacks, cyber warfare, and cyber security have gained prominence in national and international literature, prompting countries to devise defensive strategies. This study delves into the impact of cyber warfare, scrutinizing its economic, political, social, and media dimensions on both countries and international organizations, as well as on a domestic level. Furthermore, it explores the distinct defense tactics adopted by countries such as the United States, Russia, China, and Turkey. This study aims to answer the following research questions: (1) How do cyberwarfare strategies differ among major global actors? (2) What are the economic, political, and social implications of cyberwarfare? (3) How do states develop defense mechanisms against cyber threats? These questions shape of the research, emphasizing comparative analysis of selected case studies.

Keywords: Cyberwarfare, International Cyber War, Cyber Security, Cyber Attack.

Jel Codes: O17, O38, P49, H56.

[*] Doç. Dr., Uludağ Üniversitesi, İnegöl İşletme Fakültesi, melihengin@uludag.edu.tr
ORCİD: 0000-0002-4953-6119
[**] Doç. Dr., Hitit Üniversitesi, Mühendislik Fakültesi, hakankor@hitit.edu.tr
ORCİD: 0000-0002-8314-9585
[***] Yüksek Lisans Öğrencisi, Hitit Üniversitesi, muhammetfatihaykurt@gmail.com
ORCİD: 0000-0002-2698-3952

Alındığı Tarih	: 28.11.2024
Kabul Edildiği Tarih	: 31.01.2025
Açık Erişim Tarihi	: 26.06.2025

Siber Savaş Dinamikleri: Ekonomik, Politik ve Sosyal Perspektifler

Özet

İnternetin yükselişi ve yaygınlaşmasıyla birlikte dijital teknolojilerin kullanımında önemli bir artış yaşanmıştır. Hem hükümetler hem de özel kuruluşlar, operasyonlarını elektronik platformlara taşımakta ve dijitalleşmeyi bir gereklilik haline getirmektedir. Bu gelişmeler, günlük yaşamımızdaki çeşitli süreçleri kolaylaştırmaktadır. Ancak, dijital alanlarda üretilen veri miktarı arttıkça, kötü niyetli bireyler veya grupların sanal alanlara olan ilgisi de artmaktadır. Sonuç olarak, internet yeni bir savaş alanının ortaya çıkmasını kolaylaştırmış ve hem avantajlar hem de zorluklar sunmuştur. Bu alanda, siber saldırılar, siber savaş ve siber güvenlik gibi kavramlar ulusal ve uluslararası literatürde öne çıkmış, ülkeleri savunma stratejileri geliştirmeye yöneltmiştir. Bu çalışma, siber savaşın etkilerini inceleyerek, hem ülkeler hem de uluslararası örgütler ve ulusal düzeyde ekonomik, politik, sosyal ve medya boyutlarını ele almaktadır. Ayrıca, Amerika, Rusya, Çin ve Türkiye gibi ülkelerin benimsediği farklı savunma taktiklerini de incelemektedir. Bu çalışma şu araştırma sorularına yanıt aramaktadır: (1) Siber savaş stratejileri büyük küresel aktörler arasında nasıl farklılık göstermektedir? (2) Siber savaşın ekonomik, politik ve sosyal etkileri nelerdir? (3) Devletler siber tehditlere karşı nasıl savunma mekanizmaları geliştirmektedir? Bu sorular, seçilen vaka çalışmalarında karşılaştırmalı analizi öne çıkarmaktadır.

Anahtar Kelimeler: Siber Savaş, Uluslararası Siber Savaş, Siber Güvenlik, Siber Saldırı.

Jel Kodları: O17, O38, P49, H56.

Introduction

Depending on the development of information and communication technologies, humanity has developed various weapons to protect itself and to defend and attack structures that it perceives as a threat to their existence. In this context, societies that waged war with close-range weapons in the early periods has become able to attack and defend from afar, due to technological advancements. In today's world, everyone knows that modern warfare can be conduct at the push of a single button, and individuals and states develop defense strategies accordingly.

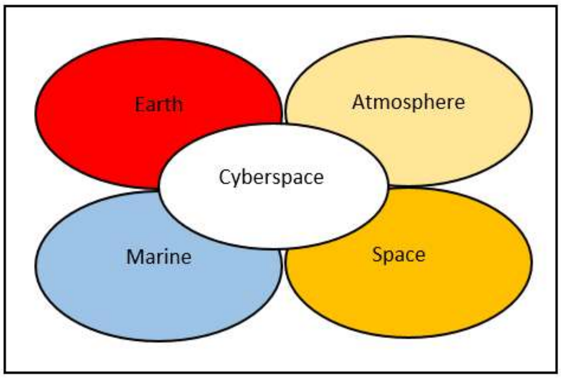
1. Material And Methods

In this study, the developments in the field of telecommunications and the effects of cyber wars on the political, economic and social structures of the in an era characterized by a departure from traditional warfare are examined and additionally, the study discusses media-driven perceptions related to cyber conflicts. In addition, the study analyzes existing researches to determine the types of security strategies countries have adopted in response to cyber warfare. In this section, cyber and fundamental concepts such as cyber space, cyber-attack and its types, and cyberwarfare are defined. This study employs a qualitative research methodology, utilizing comparative and content analyses as primary methods. Data sources include government reports, cybersecurity threat assessments, and scholarly literature published between 2010 and 2023. The study follows a case study approach, focusing on cyberwarfare incidents involving the United States, China, Russia, and Turkey.

1.1. Cyber Concept and Cyberspace

The term “cyber” was first used by Wiener(1948) referring to the control of complex systems in mechanical networks and the animal kingdom (Avcıoğlu, 2017). The concept of "Cyber Space", which is defined as a wide area that includes all telecommunication, internet, computer systems and fiber optic cables, has emerged in the past.

Fig 1. Visual Representation of Cyberspace



In the Republic of Turkey 2020-2023 National Cyber Security Policy and Action Project, the concept of "Cyber Space" is defined as " all systems and services directly or indirectly connected to internet, telecommunication and computer networks"(T.C. Ulaştırma ve Altyapı Bakanlığı, 2020). William Gibson used the concept of cyberspace in his novel 'Neuromancer' published in 1984(Weiner, 2019). The U.S. Department of Defense defines the concept of "Cyberspace" as "a global space consisting of integrated information technology subcomponents, including the internet, telecommunications networks, information systems, closed processors and control mechanisms".

1.1.1. Cyber Attack and Its Types

A cyber attack can be defined as an action that damages, destroys or renders inoperable a cyber target that is directed against it. A cyber attack in the Republic of Turkey 2020-2023 National Cyber Action Plan; It is defined as actions taken intentionally by people or information systems in any position in cyber space with the thought of destroying confidentiality, availability, and integrity of industrial and information control systems in the cyberspace or the data developed by these systems.

The security, accessibility, and integrity of information are adversely affected by all cyberattacks. These attacks aim to access systems without authorization, steal information, render the system inoperable, and modify, destroy, and prevent it.

Cyberattacks can be executed through various methods. For instance, malicious software—commonly known as viruses—represents a widely recognized attack vector designed to infect and disrupt computer systems. Attacks that damage computer systems can be listed as follows: Trojan Horses (it looks like a trojan-useful program and does different processes in the background on the system it has infiltrated), worms (slowing down worm-systems), phishing (Phishing- stealing personal data over random links and SMS), spyware (spyware-stealing information), zombie computers (botnet - use of the computer by the attacker for their own purposes), key loggers (key logger - recording of card and password information, keyboard and mouse movement tracking), adware (adware - small malicious programs installed without the user's awareness), and ransomware. Gaining economic or political advantage through unauthorised access to information is the basic principle of attacks using ransomware (software that locks a system after entering it, usually demanding money). With the understanding that these attacks are carried out under the auspices of a state in a way that threatens the security of a nation, interstate cyberwarfare becomes inevitable.

Cyberwarfare can be expressed as a new battlefield, which is the 5th dimension after land, sea, air, and space in the 21st century. In addition, as Mataracıoğlu(2010) stated in a symposium in 2010, cyberwarfare is defined as the whole organized attacks made through communication and information systems against the country determined for economic, political, military, or psychological ideals. However, Shane M. Coughlan defines cyberwarfare as “symmetrical or asymmetrical, defensive or offensive digital network actions by nations or nation-like actors that damage sensitive national infrastructures, military systems or industrial infrastructure important to the country (Tatar, 2010).

When it comes to cyber warfare, unlike traditional wars where there are many methods, attackers and defenders, bombs do not explode. It is a seemingly human form of attack that has very serious consequences when examined. The aspects of cyber wars that destroy the psychology of the enemy and create manipulation and perception can sometimes be more impactful than the explosion of a bomb in the capital city for the wounded community. The party that infiltrates a country's systems and captures critical information can use them in many ways. With methods such as disrupting, locking, or rendering systems inoperative, the infrastructures of countries can be destroyed or cause enormous economic losses. These situations will be explained in detail below with the sample analysis method and revealed with scientific data.

1.2. Impact of Cyber Wars on Countries

Cyberwars generally refer to conflicts between nations utilizing their cyber capabilities within cyber environments. The transformation of a cyber attack into a cyberwar depends on whether the attacked nation-state defines it as an attack on its national security.

One of the earliest examples of cyber attacks occurred when the United States, which noticed software that Soviet Union stole from a Canadian company as an intelligence activity in 1982, subsequently embedded a rojan Horse virus into it.

The first traces of cyber wars can be observed in the Gulf War led by the United States in 1990, when the Iraqi army, which until then was the 5th largest army in the world, received a heavy blow. Against the USA, which seized all communication traffic of the Iraqi army through radiofrequency detection systems, the Iraqi state tried to follow various communication paths with its own troops. The communication weakness in the Iraqi army, which tried to send written information through civilian truck drivers, resulted in defeat (Aslan,2013).

Fig 2. Cyber Attacks Between 1998-2021

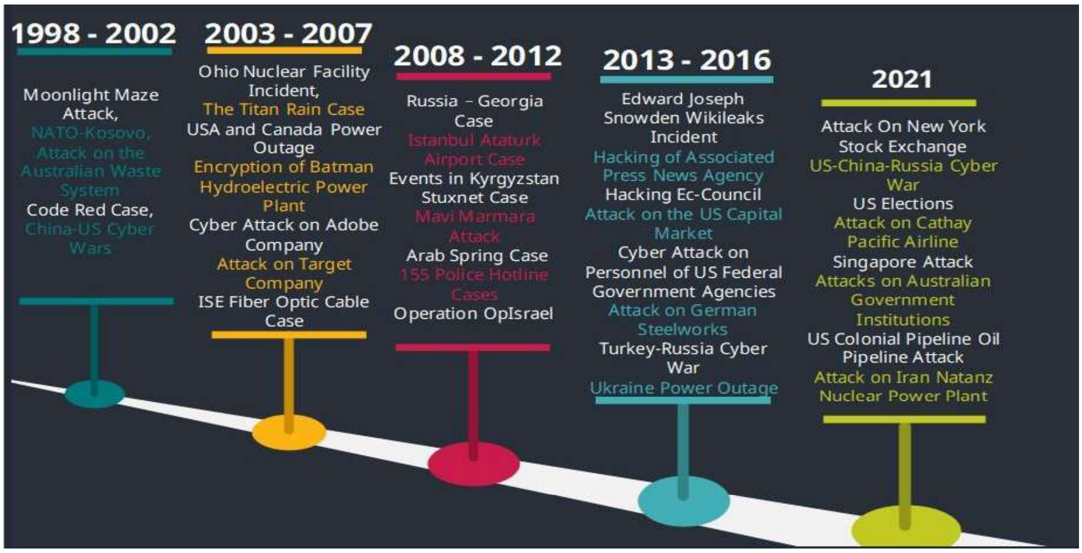

1998 - 2002
Moonlight Maze Attack,
NATO-Kosovo,
Attack on the Australian Waste System
Code Red Case,
China-US Cyber Wars
2003 - 2007
Ohio Nuclear Facility Incident,
The Titan Rain Case
USA and Canada Power Outage
Encryption of Batman Hydroelectric Power Plant
Cyber Attack on Adobe Company
Attack on Target Company
ISE Fiber Optic Cable Case
2008 - 2012
Russia – Georgia Case
Istanbul Ataturk Airport Case
Events in Kyrgyzstan
Stuxnet Case
Mavi Marmara Attack
Arab Spring Case
155 Police Hotline Cases
Operation OpIsrael
2013 - 2016
Edward Joseph Snowden Wikileaks Incident
Hacking of Associated Press News Agency
Hacking Ec-Council
Attack on the US Capital Market
Cyber Attack on Personnel of US Federal Government Agencies
Attack on German Steelworks
Turkey-Russia Cyber War
Ukraine Power Outage
2021
Attack On New York Stock Exchange
US-China-Russia Cyber War
US Elections
Attack on Cathay Pacific Airline
Singapore Attack
Attacks on Australian Government Institutions
US Colonial Pipeline Oil Pipeline Attack
Attack on Iran Natanz Nuclear Power Plant

Figure 2 lists detectable international cyber attacks from 1998 to 2021.

It has been seen that the economic dimension of some attacks has serious consequences, and some of them are effective at a level that will change the political structures of the countries rather than the economic damage. The effects of these cyberattacks on the economy, politics, social life, and media of countries will be discussed.

1.3. The Economic Impact of Cyberwarfare

Cyberwarfare is usually cheap attack that can be conducted using digital networks and software tools, but the damage they cause is grave. For example, after the cyber attack in the Canadian province of Ontario and the US states of Ohio, Michigan, Pennsylvania, New York, and New Jersey on August 14, 2003, a four-day power outage lasting for 4 days occurred. After the blackout, which affected about 50 million people, its cost to the USA was 10 million dollars. Likewise, in Ontario, Canada the loss as a result of production disruption is approximately 2.3 billion Canadian dollars (Meral, 2015). Cyberwarfare is defined differently across academic and policy literature. According to Coughlan (2003), it refers to digital network actions by nation-states that target national infrastructure. On the other hand, Mataracıoğlu (2010) defines it as a form of organized cyber aggression aiming at economic, political, and military disruption. The U.S. Department of Defense (2021) expands on this, categorizing cyberwarfare into offensive and defensive operations designed to protect critical national assets.

In another event, many websites belonging to the institutions and organizations of the American government crashed in the cyberwar between the US, China and Russia in 2016. These attacks had been in the form of DDoS, that is, combined attacks of zombie computers, and more than 78% of the USA was left without internet and the estimated damage to the country's economy was 7 billion dollars. Since these attacks were suspected to have originated from on smart devices made in China, The US stopped buying Chinese goods for a while and suffered an extra-economic loss (Anadolu Ajansı, 2021).

It has been stated by the US Federal Bureau of Investigation that the attack on the Colonial Pipeline, which carries oil from Houston, the largest pipeline system in the US, to New York Harbor on May 7, 2021, was carried out by Russia in recent history. Although this attack was made on a company that serves 50 million consumers, the US Cyber Security Command took action and responded with countermeasures after the attack. It is estimated that the pipeline, which did not operate for 5 days, damaged the US economy by close to 2 billion dollars (Euronews,2021). For example, the Colonial Pipeline ransomware attack in 2021, attributed to the DarkSide hacking group, disrupted fuel supply across the U.S. East Coast. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA, 2021), the attack led to a 4.6% increase in national gas prices and resulted in estimated economic losses exceeding $5 billion.

The economic impact of cyber attacks and the defensive measures taken by nations to counter them have reached critical levels, as demonstrated by the examples above. In this context, when the Ponemon Institute & Accenture Cyber Security 2019 Cybercrime Cost Reports and the

"2020 Global Risks Report" prepared every year by the World Economic Forum (WEF) are examined; The cost of cyber attacks and cyberwarfare was estimated at $1 trillion in 2011 and $3 trillion in 2015. By 2021, this figure was projected to reach $6 trillion (Ponemon, 2019).

1.4. The Impact of Cyber War on Politics

With the development of communication technologies, communication and social life have undergone significant changes. People can express their political thoughts through various social media networks and different communication channels, without being tied to a particular field, but the damage they cause is reaching serious proportions. However, the widespread development of communication does not always yield positive outcomes; it has also influenced national politics and, in some cases, resulted in the assassination of political leaders. States intervened and manipulated the politics and social lives of other countries from time to time within the framework of their own strategies, and tried to design domestic politics in line with their own interests by creating perceptions.

One of the most important examples for understanding the impact of cyberwars on politics is conflicts supported both internally and externally called the Arab Spring, which started in Tunisia in 2010 and spread across multiple African nations. These uprisings, often regarded as acts of popular mobilization, were backed by various nations through both rhetorical and cyber attacks, leading to the deaths of tens of thousands and resulting in regime changes across multiple countries (Durul, 2017). Anonymous group, which directly supported these rebellions, crashed eight state-owned websites together with Tunisian hackers during the uprising in Tunisia (Kara, 2013). People can express their political thoughts through various social media networks and different communication channels without being tied to a specific area, but the damage they cause is reaching serious proportions: for example, cyber-groups that prevented state institutions from functioning just before the events in the country began both fuelled the rebellious movements of the demonstrators and were effective in achieving the outcome by supporting them.

Cyber warfare can be used to exert political pressure on a sovereign state or administration, as mentioned above, as well as to cause socio-economic damage to the other party. Cyber attacks against the Myanmar government in 2010 can be shown as a good example of this situation. Before the Myanmar elections, the internet network was the target of DDoS attacks (BBC, 2024). Similar to the cyber disruptions observed during the Arab Spring, these attacks aimed to impede the flow of information both before and during the electoral process.

In the ongoing Israeli-Palestinian conflict, the Anonymous group launched a cyber attack against Israel in 2013, allegedly contributing to civilian casualties. Many international cyber organizations also supported the attacks called OpIsrael. According to the statements issued by Redhack and Anonymous groups, over 100 thousand websites, more than 40 thousand Facebook accounts and around 30 thousand bank accounts with extensions belonging to the State of Israel and the Israel Defense Forces were affected by these attacks. Thereupon, the Israeli government, which lost about 3 billion dollars only through cyberattacks, ended its attacks (Anadolu Ajansı, 2023).

1.5. Society and Media Dimensions of Cyberwarfare

Cyber warfare not only impacts the economies and political structures of nations but also brings significant changes to societal life. The increase in internet usage all over the world over the years has led to the increasing prevalence of social media. Cyber warfare can be used to exert political pressure on a sovereign state or administration, as mentioned above, as well as to inflict socio-economic damage on the other party. The damages It involves the sharing of personal data belonging to individuals who are the most important elements of society, such as bank card details, email addresses, social media account details, health records, educational history, communication data, and biometric identifiers such as fingerprints and vein patterns. The fact that people live in fear that information will be stolen has led to a loss of trust. These services, which are necessary for the continuation of social life - including transportation (e.g., airplanes, trains, and metro systems), financial and banking systems, utilities such as water, gas, and electricity, and healthcare systems - heavily depend on information and communication technologies. It is clear that cyberattacks targetting all these systems will cause serious problems. The fact that this situation is at the size of a cyber war sometimes even causes social disasters.

According to statistical data derived from the 2021 We Are Social Report, it has been determined that cyber attacks and cyber wars are intense in countries with high internet usage rates. Likewise, the use of social media has allowed the expansion of cyberwarfare. Information about people and institutions can be obtained through social media. However, as in the example of the Arab Spring, social media plays an active role in designing politics. This makes the job of cyber warriors easier. The reputations of countries are destroyed by disinformation and smear campaigns on social media. National economies can suffer significant damage due to speculation on social media. Social media is a treasure trove of information for cyber warriors. Cyber attackers and the supporting international powers behind them use this network to cause serious damage to the domestic and foreign policies of the countries.

1.6. Security Strategies of Countries

In general, when cyber security is mentioned, it comes to mind that various trainings, activities, applications and technologies constitute a whole aimed at protecting institutional and individual identities. The current era makes it necessary to develop new security policies against cyber attacks and wars. In this context, it creates firewalls by developing various security software and applications in terms of cyber security in countries. It also tries to raise awareness of individuals against cyber wars by preparing cyber attack action plans. State-sponsored ransomware attacks have become a critical geopolitical tool. In 2020, the U.S. Department of Justice indicted Russian intelligence officers for deploying NotPetya malware, which caused over $10 billion in global damages (Department of Justice, 2020).

1.7. Cyber Security Policies of the United States of America

Considering the security policies of the states, it is seen that the judicial regulations and security strategies are implemented by the USA. The U.S. which has been making various legal arrangements since 1984, has guaranteed by law that it takes this situation seriously and will impose sanctions. On May 21, 2010, Cyber Command-CYBERCOM was established. Looking at current US cybersecurity policy, when President Donald Trump's first budget proposal was being considered in 2017, it stated that it would invest $1.5 billion in cybersecurity initiatives to protect state and US critical infrastructure (Tselicov,2016).

1.8. Cyber Security Policies of the People's Republic of China

China took its first measures in 1990. With the Great Firewall system referred to as the Golden Shield Project, 50,000 internet police officers were assigned to control the internet and social media platforms. For example, YouTube, Twitter, Facebook and similar social media sites are prohibited in China. In order to meet the need for such social media sites, China created copies within its own borders and established sites such as Youku instead of Youtube, Fanfou instead of Twitter, and Renren instead of Facebook. These sites are clearly supported by the government by allocating money from the fund. This strategy aims to prevent the use of foreign-based platforms - prone to external influence and redirection - as potential tools for cyberattacks or political interference within the country (Bilgi Teknolojileri ve İletişim Kurumu, 2016).

1.9. Turkey's Cyber Security Policies

The Computer Incident Response Team (TRBOME), responsible for national cybersecurity coordination efforts, operates under TUBITAK in Turkey. Similar to other countries, Turkey has taken several steps to enhance cybersecurity through the enactment of relevant laws and regulations. As a result, the National Cyber Incidents Response Center (USOM CERT) was activated in 2013 to ensure coordination in the incidents related to cyber security under the authority of the Telecommunications Communication Presidency (Karabulut, 2015).

In the following period, the 2016-2019 Cyber Security Strategy document was published. In this document, the activities aimed to be carried out in the field of cyber security were determined by referring to the previous document. The most interesting of these activities was announced that a competition called "Cyber Star" would be held. It has been stated by the USOM that they will form a cyber army from the competent people to be determined as a result of this competition (Çakır, 2021).

According to the results of the International Telecommunication Union's Global Cyber Security Index reported in 2019, Turkey moved up 23 places compared to the previous years and rose to the 20th place in the world and the 11th in Europe based on data from 2018(T.C. Ulaştırma ve Altyapı Bakanlığı, 2020).

Conclusion and Recommendations

This study delved into the multifaceted impacts of cyberwarfare on the political, economic, social, and media dimensions of countries and international organizations, alongside analyzing the defense strategies of key nations such as the U.S., Russia, China, and Turkey.

States are increasingly leveraging information technologies and the internet as tools in cyberwarfare, surpassing traditional notions of physical intervention. The relatively low cost of cyber attacks coupled with the challenge of identifying their sources makes them particularly insidious. Notably, cyber attacks often result in significant economic losses, with repercussions extending beyond financial domains into the political and social spheres. The economic impact of cyberwarfare can be profound. For instance, incidents such as the 2003 Northeast Blackout, which affected millions, or the 2016 cyber attacks on U.S. government websites highlight the immense financial repercussions of cyber threats. Moreover, recent events such as the Colonial Pipeline ransomware attack demonstrate the vulnerability of critical infrastructure to cyber threats, with potential damages reaching billions of dollars.

In the realm of politics, cyberwarfare has reshaped the landscape of international relations. Events like the Arab Spring exemplify how cyber attacks, combined with social media manipulation, can catalyze political upheaval and regime changes. Similarly, conflicts like the Israeli-Palestinian struggle have witnessed cyber attacks aiming to disrupt infrastructure and sow discord, showcasing the intersection of cyber and geopolitical strategies. Moreover, cyberwarfare has profound societal and media dimensions. The pervasive nature of the internet and social media renders societies vulnerable to manipulation and misinformation campaigns. Cyber attacks targeting critical services such as transportation, finance, and healthcare can destabilize societies and erode public trust. In response to these threats, countries have developed various cyber security policies and strategies. From the establishment of dedicated cyber security commands to legislative measures and international collaborations, efforts to bolster cyber defenses are underway worldwide. Notably, Turkey's ascent in the Global Cyber Security Index underscores the importance of proactive cyber security measures in safeguarding national interests. Future cybersecurity policies should emphasize international cooperation, investment in cyber resilience, and the establishment of global cybersecurity norms (World Economic Forum, 2023).

In conclusion, the evolving landscape of cyberwarfare necessitates concerted efforts at the national and international levels. Collaboration, technological innovation, and strategic foresight are paramount in mitigating the risks posed by cyber threats and ensuring the security and stability of nations in an increasingly interconnected world.

REFERENCES

Anadolu Ajansı. (2016, October 22). ABD'deki siber saldırı 7 milyar dolarlık zarara yol açtı. https://www.aa.com.tr/tr/dunya/abd-deki-siber-saldiri-7-milyar-dolarlik-zarara-yol-acti/

Anadolu Ajansı. (2012, November 20). İsrail ordusu siber savaşı kaybetti. https://www.aa.com.tr/tr/dunya/israil-ordusu-siber-savasi-kaybetti/307287

BBC. (2012). Anonymous İsrail'e siber savaş ilan etti. https://www.bbc.com/turkce/haberler/2012/10/10100_declares_cyberwar

BBC. (2010). Burma'ya siber saldırı. https://www.bbc.com/turkce/haberler/2010/11/101104_burma_cyber_attack

CNN. (2012, November 20). Middle East conflict moves online. http://edition.cnn.com/2012/11/19

Siberbülten. (2017). Trump'dan devrim gibi karar: Her bakanlık kendi siber güvenliğinden sorumlu. https://siberbulten.com/uluslararasi-iliskiler/trumpdan-devrim-gibi-karar-her-bakanlik-kendi-siber-guvenliginden-sorumlu/

Aslan, E. (2013). Sızma sanatı. Ankara: ODTÜ Yayıncılık.

Avcıoğlu, G. Ş. (2017). Emek, sibernetik ve toplum. Selçuk Üniversitesi Edebiyat Fakültesi Dergisi, (37), 515–518.

Bilgi Teknolojileri ve İletişim Kurumu. (2017). Unvan. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Bilgi Teknolojileri ve İletişim Kurumu. (2016). 6757 sayılı kanun: OHAL kapsamında kurumlara ilişkin düzenleme. Resmî Gazete.

Coughlan, S. M. (2003). Is there a common understanding of what constitutes cyber warfare? Birmingham: The University of Birmingham.

Çakır, H., & Arınmış Uzun, S. (2021). Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi. Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi, 7(2), 353–379.

Durul, T. (2017, August 11). Çin'de sosyal medya devlerine soruşturma. Anadolu Ajansı. https://www.aa.com.tr/tr/dunya/cinde-sosyal-medya-devlerine-sorusturma/882066

euronews. (2021). ABD'de siber saldırıyla felce uğrayan petrol boru hattı yeniden açıldı. https://tr.euronews.com/2021/05/13/abd-de-siber-sald-r-yla-felce-ugrayan-petrol-boru-hatt-yeniden-ac-ld

Intelligence Resource Program. (2021). DoD Dictionary of Military and Associated Terms. https://irp.fas.org/doddir/dod/dictionary.pdf

Kara, M. (2013). Siber saldırılar-siber savaşlar ve etkileri. [Yüksek lisans tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü].

Karabulut, Y. E., Boylu, G., & Küçüksille, E. U. (2015). Characteristics of cyber incident response teams in the world and recommendations for Turkey. Balkan Journal of Electrical and Computer Engineering, 3(3), 175–178.

Mataracıoğlu, T. (2010). Cyber warfare: The new battlefield of the 21st century. Proceedings of the International Cyber Security Symposium.

Meral, M. (2015). Siber güvenlik kapsamında kritik altyapıların korunmasının önemi. Stratejik Araştırmalar Enstitüsü.

NATO Cooperative Cyber Defence Centre of Excellence. (2022). Cyber conflict and hybrid warfare: Current developments. Journal of Cyber Policy, 7(3), 230–245. https://doi.org/10.1080/23738871.2022.2093267

Ponemon Institute & Accenture. (2019). Siber suç maliyet raporu.

Robinson, M., Jones, K., & Janicke, H. (2021). Cyber warfare: Contemporary threats and responses. Computers & Security, 100, 103052. https://doi.org/10.1016/j.cose.2021.103052

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers & Security, 49, 70–94.

T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). Ulusal Siber Güvenlik Stratejisi 2020–2023. https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf

Tselicov, A. (2021). The tightening web of Russian internet regulation. Research Publication, 7.

U.S. Department of Defense. (2021). Cyber warfare and national security strategies. Washington, DC: Government Printing Office.

U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2021). Colonial Pipeline ransomware attack and its economic implications. Washington, DC: CISA. https://www.cisa.gov

U.S. Department of Justice. (2020). Russian cyber operations and NotPetya malware attacks. Washington, DC: DOJ. https://www.justice.gov

Wiener, N. (2019). Cybernetics: Or control and communication in the animal and the machine. MIT Press.

World Economic Forum. (2023). Global risks report: Cybersecurity and geopolitical threats. Geneva, Switzerland: WEF. https://www.weforum.org/reports/global-risks-report-2023

Yayla, M. (2013). Hukuki bir terim olarak siber savaş. Türkiye Barolar Birliği Dergisi, (104), 177–202.