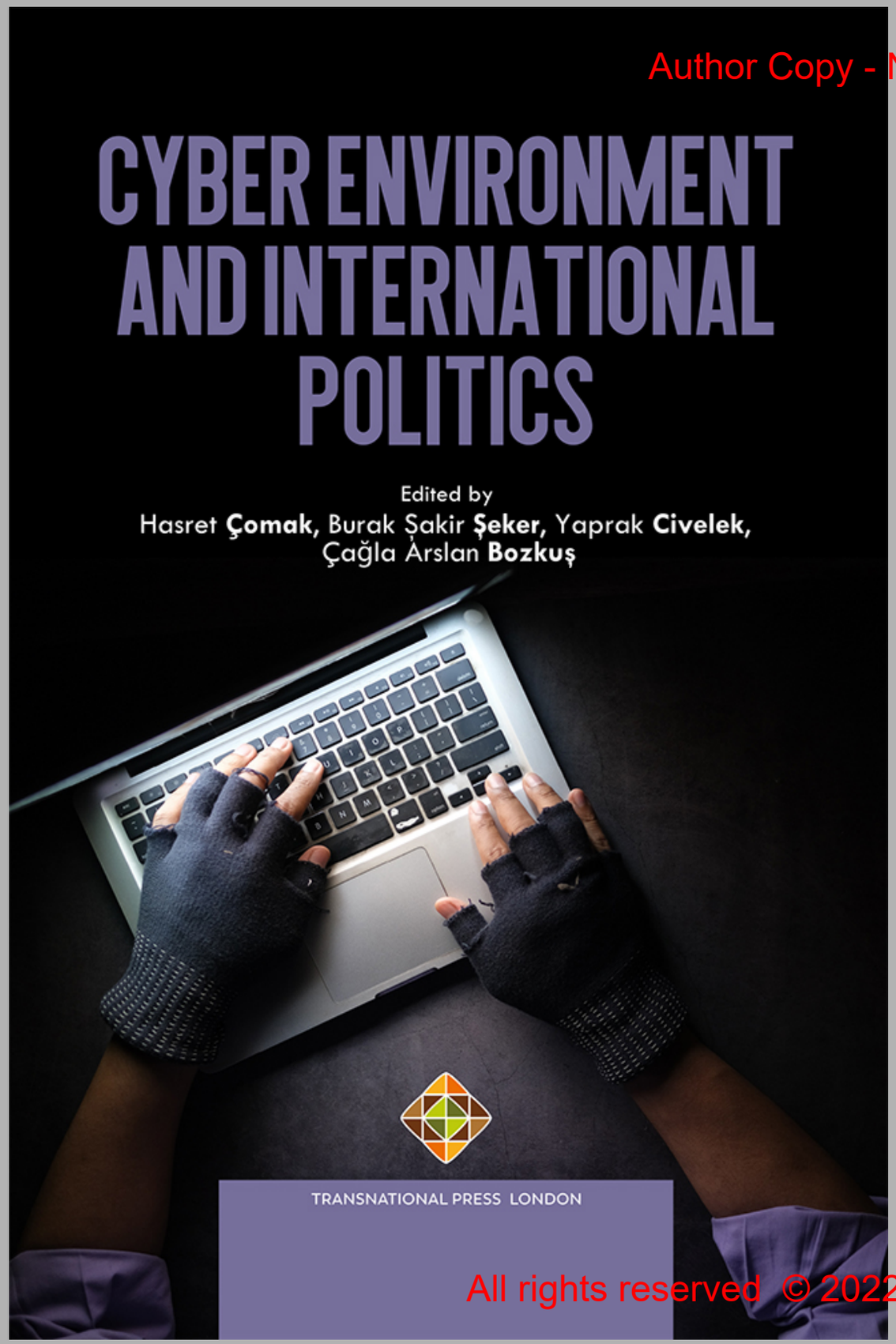

POLICY SERIES: 12

Cyber Environment and International Politics

Edited by Hasret Çomak, Burak Şakir Şeker, Yaprak Civelek,

Çağla Arslan Bozkuş

First Published in 2022 by TRANSNATIONAL PRESS LONDON in the United Kingdom, 13 Stamford Place, Sale, M33 3BT, UK.

www.tplondon.com

Paperback

ISBN: 978-1-80135-146-1

Digital

ISBN: 978-1-80135-147-8

Cover Design: Nihal Yazgan

Cover Photo by Towfiqu Barbhuiya on https://unsplash.com/photos/em5w9_xj3uU

Transnational Press London Ltd. is a company registered in England and Wales No. 8771684.

CYBER ENVIRONMENT AND INTERNATIONAL POLITICS

Edited by

Hasret Çomak

Burak Şakir Şeker

Yaprak Civelek

Çağla Arslan Bozkuş

TRANSNATIONAL PRESS LONDON

2022

CONTENTS

PREFACE

The major revolutions in the field of communication represent the most significant shift of the twenty-first century. The technological revolution has been reduced to a human-scale revolution, with new communication tools made available to everyone. The developments that began with space technology spread quickly. It's important noting that new communication technologies are concentrated in hubs run by global corporations and governments.

Despite the fact that the internet is one of the most fundamental components of cyberspace, cyberspace is not limited to it. It encompasses a wide range of systems and technology, including communication networks, closed military networks based on system technologies, energy distribution networks, mobile phone software-based radios, electronic command systems, satellite systems, and unmanned aerial vehicles.

Actors in the cyber sphere include countries' armed forces, intelligence organizations, legal authorities, and natural and legal persons. Cyber War is defined as the intrusion by one state to destroy or disrupt the computer systems or networks of another state. It is defined as "the sort of warfare in which computer systems are employed to damage or destroy adversary systems" in the United Nations Glossary, in the same way as information warfare. Cyber warfare moves at a breakneck speed. It's a global phenomenon that occurs before the traditional battleground.

There are two forms of cyber warfare: internal and external. The basic goal of cyber warfare is to achieve an external goal. It can entail subduing the other party, stealing their knowledge, temporarily halting their system, or fully contaminating it. The internal goal is to figure out how to use cyber warfare and avoid escalation. "Strategic cyber warfare" refers to the use of cyber attacks against a state and its nation, with the goal of changing the state's attitude. "Operational cyber warfare" refers to a cyber attack against the enemy's military targets and civilian targets associated with its armed forces during conventional combat.

The act of providing and/or disclosing this information for political or military goals is known as cyber espionage. It is the hidden seizure of a country's, institution's, or person's sensitive information utilizing the cyber environment as a tool." Cyber espionage is a highly technical and specialized job that has evolved through time to become more institutionalized and specialized. Therefore, the crime of espionage is the most severe and dangerous threat to the state's security.

The definition of "attack" was made according to the resolution of the United Nations General Assembly dated 1974 and numbered 3814. According to this definition, an attack is the use of armed force against the sovereignty, territorial integrity or political independence of a state. Again, according to this definition, any action that is incompatible with the United Nations Charter. The use of

armed forces in such a manner is also considered an attack.

According to United Nations law, cyber attacks do not qualify as "armed attacks". It is still debated whether it is possible for a state subjected to cyber attacks to use weapons within the framework of the right of self-defense in terms of the United Nations Convention.

Cyber Terrorism is the realization of terrorist activities using the cyber space. It can be defined as terrorist organizations' use of cyber space as a tool. According to another definition, cyber terrorism is the combination of cyber space and terrorism. Cyber terrorism is an unlawful attack or threat of attack on computers, networks, or places where information is stored, in order to humiliate or intimidate a state or its citizens in order to achieve political or social goals.

The main thing is whether cyber attacks can be considered armed attacks or not. Most opinions are that a cyber attack can come to the brink of an armed attack in today's technology. Article 51 of the United Nations Charter regulates the right of self-defense. There are deep divergences between states regarding whether the said regulation, which gives the right to use force, can be applied for cyber attacks. Today, a "common analytical framework" for cyber attacks has not been developed. This situation complicates the solution.

Despite this difficulty in reaching a common definition of state-sponsored cyberattacks and cyberattacks by non-state actors, it is important to discuss under what conditions these attacks can constitute an armed attack within the framework of Article 51 of the United Nations Charter. As a prerequisite for exercising the right of self-defense, according to Article 51 of the United Nations Charter, it has to be an "armed attack", not just an "attack". The capabilities of developing technology and cyber weapons show that the concept of "armed attack" in Article 51 of the United Nations Charter and the concept of "use of armed force" is evolving.

When the United Nations Charter was prepared, it undoubtedly referred to the use of military force with conventional weapons to describe an "armed attack". However, in the information age, the concept of "conventional use of military force" no longer means much.

There are three views on when a cyber attack will be considered as an "armed attack" and whether it will trigger the right of self-defense or not. These are tool based, goal based and impact based approaches. According to the tool-based approach, cyber attacks cannot be considered as an armed attack under Article 51 of the United Nations Charter. In the target-based approach, an armed attack means targeting a critical computer system in a cyber attack. In this approach, for preventive self-defense, the cyber-attack must be a sign of significant and sufficiently probable damage. In the impact-based approach, a cyber attack will be considered an armed attack depending on the gravity of the impact. This approach is accepted particularly by states with advanced technology and those most exposed to such attacks.

There are different opinions about measuring the weight of the impact of the cyber attack that will give rise to the right of self-defense. In the effect-based approach, there are seven criteria for deciding whether a particular cyberattack contains "force" or not. These are *Severity, Immediacy, Directness, Invasiveness, Measurability, Presumptive legitimacy* and *Responsibility*. Since it is very difficult to detect the effects of cyber attacks, it is not easy to determine which actions are destructive.

Information and communication technologies continue to advance. The fact that the International Conventions have not been updated delays taking appropriate measures aligned with new technological developments. This causes an increase in cyber attacks. For this reason, decisions involving sanctions against cyber crimes and cyber attacks cannot be taken hastily. This can create an even conducive environment for attacking groups. Measures taken by constitutional and legal levels cannot cope with new types of technological crimes. In addition to technological and legal regulations and corresponding measures, the causes and factors offering a favourable environment for such crimes should be eliminated.

In order to counter cyber crimes and related issues, more studies needed to improve our understanding, inform policies and develop and strengthen cooperation between individuals, institutions and countries. All states need to take constitutional, legal, technical and administrative measures on cybersecurity. For this purpose, "national virtual environment security policies" should be developed and constantly updated. National information security should be given utmost importance. A cyber security awareness culture should be established and supported by regional and global international institutions and organizations. A common understanding on cyber security needs to be adopted at all levels.

Against such context, we have endeavoured to bring together contributions from a multidimensional perspective in this edited book titled "*Cyber Environment and International Politics*". We aimed to clarify a wide array of topics while also bringing depth, timeliness and richness to this field of scholarship.

We would like to express our sincere thanks to our invaluable colleagues and researchers who contributed and supported us in completing this book, and congratulate them all wholeheartedly. In addition, we express our warm gratitude to Ibrahim Sirkeci, Chief Publications Editor of Transnational Press London, who supported the publication of this book throughout.

We sincerely hope that the work will be of use to those interested in this field.

Hasret Çomak, Burak Şakir Şeker, Yaprak Civelek, Çağla Arslan Bozkuş

Istanbul, April 2022

causes, effects and results. France is defining a practical approach to strengthening the cybersecurity of its industrial infrastructure and is preparing a number of documents. The cyber attacks have increased the concerns about cybersecurity and the effectiveness of ANSSI. Thus, partly as a result of ANSSI's leadership, the number of cyber attacks in France is decreasing.

The increase in international cyber attacks has been effective in the formation of France's cyber security policy. After the ever-increasing number of cyberattacks, France realized that it lagged behind its global competitors in terms of security and defence. Thus, it has increased efforts to increase national cybersecurity and defence capabilities and to achieve more effective international cooperation and coordination, especially with the European Union and NATO.

Although France has come a long way in terms of its cyber policy, organization and budget, the increase in attempted and successful cyber attacks continues. There are yet many challenges in the public and private sectors in France, such as increasing the budget, structuring the institutions, and updating the legal regulations.

France understood that its national sovereignty would be irreparably shaken if it did not allocate the necessary financial resources for cyberspace. For this reason, the budget allocated by France for cyber defense has increased significantly.

France has conceptualized and adopted a rather offensive cybersecurity and cyber defence model in recent years. The recently published offensive doctrine represents the peak of this profound transformation, mainly in the armed forces.

An aggressive strategy document by France's Minister Parly has concrete indications that Russia is seen as an enemy in cyber warfare. In addition, France did not have strict statements about Russia on cyber issues in the past years. With this statement, France has also shown in cyberspace that it is with the Western Bloc, which includes the USA and the EU.

In conclusion, it would be appropriate to say that cyber security is an area that needs to be given great importance and investment. France aims to promote international rules and stability in cyberspace to prevent the escalation of cyber crises. However, it seems that France is trying to create a room for manoeuvre to support traditional operations, deterrence and return to ensure its national security in cyberspace. In this context, France wants to create a safe and delicate balance within the anarchic structure in cyberspace. When creating this balance, it grabs many opportunities and, at the same time, it faces as many risks and threats.

TURKEY'S CYBER SECURITY POLICIES

Ozan Örmeci[1], Eren Alper Yılmaz[2], and Ahmet Emre Köker[3]

Introduction

There is no denying that with the development of Internet technologies and social media, all industries and various aspects of life have become more Internet-based or online in the last three decades. During the recent Covid-19 (coronavirus) pandemic, the dense effects of the mighty Internet became even more significant through rapidly spreading online education systems and the explosion of E-commerce. There is no doubt that the Internet has made life easier and more comfortable. This technology has increased personal freedoms considerably. However, malignant, criminal-minded people, as well as terrorist organizations and hostile states, also take advantage of Internet freedoms. For this reason, cyber security has become a major concern for all states in the last two decades. Turkey, as a developing country, is no exception, and has therefore been trying to adapt itself to the conditions inherent in the Worldwide Web.

Since the early 1990s, upon the globalization process, the concept of information has played a major role in the globalization process. Because of the quick spread of information and communication technologies in developed states, the concept of "security" has been redefined due to new perceptions of threats against states. Organized crime, human smuggling, illegal immigration, money laundering etc. have disrupted the balance of the international system and revealed new enemies for states. Especially the rising tension after the disaster of 11 September 2001 (9/11) has led to a "Digital Catastrophe" scenario and created the fear of cyber terrorism against the West. In recent years, the emergence of fundamentalist Islamic terrorist organizations such as the Islamic State of Iraq and the Levant (ISIS) has coincided with the spectre of cyber terrorism.

This chapter analyzes Turkey's cyber security policies by focusing on the primary sources (official documents and statements made by top state officials, as well as legislation) and secondary sources (books, theses, academic articles, news, and analysis). We begin by introducing the reader to some key concepts related to cyber security. Secondly, we elaborate on the changing security perspective and perception after the end of the Cold War period. This considers the rapid development of Internet technologies and the addition of cyber security

[1] Associate Professor, Political Science and Public Administration Department, Istanbul Kent University, Turkey. E-mail: ozan.ormeci@kent.edu.tr / ozanormeci@gmail.com. ORCID: 0000-0001-8850-6089.
[2] Research Assistant, Public Administration Department, Aydın Adnan Menderes University, Aydın, Turkey. E-mail: alpery@adu.edu.tr. ORCID: 0000-0002-5137-4948.
[3] PTT A.Ş. Genel Müdürlüğü, Ankara, Turkey. E-mail: a.emrekoker@hotmail.com
ORCID: 0000-0002-8032-4237.

to the classical security paradigm. Thirdly, the authors will focus on cyber security institutions in Turkey and the existing legal framework. Fourth and finally, we review the statistical aspects of cybercrimes committed in Turkey.

Key Concepts

Cyber/Cyberspace

The term "cyber" refers to computers, computer networks, and related things that are broadly described as the Internet and its virtual environment.[4] However, this term is often used synonymously with the term "cyberspace" in the literature. The United Nations (UN) defines cyberspace as "the global system of systems of internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net. "[5] This mostly means the Internet, but the term may also be used to denote a specific and limited electronic information environment of a military, a corporation, and/or a government.[6]

An essential definition of cyberspace was made by Singer and Friedman as "the domain characterized by the use of the electronic and electromagnetic spectrum from computers and missiles to rays coming from the sun."[7] By another definition, cyberspace is "the numeric environment composed of information systems spread over the entire world and space, the networks interconnecting these systems or independent information systems. "[8] The National Military Strategy for Cyberspace Operations, on the other hand, defines cyberspace as the "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. "[9]

The cyberspace consists of two unified structures: physical and virtual. The physical structure contains all kinds of information and communication systems and users. These include digital electronic devices, computers, smart phones, smart objects, sensors/detectors, satellite systems, and all computer networks. The virtual structure includes all kinds of data and information produced with software and codes, stored, transmitted, and used for various purposes, especially operating systems in the physical environment.[10] The complexity of cyberspace

[4] Merriam-Webster Dictionary, "Definition of Cyber," https://www.merriam-webster.com/dictionary/cyber (Access 03.10.2021).
[5] The United Nations Terminology Database, "Cyberspace," https://unterm.un.org/UNTERM/dgaacs/unterm.nsf/webview/99b98bdbcbab096185256e620052efd3?opendocument (Access 02.10.2021).
[6] Jason Andress, Steve Winterfield, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham, MA, Elsevier Inc., 2014, p. 4.
[7] P. W. Singer, Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know*, Oxford, Oxford University Press, 2014, p. 13
[8] Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy,* p. 7, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf (Access 03.09.2021).
[9] Jason Andres, Steve Winterfield, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, p. 3.
[10] Mustafa Şenol, Türkiye'nin Ulusal Siber Güvenlik Strateji ve Politikalarının Oluşturulması Çerçevesinde

begins with the distinction between two separate spheres of implementation. First we consider the commercial Internet that serves the daily activities of the public and is generally the target of non-state actors. The vulnerability of this area was revealed by the cyber-attacks that took place in Estonia and Georgia in April-May 2007 and August 2008, respectively. Secondly, military networks have gained importance in a way that could threaten the security of other states. Over the past two decades, the militaries of various states have attempted to enhance warfighting capabilities through network-centric warfare. For instance, according to Carafano and Sayers, states such as the People's Republic of China (China) and the Russian Federation (Russia), which remain militarily inferior to the United States of America (USA), have identified the vulnerability of USA cyberspace and worked elaborately to benefit from military information gained by spying.[11]

Cyber Security

Cyber security aims to create and maintain the security features of institutions, organizations, and users in a way that can counter the security risks in the cyber environment. This definition includes personnel, infrastructures, applications, services, electronic communication systems, and all information transmitted and stored in the cyber environment of institutions, organizations, and users.[12] According to the 2016-2019 National Cyber Security Strategy of Turkey, cyber security means the "protection of information systems forming cyber space from attacks, assuring confidentiality, integrity, and availability of information/data processed in this environment, detection of attacks and cyber security incidents, activation of counter-response mechanisms, and recovering systems to conditions prior the cyber security incident."[13] The basic principles of cyber security form the heart of information security to protect countries against cyber risks and threats. If any of these principles, known as the "CIA triangle—confidentiality, integrity and availability," is damaged, security is compromised. When these three principles of data are damaged, infrastructures that contain information systems may cause loss of life, large scale economic loss, national security gaps or disturbance of public order.[14]

Cyber Deterrence

Explaining deterrence in general as "intimidating the others not to commit hostile acts," Libicki defines cyber deterrence as "deterring the aggressor from a cyber-attack by punishing its action in the cyber environment and creating

Caydırıcılık, PhD thesis, İstanbul, İstanbul Technical University, 2020, p. 9.
[11] James Jay Carafano, Eric Sayers, "Building Cyber Security Leadership for the 21st Century," The Heritage Foundation, 16.12.2008, https://www.heritage.org/defense/report/building-cyber-security-leadership-the-21st-century (Access 02.09.2021).
[12] M. Emin Ulaşanoğlu, Ramazan Yılmaz, M. Alper Tekin, *Bilgi Güvenliği: Riskler ve Öneriler*, Ankara, Bilgi Teknolojiler ve İletişim Kurumu (BTK), 2010, p. 8.
[13] Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy*, p. 10.
[14] *Ibid.*, p. 9.

disincentives for starting or carrying out further hostile action. "[15] Punitive measures feed into the enemy's calculation of whether the costs of cyber aggression outweigh the benefits. In addition to that, in Iasiello's view, "cyber deterrence is a strategy by which a defending state seeks to maintain the status quo by signaling its intentions to deter hostile cyber activity by targeting and influencing an adversary's decision-making apparatus to avoid engaging in destructive cyber activity for fear of a greater reprisal by the initial aggressor. "[16]

Cyber deterrence is so difficult to execute because there are many techniques that should be put into practice in order to achieve successful deterrence results. A cyber deterrence strategy should have some basic parameters that operate the process effectively. Without these parameters, an aggressor will not be able to receive and process the defender's intent, so states can run the risks of misunderstanding or misinterpreting. These parameters are communication, signaling, attribution, and proportionality.[17]

Cybercrime

Cybercrime, which seems as an international issue, is generally understood as "the acts that has automatic processing of information and constitute a contradiction against the law about the transfer of data via computers. "[18] In 2002, in the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, it is explained as "illegal actions targeting information system security/data transaction and realizing via information system/network."[19]

Cybercrime is also defined as the use of digital tools by criminals to steal or otherwise carry out illegal activities. The most common type of cybercrime is credential fraud, or the abuse of account details to defraud financial and payment systems. Such systems include credit cards, ATM accounts, and online banking accounts.[20]

The Council of Europe Cybercrime Convention (2004) determined that, in addition to crimes of unauthorized access, systemic interference and fraud, quantitatively emerging actions such as child pornography and copyright violations using widespread information and Internet systems are included within the scope of cybercrime.[21]

[15] Martin C. Libicki, *Cyber Deterrence and Cyberwar*, California, RAND Corporation, 2009, p. 28.
[16] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security*, Vol. 7, No: 1, Spring 2014, p. 55.
[17] *Ibid.*, pp. 56-59.
[18] Hüseyin Çakır, M.Serkan Kılıç, *Güncel Tehdit Siber Suçlar*, Ankara, Seçkin Yayınları, 2014, p. 50.
[19] Oğuzhan Turhan, "Bilgisayar Ağları İle İlgili Suçlar", Planlama Uzmanlığı Tezi, Ankara, DPT Müsteşarlığı, 2006, p. 30.
[20] P. W. Singer, Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs To Know, p. 85.
[21] Mehmet Yayla, "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı," Hacettepe Hukuk Fakültesi Dergisi, Vol. 4, No: 2, 2014, p. 190.

Cyber Terrorism

Today's modern terrorist organizations widely use information technologies in order to structure their organizations, recruit personnel, and organize actions to accomplish their aims. Thus, they carry out cyber-attacks against the information systems of public and private institutions. Cyber terrorism acts, which intensified especially in the 2000s, aim to provide secret information and money flow by targeting key institutions. Yayla makes a general assessment of cyber terrorism as "illegal threats and damaging attacks on computers, network systems, and databases using information technology capabilities with the aim of realizing political or social goals, of threatening the states and its citizens, of forcing the states to change their policies."[22] The Federal Bureau of Investigation (FBI) defines cyber terrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[23] This consideration includes illegal and damaging attacks towards the network connections, computer systems, information systems and institutional databases so as to put pressure on political-social authorities and/or intimidate individuals.[24]

Jalil analyzes cyber terrorism under the following categories:

- Attack: The main purpose of cyber terrorists is to gain information by accessing a network or to gain an advantage over the other party by changing information in the system. This method is very common and widely used with a high success rate.

- Destruction: The main purpose is to destroy or damage computer systems. The consequences of such an attack can be terrible, whereby organizations might be forced to be out of operations for an uncertain time because of the intensity of the attacks.

- Disinformation: The goal is to foment an atmosphere of fear and chaos within the state by creating rumors and polluting information. This type of attack is so difficult to control because it can be done almost immediately without the need to access the target's computer and network systems.[25]

Cyber Warfare

Cyber warfare basically means "acting by one state to cause damage or disruption by infiltrating another state's computer systems and networks."[26] By this definition, cyber warfare occurs between states in cyberspace. According to

[22] Ibid., p. 195.
[23] P. W. Singer, Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs To Know, p. 96.
[24] Furkan Abacı, **Türkiye'de Siber Terörizme Karşı Bilişim Teknolojilerinin Kullanımı** (Unpublished Master Thesis), Osmaniye, Osmaniye Korkut Ata University Social Sciences Institute, 2020, p. 24.
[25] Shamsuddin Abdul Jalil, "Countering Cyber Terrorism Effectively: Are We Ready to Rumble?" SANS Institute, 2003, p. 8.
[26] Richard A Clark and Robert K. Knake, *Siber Savaş*, Translated by Murat Erduran, İstanbul Kültür University, İKÜ Publishing, 2011, p. 8.

a congressional report prepared by Steven A. Hildreth in 2001, cyber warfare involves a wide variety of elements for defending computer networks from attacks in cyberspace, denying the enemy's ability to launch the same attack in the future.[27]

Cyber warfare is symmetrical or asymmetrical, offensive or defensive digital network activities carried out by states or state-backed groups. These disruptions threaten critical national infrastructures, military systems, and/or serious industrial structures within the target country. For instance, cyber warfare has, in recent years, escalated with reports emerging of hackers supported by Russia and China launching attacks against other countries, including the Ukraine. Even in the United Kingdom, it was reported that the British Army had been examining ways of using malware as a military tool.[28]

Changing Security Perception/Perspective after the Cold War

Changing Security Perspective in the Post-Cold War Era

The world of the 20th century was shaped by classical security doctrines. With the development of sophisticated weapons, the First World War (1914-1918) was the first major event in which approximately 20-21 million people—combatants and civilians—were killed.[29] The amount of violence and bloodshed increased further with approximately 60 million casualties in the Second World War (1939-1945).[30] With the emergence of nuclear bombs, conventional warfare and security doctrines changed. The Cold War waged between the United States-led capitalist Western bloc and the Soviet Russia-led communist Eastern bloc during the second half of the 20th century (1945-1991) was dominated by nuclear weapon-based security strategies and concepts such as the "balance of terror." The international system of that period, which was shaped by two blocs, did not allow changes in power relations, neither internally, nor externally. During those years, the great existential risk posed by the "nuclear balance" maintained a stagnant stability in domestic and foreign policies.[31] Here, the "balance of terror" strategy was followed in order to guarantee mutually assured destruction as the paradoxical security of nuclear states against others if the dreadful necessity arose.[32] The Cold War was successful in preventing the emergence of large scale world wars, but other small scale wars were fought by proxy between the USA

[27] Steven A. Hildreth, "Cyberwarfare," Congressional Research Service, Order Code: RL30735, 19.06.2001, p. 1, https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-014.pdf (Access 01.09.2021).
[28] ITPro, "What is Cyber Warfare?" 15.10.2021, https://www.itpro.co.uk/security/28170/what-is-cyber-warfare (Access 03.10.2021).
[29] Britannica, "World War I: Killed, Wounded, and Missing," https://www.britannica.com/event/World-War-I/Killed-wounded-and-missing (Access 02.10.2021).
[30] The National WWII Museum, "Research Starters: Worldwide Deaths in World War II," https://www.nationalww2museum.org/students-teachers/student-resources/research-starters/research-starters-worldwide-deaths-world-war (Access 02.10.2021).
[31] Ali Karaosmanoğlu, "Savunma Planlaması ve Stratejik Belirsizlik," *Bilge Strateji,* Vol. 7, No: 12, 2015, pp. 23-45.
[32] Stephen Twigge, Alan McMillan, "Britain, United States and the Development of NATO Strategy 1950-1964", *Journal of Strategic Studies*, Vol. 9, No: 2, 1996, p. 271.

and USSR. Eventually, with the end of the Cold War and dissolution of the Soviet Union in the early 1990s, the world transformed into a different place.

The new paradigm seemed unipolar at the beginning, though it was quickly understood that even the USA was incapable of controlling the globe. Thus, a growing multipolarism was the distinctive feature of the 21st century world order with the USA and Russia gradually losing power. China's rapid rise and the formation of a strong union between 27 European states were other important features of the new global order. But more importantly, the world has transformed a lot since the 1990s due to technological transformation. Computers, Internet technologies, cell phones, remote systems, drones, and social media have become regular features in the early 21st century due to technological progress. These technologies and platforms created a more comfortable life for people, but also new risks for individuals, companies, and states.

Since the early 1990s, information has played a key role in the discipline of International Relations due to its importance for political means. Information and communication technologies now predominate in several aspects of industrialized states.[33] The deepening and expansion of security is basically related to the proliferation of security threats. In this context, it is necessary to examine the relationship between security, globalization, and technology. The permeability of borders and fluidity created by globalization and technology have also increased the number of threats towards individuals and the state.[34] Since the 1990s, due to the acceleration of the globalization phenomenon, a very rapid and unavoidable change process has begun. Globalization has multiplied the differentiation of security threats so thoroughly that the very concept of security requires reassessment. New threats such as organized crime, illegal immigration, human smuggling, drug/weapon smuggling, and money laundering have appeared huge international destabilisers. Thus, traditional threat perceptions and methods of struggling with these elements have been insufficient in combating these new dangers. This inadequacy has required a new security definition as well as new tools to implement an adequate response.[35] The increasing rate of cyber-attacks has caused nation states or international actors to work rapidly in this area. The development of basic critical infrastructures and cyber security is crucial for national interests. That is why each actor has started to give importance to cyber warfare not only for defence, but also for building offensive capabilities. Recent developments show that cyber wars will remain a reality in the 21st century.[36]

[33] Myriam Dunn Cavelty, "Cyber Security," in *The Routledge Handbook of New Security Studies*, J. Peter Burgess (Ed.), New York, Taylor & Francis Group, 2010, p. 159.
[34] Muharrem Aksu, Turhan Faruk, "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik," *Uluslararası Alanya İşletme Fakültesi Dergisi*, Vol. 4, No: 2, 2012, p. 71.
[35] Bilal Karabulut, Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek, Ankara, Barış Kitabevi, 2015, p. 119.
[36] Ayhan Gücüyener, "21. Yüzyılda 'Siber' Rekabet: Yeni Hedef Kritik Altyapılar mı?" LinkedIn, 10.03.2016, https://www.linkedin.com/pulse/21-y%C3%BCzy%C4%B1lda-siber-rekabet-yeni-hedef-

Cyber-attacks and Cyber Security Initiatives After 9/11

After the Cold War, the most important event that deeply affected and shaped the global security environment was the 11 September 2001 terrorist attacks in the USA. Before 9/11, cyberspace's risks and security problems were topics discussed only by a small group of experts. Since that day, the cyber world has created serious risks for societies increasingly dependent on each other.

The airplanes that crashed into various targets in New York and Washington D.C. completely changed the definitions of security, threats, and agenda in the international system. As a result of these attacks, the concept of national security, which became relatively obscure after the Cold War, took top place on the priority lists of many countries once again. The so-called war on terror not only entered the agenda of governments whose nations were exposed to attacks but also almost all actors in the system, accelerating precipitously under the leadership of the USA.

Just after the dust settled on the wreckage, it was understood that the terrorists who carried out the attacks had communicated among themselves over the Internet and had worked previously with these planes in simulations. This revelation reinforced the idea that the Internet could be used for terrorism.[37] For instance, all of the 9/11 attackers had *Hotmail* accounts and they were thought to have coordinated via notes left in the guestbook section of a website run by the brother-in-law of one of Osama bin Laden's lieutenants.[38] Richard Clarke, the chair of the President's Critical Infrastructure Protection Board, states that the Al-Qaeda terrorist organization was using the Internet to discover American vehicles and facilities before 9/11. If someone aggregates restricted and non-classified data, they can gain access to confidential information.[39]

In the period of high tension after 9/11, one of the most discussed issues in the international arena was the Digital Catastrophe scenario that would hypothetically cripple one of the NATO members. The possibility of cyber-attacks by terrorist groups raised expectations for a possible "Digital Pearl Harbor." It was considered that the economic and other critical infrastructures of nation states could be destroyed as a result of attacks on their cyber systems.[40] Since such concerns were closely associated with national security, many countries have added cyber security strategies to their national security documents and updated these regularly.

The Cyber Security Law was passed in the USA on November 13, 2001,

kritik-m%C4%B1-ayhan-gucuyener (Access 01.10.2021).

[37] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning," *Parameters*, Vol. 33, No: 1, 2003, p. 120.

[38] P. W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs To Know, p. 101.

[39] Global Savunma, "Siber Tehditler ve Siber Terörizm," 25.05.2020, https://www.globalsavunma.com.tr/ siber-tehditler-ve-siber-terorizm.html (Access 15.10.2021).

[40] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School," *International Studies Quarterly,* Vol. 53, No: 4, 2009, p. 1160.

which allowed the police to wiretap or use electronic surveillance without warrant. In that context, a "Total Information Awareness" plan developed by the Department of Defense to fight terrorism was put into use all over the country.[41]

Cyber-attacks against Estonia in 2007 were also a clear example of the increasing cyber threat after the Cold War. Following the collapse of the Soviet Union, there was constant conflict between Russia and Estonia. Relations between these nations were strained when the Estonian authorities removed the Soviet war monument, called the Bronze Soldier, from a central city square in Tallinn on April 26, 2007. In this process, Estonia, which included a large Russian minority, was exposed to intense cyber-attacks for three weeks. The attacks targeted the Estonian presidency and parliament, political parties, all ministries of the state, the country's most famous three media organizations, the largest bank, and communication companies. Cyber-attacks brought life to a halt in Estonia, which had Europe's strongest cable society and highest-level E-government application.

The event was not specified as a Cyberwar by NATO or the EU, but rather was classified as a cyber-attack. Due to the absence of significant material damage or harm to people, it was not accepted as an act of war. It was clearly stated that it was difficult to define cyber-attacks as clear military action.[42] Upon this attack, the NATO Cooperative Cyber Defense Center of Excellence was established between NATO and Estonia.

Moreover, in 2008, as a result of the mutual political crisis between Russia and Georgia, Russia launched a cyber-attack against Georgia. Russian cyber warfare was also deployed against Georgia's government websites and many of the country's commercial websites as well.[43] This sabotage shut down the Internet for several days and even led to electrical power outages. However, since Georgia's Internet networks were not very developed, the cyber-attacks did not lead to damage as great as that suffered in Estonia.

In recent history, another major cyber-attack that made a tremendous impact was the Stuxnet attack. The USA carried out this sabotage of Iranian nuclear power plants in 2009. Although the US authorities did not take responsibility for the attacks, the political answers and analysis revealed that the USA had a role in this case.[44] Thereafter, Edward Snowden stated in his interview that this was a

[41] TUİÇ, "Gözetim Politikaları ve Terörizm: 11 Eylül 2001", 04.01.2017, https://www.tuicakademi.org/gozetim-politikalari-terorizm-11-eylul-2001/ (Access 05.09.2021).

[42] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival,* Vol. 53, No: 1, 2011, p. 32.

[43] Asher Moses, "Georgian Websites Forced Offline İn 'Cyber War'," *The Sydney Morning Herald*, 12.08.2008, https://www.smh.com.au/technology/georgian-websites-forced-offline-in-cyber-war-20080812-gdsqac.html (Access 01.09.2021).

[44] Şener Çelik, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, Vol. 15, No: 1, 2014, p. 144.

joint attack by Israel and the National Security Agency (NSA) of the USA.[45] The attack was detected in 2010. The fact that the centrifuges, which were replaced in Iran's enriched uranium facilities during a year, reached 10 % revealed there was a problem with the system. A one-year study proved that the changes in centrifuges were actually due to a computer malfunction. The program was so powerful that it provided connections to more than 100,000 computers.[46]

In recent years, fundamentalist Islamic terrorist organizations have also frequently used cyber methods. For instance, ISIS carried out a cyber-attack against the official Twitter and YouTube accounts of The United States Central Command (CENTCOM) in 2015. The hackers shared the message from the accounts they hacked: "American soldiers, we are coming, watch your back. We know your personal phones and families. "[47] It was claimed that an ISIS-affiliated group calling themselves the Cyber Caliphate organized these attacks. According to the USA media, the attack was organized by British hacker Junaid Hussein (Abu Hussein El Britani), who is described as the most successful computer magician of ISIS.[48]

Moreover, in France, in 2015, ISIS launched a cyber-attack against the global broadcasting organization TV5 Monde, whose programs are broadcast in more than 200 countries worldwide. Hackers, who also seized the channel's websites, Facebook and Twitter accounts, published the message "I am ISIS" under the name "Cyber jihadists". Their messages also threatened French President François Hollande and the French Army.[49]

Bitcoin financing of the bombing attack carried out by ISIS in Sri Lanka in 2019 and the transfer of money by ISIS militants and sympathizers to the organization via Bitcoin reveals the extent of cyber terrorism. Although ISIS has suffered a major blow in the physical world, it has become increasingly active in the cyber arena in the last few years.[50]

Copenhagen School and the Securitization of the Internet

The Copenhagen School[51] is an influential school of thought within the

[45] *Spiegel International*, "The NSA and Its Willing Helpers," 08.07.2013, http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html (Access 01.10.2021).
[46] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired, 07.11.2011, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ (Access 01.10.2021).
[47] *Reuters*, "Apparent Islamic State Backers Hack U.S. Military Twitter Feed," 12.01.2015, https://www.reuters.com/article/us-cybersecurity-centcom-hack-idUSKBN0KL1UZ20150112 (Access 16.10.2021).
[48] *The Guardian,* "Briton Lead Suspect after US Central Command's Twitter Account is Hacked," 14.01.2015, https://www.theguardian.com/us-news/2015/jan/14/briton-suspect-us-central-command-twitter-hack-junaid-hussain-tony-blair (Access 16.10.2021).
[49] *The Local Fr*, "'Phishing email' the Key to Hacking of TV5Monde," 14.04.2015 (Access 16.10.2021).
[50] Emine Çelik, "Siber Terörizm ve IŞİD-Bitcoin İlişkisi," *Ortadoğu Analiz*, Vol. 10, No: 89, 2019, pp. 90-91.
[51] For details, see: Serdar Çukur, "Kopenhag Okulu'nun Güvenlikleştirme Teorisi Bağlamında ABD'nin Irak Politikası: 2000-2008," *UPA Strategic Affairs*, Vol. 1, No: 1, 2020, pp. 51-72.

International Relations discipline. Its origins are in scholar Barry Buzan's famous book *People, States and Fear: The National Security Problem in International Relations* (1983). Other than Buzan, the Copenhagen School has important representatives and theorists such as Ole Wæver and Jaap de Wilde. The Copenhagen School places particular emphasis on the non-military aspects of security, thus representing a shift away from traditional security studies. The theory takes its name from the Danish research institute, Copenhagen Peace Research Institute (COPRI) since many of its members worked at this institution. The fundamental reference for this concept is *Security: A New Framework for Analysis*, written by Buzan, Wæver and De Wilde in 1998.

The main contribution of the Copenhagen School is its explanation of how the securitization mechanism works. By making a mixture of Neo-Realist and Social Constructivist concepts, theorists of this school focused on how an event or a group becomes a security issue when it poses an existential threat to some object.[52] The core of Securitization Theory lies in the fact that, in International Relations, an issue becomes a security issue not because something constitutes a real objective threat to a state (or another referent entity), but rather because an actor has declared something as an existential threat to its survival. By doing so, the actor (very often nation states) has claimed the right to handle the issue through extraordinary means to ensure the referent object's survival. However, the fact that security is a social and intersubjective construct does not mean that everything can become easily securitized. In order to successfully securitize an issue, a securitizing actor has to perform a securitizing move that then must be accepted by a targeted audience.[53] Only by gaining acceptance from the audience can the issue be moved above the sphere of normal politics, allowing elites to break normal procedures and rules in order to implement emergency measures.

Keeping basic arguments of the Copenhagen School in mind, one could easily understand how the Internet has become a more securitized issue and platform in recent years because of various types of cybercrimes committed as well as cyber terrorism and/or cyber warfare. The comfortable ground for the securitization of the Internet was created by the statements and rhetoric of important politicians who can influence public opinion. For instance, İsmail Demir, the President of the Turkish Defense Industries, emphasizes that a country's defence is not limited to weapons, cannon, rifles, satellites and defence systems, but also consists of cyber security. He pointed out one of Turkey's basic goals is to develop a system using domestic and national products to enable the cyber security solutions that Turkey needs.[54] In addition to that, Turkish

[52] Ali Diskaya, "Towards a Critical Securitization Theory: The Copenhagen and Aberystwyth Schools of Security Studies," *E-International Relations*, 01.02.2013, https://www.e-ir.info/2013/02/01/towards-a-critical-securitization-theory-the-copenhagen-and-aberystwyth-schools-of-security-studies/ (Access 06.11.2021).
[53] *Ibid.*
[54] *AA,* "Cumhurbaşkanlığı Savunma Sanayii Başkanı Demir: Siber Güvelik Kümelenmesi hareketini başlattık," 21.12.2020, https://www.aa.com.tr/tr/bilim-teknoloji/cumhurbaskanligi-savunma-sanayii-baskani-demir-siber-guvelik-kumelenmesi-hareketini-baslattik/2083869, (Access 07.11.2021).

President Recep Tayyip Erdoğan has repeatedly emphasized that crimes committed on the Internet are also open to legal investigations.[55]

In the USA, the same tactic was utilized by ex-President Donald Trump for blaming China.[56] Current President Biden's administration also uses similar arguments to accuse China of cyber-attacks against the USA.[57] Besides these speeches, the USA Defense Department Acting Chief Information Officer, Kelly Fletcher, states that the National Security Agency (NSA) works with powerful defense industrial base companies to share resources related to cyber issues.[58] By making these statements, leaders of many countries garner public support for regulating the Internet. Thus, the basic mechanism explained by the Copenhagen School perfectly explains how securitization of the Internet has become a major International Relations issue in recent years.

Cyber Security in Turkey

In Turkey, 48 million of 80 million residents use the Internet.[59] According to this statistic, Internet and computer users constitute more than half of Turkey's total population (60 %). Increasing use of the Internet and computer creates many cyber security risks. These security risks include the security of critical infrastructures, disruption of confidentiality, the integrity or accessibility of information, a large-scale economic damage, the emergence of national security vulnerabilities or disruption of public order. On the other hand, with the increase in mobile devices in Turkey and development of the "Internet of things," the operation of all processes has entered the cyber realm. Therefore, this unexpected expansion of cyberspace has made it vulnerable to all kinds of attacks.[60]

Cyber Security Institutions in Turkey

Turkey's Ministry of Transport and Infrastructure is the main institution responsible for control and management of cyberspace in Turkey. Its activities

[55] Muhammed Boztepe, Muhammed Ali Toruntay, Özcan Yıldırım, Zafer Fatih Beyaz, "Cumhurbaşkanı Erdoğan: İnternet mecralarını kullananlar suç işlemede layüsel değildir," *Anadolu Ajansı*, 01.07.2020, https://www.aa.com.tr/tr/turkiye/cumhurbaskani-erdogan-internet-mecralarini-kullananlar-suc-islemede-layusel-degildir/1895629 (Access 06.11.2021).

[56] Justin Sink, "Faced with Massive Suspected Russian Cyber-attack on the U.S. government, Trump blames China," *Fortune*, 21.12.2020, https://fortune.com/2020/12/21/faced-with-massive-suspected-russian-cyber-attack-on-the-u-s-government-trump-blames-china/ (Access 06.11.2021).

[57] Dustin Volz and Aruna Viswanatha, "Biden Administration Blames Hackers Tied to China for Microsoft Cyberattack Spree," *The Wall Street Journal*, 19.07.2021, https://www.wsj.com/articles/biden-administration-to-blame-hackers-tied-to-china-for-microsoft-cyberattack-spree-11626692401 (Access 06.11.2021).

[58] Bhavya Sukheja, "Pentagon Says NSA Working with Major Firms on Cyber Issues, Defense Information Sharing," *Republic World*, 08.10.2021, https://www.republicworld.com/world-news/us-news/pentagon-says-nsa-working-with-major-firms-on-cyber-issues-defense-information-sharing.html (Access 07.11.2021).

[59] Fulya Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi," *International Journal of Multidisciplinary Studies and Innovative Technologies*, Vol. 1, No: 1, 2017, pp. 24-28.

[60] Kerim Göztepe, Recep Kılıç, Alper Kayaalp, "Cyber Defense in Depth: Designing Cyber Security Agency Organization for Turkey," *Journal Of Naval Science And Engineering*, Vol. 10, No: 1, 2014, pp. 1-24.

are carried out by the Information Technologies and Communications Authority (*Bilgi Teknolojileri ve İletişim Kurumu*, or BTK). The Ministry of Transport and Infrastructure has been authorized to prevent cyber-attacks and to ensure national cyber security. Within the framework of this authority, the Ministry takes decisions regarding the execution, management, and coordination of Turkey's national cyber security activities. Within the framework of the decisions taken, transformations are carried out to ensure cyber security in institutions responsible for national security.[61]

The most concrete indicator of the institutional transformation was realized with the activation of the BTK in 2000.[62] The BTK is the official regulatory agency for the Turkish telecommunications sector. Accordingly, business and transactions within the country are monitored by the Cyber Security Operations Center (Siber Güvenlik Operasyon Merkezi) and the TR-CERT/Computer Emergency Response Team of the Republic of Turkey (*Ulusal Siber Olaylara Müdahale Merkezi*, or USOM) within the BTK.[63] These two branches of the BTK are operated 24 hours a day, 7 days a week. Software projects such as "Hunter", "Azad", and "Kasırga" are developed with corporate internal resources within the body of BTK, which provides uninterrupted security services to protect Turkey in cyberspace.[64] These software projects have made very important contributions to Turkey's national cyber security. With these domestic and national projects and applications, According to Turkey's Minister of Transport and Infrastructure, Adil Karaismailoğlu, implementation of these domestic projects and national applications has prevented more than 500,000 cyber-attacks against Turkey since 2017.[65]

In order to increase awareness and readiness, in recent years the BTK has conducted cyber defense exercises. These exercises have a significant impact on the prevention of cyber-attacks. Cyber security agreements are signed and alliance relations are developed simultaneously with the exercises. As the importance of cyber defence exercises at the global level increases, the importance given to cyber defence exercises in Turkey is also increasing. BTK conducts the following exercises as part of its mission:[66]

1. National Cyber Security Exercise (25-28 January 2011): The 1st National Cyber Security Exercise (NCSE '11) was held with the participation of 41 public, private, and non-governmental organizations (NGOs), as well as various

[61] Hakan Hekim and Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları," *Uluslararası Güvenlik ve Terörizm Dergisi*, Vol. 4, No: 2, 2013, pp. 135-158.

[62] For its website, see: https://www.btk.gov.tr/.

[63] For its website, see: https://www.usom.gov.tr/.

[64] Havelsan, "Siber savaşlara hazır mıyız?" *Yurtta ve Dünyada Siber Güvenlik*, August-September-October 2019, p. 63, https://savunmasanayiidergilik.com/public/images/uploads/Pdf/2212020165842662-havelsan-dergi-sayi-3-min.pdf (Access 07.11.2021).

[65] Ayşe Böcüoğlu Bodur, "Yerli ve milli uygulamalarla 500 binden fazla siber saldırı engellendi," Anadolu Ajansı, 17.10.2021, https://www.aa.com.tr/tr/bilim-teknoloji/yerli-ve-milli-uygulamalarla-500-binden-fazla-siber-saldiri-engellendi/2394540 (Access 06.11.2021).

[66] Bilgi Teknolojileri ve İletişim Kurumu, "Siber Güvenlik Tatbikatları," https://www.btk.gov.tr/siber-guvenlik-tatbikatlari (Access 21.10.2021).

ministries, judicial and law enforcement forces.[67]

2. Cyber Shield Exercise '12 (May 2012): It was held under the coordination of BTK with the participation of 12 operators representing 99.9 % of Turkey's national Internet infrastructure.[68]

3. National Cyber Security Exercise (NCSE '13): It was held under the coordination of the Ministry of Transport, Maritime Affairs, and Communications with the participation of 61 public and private sectors, together with the Scientific and Technological Research Council of Turkey (TÜBITAK).[69]

4. National Cyber Defense 2017 Exercise: It was organized within the framework of the 2016-19 National Cyber Security Strategy and Action Plan. In this exercise, unlike previous exercises, real cyber-attacks were launched against institutions in the first phase.[70]

5. Cyber Shield Security Exercise 2019: The technical infrastructure and scenarios of the Cyber Shield Security Exercise held in 2019 were prepared by the National Cyber Incidents Response Center (USOM). It was held with the participation of approximately 90 competitors on 19 teams from 17 different countries, including Turkey.[71]

6. International Cyber Shield 2021: BTK organized this event in 2021.[72]

The mechanism that carries out efforts to ensure cyber security in Turkey is based on the activities of the TR-CERT/Computer Emergency Response Team of the Republic of Turkey (USOM), which operates under the BTK. All these cyber defense exercises aim to increase the awareness of cyber security and create the necessary capability to act in different possible scenarios that may occur in the cyber field.

The Ministry of Transport and Infrastructure has another institution called the Cyber Security Council (*T.C. Ulaştırma ve Altyapı Bakanlığı Siber Güvenlik Kurulu*), which was established in 2012.[73] The institution's main duties are listed as:[74]

[67] TÜBİTAK BİLGEM, "Siber Güvenlik Tatbikatı," https://bilgem.tubitak.gov.tr/tr/haber/siber-guvenlik-tatbikati (Access 21.10.2021).
[68] *Bilişim Dergisi,* "Siber Kalkan Tatbikatı 2012 tamamlandı," pp. 178-179 (Access 21.10.2021).
[69] *BT News,* "Ulusal Siber Güvenlik Tatbikatı 2013 başladı," https://www.bthaber.com/ulusal-siber-guvenlik-tatbikati-2013-basladi/ (Access 21.10.2021).
[70] Rekabet Kurumu, "Ulusal Siber Savunma 2017," 13.12.2017, https://www.rekabet.gov.tr/tr/Haber/ulusal-siber-savunma-2017-1d4f3e6d0be0e71180e00050568d4f05 (Access 21.10.2021).
[71] Bilgi Teknolojileri ve İletişim Kurumu, "Siber Kalkan 2019 Sona Erdi," https://www.btk.gov.tr/haberler/siber-kalkan-2019-sona-erdi (Access 21.10.2021).
[72] Arife Yıldız Ünal, "Ulusal Siber Kalkan 2021 Tatbikatı Başladı," *Anadolu Ajansı*, 12.10.2021, https://www.aa.com.tr/tr/bilim-teknoloji/ulusal-siber-kalkan-2021-tatbikati-basladi/2389588 (Access 21.10.2021).
[73] For its website, see; https://www.btk.gov.tr/siber-guvenlik-kurulu.
[74] "Siber Güvenlik Kurulu," Bilgi Teknolojileri ve İletişim Kurumu, https://www.btk.gov.tr/siber-

1. Approving cyber security related policies, strategies, and action plans, and taking necessary precautions to implement them;
2. Deciding on proposals for critical infrastructures;
3. Determining institutions that are exempted from cyber security regulations or some portions of these regulations;
4. Conducting other duties set by law.

The Cyber Security Council works in order to determine cyber security measures to be taken by public institutions and organizations, real and legal persons. The Council approves prepared plans, programs, reports, procedures, principles and standards, then ensures their implementation and coordination.

Other than BTK-related branches, there are some other institutions that have operational roles in Turkey's cyber security. Among them, one critical institution is the General Directorate of Security-Combating Cybercrimes Department (*Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı*).[75] This institution was established in 2011 in order to conduct the legal/forensic aspect of cybercrime fighting from a single, centralized directorate. The General Directorate of Security-Combating Cybercrimes Department is responsible for eliminating cyber incidents, reducing possible damage, and carrying out cyber incident management in coordination and cooperation at the national level. The Directorate's main goals are:[76]

1. Fighting cybercrime;
2. Increasing awareness about cybercrimes;
3. Developing international cooperation in the fight against cybercrime;
4. Analyzing cyber security threats against Turkey and developing necessary defenses;
5. Training professional cybercrime fighters;
6. Following technological developments closely and increasing the institution's capabilities.

Another institution important for cyber security is the Turkish Armed Forces (TAF) Cyber Defense Command (*TSK Siber Savunma Komutanlığı*). The command was set up in 2012 and works actively to eliminate threats against Turkey's cyber security. The TAF Cyber Defense Command is assigned to strengthen the cyber security of information systems through national software and to instantly react to cyber incidents targeting the armed forces.[77] The institution works in

guvenlik-kurulu (Access 07.11.2021).
75 For its website, see: https://www.egm.gov.tr/siber.
[76] "Hakkımızda," Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, https://www.egm.gov.tr/siber/hakkimizda2 (Access 07.11.2021).
[77] Tuba Eldem, "The Governance of Turkey's Cyberspace: Between Cyber Security and Information

coordination with other related institutions such as the Ministry of Transport and Infrastructure, the Ministry of Foreign Affairs, and TÜBİTAK.[78] The command also works in coordination with NATO and its related branches. Together with Turkey's Presidency of Defense Industries (*Savunma Sanayii Başkanlığı*/SSB), the command initiated a new project called "*SİSAMER*" a few years ago in order to create a new centre where all related information will be collected for monitoring threats against Turkey.[79]

TÜBİTAK is also influential in Turkey's cyber security policies.[80] TÜBİTAK's stated goal is to develop "science, technology and innovation" policies, support and conduct research and development, and to "play a leading role in the creation of a science and technology culture" in Turkey. TÜBİTAK was founded in 1963 as an autonomous public institution, governed by a Science Board. One of the Council's branches is the Cyber Security Institute (*Siber Güvenlik Enstitüsü*), which was established in 2012 to conduct scientific studies with the objective of increasing Turkey's technological capacity.[81] Cyber Security Institute is tied to TÜBİTAK's Informatics and Information Security Research Center (BİLGEM).

The last important institution to be active in Turkey's cyber security policies is Turkey Cyber Security Cluster (*Türkiye Siber Güvenlik Kümelenmesi*).[82] The Cyber Security Cluster is a project conducted by SSTEK A.Ş. (a subsidiary of Turkey's Presidency of Defense Industries/SSB) and supported by SSB and the Digital Transformation Office of the Presidency of Turkey (*Dijital Dönüşüm Ofisi Başkanlığı*). The goals of the project are stated as:[83]

- Increasing the number of cyber security firms in Turkey;
- Helping its members' technical, administrative, and financial development;
- Improving the standards of cyber security in Turkey;
- Helping to the branding process of its members' products and services;
- Improving the competitiveness of its members in the national and global market;
- Raising the number and quality of the social capital in the cyber security field;
- Increasing the awareness and culture of cyber security throughout society.

As we can see in the examples above, many Turkish cyber security institutions are coordinated in a democratic and secure atmosphere.

Turkey's Cyber Security Policies: An Analysis of the Legal Framework

In this section, Turkey's cyber security policies from 2008 to the present will be analyzed within the context of the legal framework.

The 5809 Electronic Communications Law (2008)

Firstly, Turkey's cyber security policies were prepared by adding some annexes to the 5809 Electronic Communications Law that was put into action in 2008.[84] The first decision on cyber security was to determine policies, strategies, and targets for the purpose of ensuring national cyber security. The intent was to determine the procedures and principles regarding the provision of cyber security for public institutions and organizations, as well as for real and legal persons. The law codified procedures and principles that real and legal persons must obey (Annex: 6/2/2014-6518/102 art).

Additionally, this law regulates cyber security and Internet domain names via the Presidency of Telecommunication and Communication or other units (Annex: 6/2/2014-6518/103 art). Besides these decisions, the institution takes all kinds of measures to protect public institutions and organizations, as well as real and legal persons, from cyber-attacks and to provide deterrence against such attacks (Annex: 15/8/2016-KHK-671/25 art).

Cabinet Decree No. 2012/3842 on Execution, Management and Coordination of National Cybersecurity Works

In 2012, the Cabinet Decree No. 2012/3842 on Execution, Management and Coordination of National Cybersecurity Works was put into force by the Republic of Turkey.[85] According to this decision, it is necessary for public institutions and organizations to comply with the plans, programs, procedures, and principles published by the Ministry of Transport, Maritime Affairs, and Communication in order to ensure national cyber security. During the development of national cyber security, it is essential to devise national solutions in all possible areas and use national resources in software and hardware infrastructures (Article 3).

In line with this decision, a Cyber Security Council (*T.C. Ulaştırma ve Altyapı Bakanlığı Siber Güvenlik Kurulu*) was established under the Ministry of Transport

Security," *International Journal of Public Administration*, Vol. 43, No: 5, 2020, pp. 452-465.

[78] *Hürriyet*, "Türk ordusunun yeni kuvveti siber savunma," 06.06.2016, https://www.hurriyet.com.tr/teknoloji/turk-ordusunun-yeni-kuvveti-siber-savunma-40113652 (Access 07.11.2021).

[79] Liy Ajans, "Siber Savunma Merkezi (SİSAMER)," 10.11.2015, https://www.liyajans.com/portfolio/sisamer/ (Access 07.11.2021).

[80] For its website, see: https://tubitak.gov.tr/.

[81] For its website, see: https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi.

[82] For its website, see: https://siberkume.org.tr/Index.

[83] Türkiye Siber Güvenlik Kümelenmesi, "Hakkımızda," https://siberkume.org.tr/About (Access 07.11.2021).

[84] *Resmi Gazete,* "Elektronik Haberleşme Kanunu," 27050, 10.11.2008, https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm (Access 15.10.2021).

[85] *Resmi Gazete*, "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar," 28447, 20.10.2012, https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm (Access 15.10.2021).

and Infrastructure. This council's duty is to determine measures regarding cyber security, to approve the prepared report, procedures and principles, and to ensure their implementation and coordination (Article 4). In addition to this, the council dictates authorities and duties of the Ministry of Transport and Infrastructure relevant to cyber security. In this context, the Ministry is responsible for preparing policy, strategy and action plans, ensuring the establishment of technical infrastructure in public institutions and organizations, carrying out awareness and training activities on national cyber security etc. (Article 5).

Law on Crimes Committed in the Cyber Environment

European Council members including Turkey signed another agreement on cyber security called the Law on Crimes Committed in the Cyber Environment.[86] The framework of this decision encapsulates policies for protecting society from crimes committed in the virtual environment, increasing cooperation between the state and private sector to prevent cyber-attacks, aggravating sanctions against cybercriminals, and ensuring data privacy. In this document, cybercrimes are particularly explained and the with explicit emphasis on necessary precautions.

National Cyber Security Strategy and 2013-2014 Action Plan

In 2013, Turkey's Ministry of Transport, Maritime Affairs, and Communications published a detailed "National Cyber Security Strategy and 2013-2014 Action Plan. "[87] The action plan outlined some definitions, objectives, and principles for cyber security to be carried out in the short term. For instance, one of the main objectives of National Cyber Security Strategy and 2013-14 Action Plan was to create an infrastructure towards achieving the following goals:88

- Cyber security of all services, processes, and data provided by public organizations and agencies using information technologies;

- Cyber security for information systems of critical infrastructures operated by both the public and private sectors;

- Decrease the effects of cyber security incidents, determine strategic cyber security actions to restore systems to their regular operational states as soon as possible following incidents, and support investigation and prosecution of the incident by law enforcement and judicial authorities.

Furthermore, these are some principles to be considered in ensuring national cyber security:[89]

[86] *Resmi Gazete*, "Milletlerarası Sözleşme: Sanal Ortamda İşlenen Suçlar Sözleşmesi," 29083, 09.08.2014, https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5.htm (Access 15.10.2021).
[87] *Resmi Gazete*, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nın kabulü," 28683, 25.03.2013, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm (Access 15.10.2021).
[88] Ibid.
[89] Ibid.

- Cyber security must be ensured by methods based on risk management and continual improvement;

- An integrated approach must be adopted that would involve determining strong and weak sides in legal, administrative, political, economic, and social dimensions, as well as threats and opportunities beyond the technical dimension;

- Risk management must be based on strategies for removing technical vulnerabilities, avoiding attacks and threats, and reducing potential damages.

National Cyber Security Strategy (2016-2019)

The 2013 action plan was superseded by the "2016-2019 National Cyber Security Strategy and Action Plan. "[90] The new plan was prepared to be more accessible compared to the 2013-2014 Action Plan. While definitions related to the cyber concept were included in the plan's introduction, the aim, scope, vision, and missions were emphasized in other parts. Additionally, a "List of Cyber Security Board Member Institutions," "List of Regulatory and Supervisory Institutions," and "List of Sectoral CIRT" (Cyber Security Incident Response Team) were included in the plan.

The Cyber Security Council's member institutions consist mostly of ministries such as the Ministry of Transportation, Maritime Affairs, and Communication; the Ministry of Foreign Affairs; and the Ministry of Interior. Also included are regulatory and supervisory institutions such as the Banking Regulation and Supervision Agency (*Bankacılık Düzenleme ve Denetleme Kurumu,* or BDDK) and the BTK. In addition, the General Directorate of Highway Regulation (*Karayolları Genel Müdürlüğü*, or KGM) and Energy Market Regulatory Authority (*Enerji Piyasası Düzenleme Kurumu*-EPDK) figure among the sectoral-based institutions.

Procedures and Principles Regarding Connecting to the KamuNet Network and Auditing of the KamuNet Network

The 2016-19 Action Plan, which entered into force in 2017, introduced the concept of "KamuNet," defined as "a closed-circuit and public virtual network infrastructure that is more secure against physical and cyber-attacks, where service, transaction and data traffic will be transferred by isolated from the private network and internet environment via public institutions and organizations. "[91] This legislation's purpose is to determine minimum requirements for the information and communication systems connected to KamuNet and to form the procedures and principles for supervising these institutions.

[90] Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy*, pp. 1-26, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf (Access 03.09.2021).
[91] *Resmi Gazete*, "Kamunet Ağına Bağlanma ve Kamunet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ," 30103, 21.06.2017, https://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm (Access 15.10.2021).

In this context, a public institution that would be included in KamuNet meets minimum requirements and records data regarding KamuNet, establishes and operates the Information Security Management System, forms a team responsible for KamuNet, and takes measures against malicious software such as computer viruses, worms, trojan horses, and similar in order to protect the confidentiality, integrity, and accessibility of information and software within KamuNet information systems.[92]

National Cybersecurity Strategy and Action Plan (2020-2023)

Turkey's "National Cyber Security Strategy and Action Plan (2020-2023)" includes all components of cyber space at national scale, including public information systems, information systems for critical infrastructures operated by the public and private sector, small and medium-sized industry, all private and legal entities. There are 40 actions and 75 implementation steps associated with a total of 8 strategic objectives to be realized within the scope of the National Cyber Security Strategy and Action Plan.[93] The strategic objectives determined for the realization of Turkey's 2023 vision in cyber security are protecting critical infrastructures, developing national capacity, security of new generation technologies, fighting cybercrime, developing and supporting domestic and national technologies.[94]

The Law to Amend the Law on Regulation of Broadcast on the Internet and Fighting Crimes Committed Through These Publications

This law entered into force after publication in the *Official Gazette* (*Resmi Gazete*) dated July 31, 2020. In this law, social network providers are defined and "port information" is added to the definition of traffic information. Also, notification procedures for administrative fines imposed on content, location or access provider carrying out its activities abroad are determined. In addition to all these actions, the fine to be imposed on the hosting provider who does not notify for providing hosting or does not fulfil its legal obligations is increased.[95]

All these legal regulations mentioned above form the basis of current cyber space protocols in Turkey. Especially with the regulations made after 2016, the state has increased its authority in cyber space. Some of these regulations are transferring of TIB (*Presidency of Telecommunication and Communication*) into BTK *(Information and Communication Technologies Authority)*, direct government control of ISPs (*Internet Service Providers*), and facilitating social media censorship through statutory decrees.[96]

[92] Ibid.
[93] T.C. Ulaştırma ve Altyapı Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023," https://hgm.uab.gov.tr/haberler/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023-yayimlandi (Access 07.11.2021).
[94] Ibid.
[95] *Resmi Gazete*, "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun," 31202, 20.07.2020, https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm (Access 15.10.2021).
[96] Bilge Yeşil, Efe Kerem Sözeri, Emad Khazraee," Turkey's Internet Policy After the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance," *Internet Policy Observatory*, 2017, p. 4, http://repository.upenn.edu/internetpolicyobservatory/22 (Access 03.10.2021).
[97] *Sözcü*, "Türkiye'ye Karşı 102 Bin Siber Saldırı Gerçekleştirildi," 03.12.2020, https://www.sozcu.com.tr/2020/teknoloji/turkiye-karsi-102-bin-siber-saldiri-gerceklestirildi-6152249/ (Access 15.10.2021).
[98] *Yeni Şafak*, "Siber Saldırıya Yerli Kalkan: 500 Binden Fazla Saldırı Önlendi," 18.10.2021, https://www.yenisafak.com/teknoloji/siber-saldiriya-yerli-kalkan-500-binden-fazla-saldiri-onlendi-3707432 (Access 21.10.2021).
[99] NCSI, "National Cyber Security Index Global Cybersecurity Index," E-Governance Academy, 04.03.2020, https://ncsi.ega.ee/country/tr/ (Access 15.10.2021).
[100] Susan Brenner, "At Light Speed: Attribution and Response to Cybercrime, Terrorism, Warfare," *The Journal Of Criminal Law And Criminology*, 2007, p. 382. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1008542 (Access 07.11.2021).
[101] Taner Altınok and Haydar Çakmak, *Suç, Terör, Savaş Üçgeninde Siber Dünya*, Ankara, Barış Platin Yayınları, 2009, p. 29.
[102] Richard A. Clark and Robert K. Knake, *Siber Savaş*, Translated by Murat Erduran, İstanbul Kültür

Cybercrimes Statistics in Turkey in Recent Years

The number of blocked cyber-attacks targeting Turkey is increasing day by day. When we examine the development of cyber-attacks, especially in recent years, we see that there were approximately 73,000 in 2018; 150,000 in 2019; and 200,000 in 2020.[97] According to a statement made by Turkey's Minister of Transport and Infrastructure, 60,795 cyber-attacks were prevented as of October 1, 2021.[98]

Against these intensifying cyber-attacks, Turkey is increasing its cyber security practices. Turkey ranks in 11th place in the Global Cyber Security Index prepared according to National Cyber Security Index (NCSI).[99] These data show us that Turkey still has a serious process ahead. Here is a sampling of some of the cyber-attacks against Turkey by state-sponsored or terrorist organizations:

Cyber-attacks Associated with Governments

Traditionally, we can divide national security threats into internal and external threats. Crime and terrorism can be classified as internal threats, while war can be classified as an external threat. However, such a classification cannot be carried out so easily when it comes to cyber threats because there are no limits for cyber-attacks.[100]

The borders in the triangle of crime, terror, and war are blurred. This blurring of the cyber environment provides great convenience for all actors of International Relations in the implementation of threats.[101] At the same time, features of cyberspace such as obscurity and unpredictability provide opportunities for states to make their rivals accept terms without need for escalating conflict.

Here are some examples of cyber-attacks where these threats are visible:

- F-15 and F-16 warplanes of the Israeli Air Force carried out air strikes against Syria on September 6, 2007. After the cyber-attacks that took place simultaneously with this conventional attack, neither Turkish nor Syrian radars could detect those jets.[102] After the attack,

a botnet attack was carried out on the official website of the UN by Turkish hackers to protest USA and Israeli Middle East policy.[103]

- In 2007, Ukrainian hacker Maksim Yastremski gained unfair advantage through unauthorized access to information systems of 12 banks in Turkey.[104]
- After a Russian plane was shot down on November 24, 2015, cyber-attacks against Turkey started on December 14, 2015. These cyber-attacks against E-mail addresses with the extension ".tr" lasted for three days. METU, which is responsible for the management of ".tr" domain names and DNS servers, stated that the necessary intervention was carried out to halt the attacks.[105]
- In 2020, there were discussions about the continental shelf and the Eastern Mediterranean exclusive economic zone. France was also involved in that crisis between Greece and Turkey, especially with regard to ownership of energy resources. After France became involved in the issue, the French Navy arrived in the region. Radars of the French warships were locked by cyber-attacks carried out by Turkey to thwart Gallic intervention.[106]

The cases mentioned above are some of the known examples. In particular, attacks against E-mail addresses with the extension ".gov" or ".tr" occur regularly every day. All of these cyber-attacks are actually attacks against the virtual borders of the nation state.

Cyber-attacks by Terrorist Organizations Against Turkey

Traditional terrorism aims to manipulate government policies, negatively impact people on a global level, and cause physical damage to infrastructure. With the development of technology, terrorist groups have begun to adapt and benefit from cyber tools and capabilities. An orientation towards cyber terrorism has increased the use of computers and the Internet in the rate of terrorist attacks.

The term cyber terrorism includes worms, viruses, phishing activities, and various other malware and programming commands. The basis of cyber terrorism is to gain an advantage through the deliberate disruption of computer networks, inflicting serious bodily harm, theft or obfuscation by various means.

University, İKÜ Publishing, 2011, pp. 4-12.

[103] Mehmet Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, İstanbul, Beta Yayınları, 2017, p. 50

[104] *Hürriyet*, "Ukraynalı Hacker Antalya'da Yanacak," 23.08.2008, https://www.hurriyet.com.tr/gundem/ukraynali-hacker-yakalanmisti-9728016 (Access 15.10.2021).

[105] Rengin Arslan, "Türkiye'ye Siber Saldırının 10 Günü: Ne Oldu?" *BBC Türkçe*, 24.12.2015, https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan (Access 15.10.2021).

[106] *Euronews*, "Fransa: Türk Ordusu Gemimizi Taciz Etti"; Üç Kez Radar Kilidi Attı," 18.06.2020, https://tr.euronews.com/2020/06/18/fransa-turkiye-yi-nato-ya-sikayet-etti-akdeniz-de-gemimizi-radar-kilidiyle-uyard (Access 15.10.2021).

Furthermore, acts of cyber terrorism are often aimed at gaining political or ideological advantages through intimidation, fear and threat. In this context, there are various definitions of the concept.

Dorothy Denning makes the claim in *Activism, Hacktivism and Cyberterrorism* that uncertainty in definition brings uncertainty in action.[107] In other words, an e-mail bomb may be considered hacktivism by some and cyber terrorism by others. To summarize it briefly, the term cyber terrorism means the use of the Internet for terrorist purposes. In this context, here we enumerate some of the cyber-attacks carried out by hostile organizations against Turkey:

- On November 19, 2008, the Kurdistan Workers' Party (PKK) hacker who stole data from the National Intelligence Organization (MIT) and the General Staff was caught.[108]
- On November 10, 2011, the PKK attacked and hacked the Turkish Finance Ministry's website.[109]
- On July 27, 2012, the PKK hacked the accounts of Turkey's most popular companies, including Teknosa, TTNET, Garanti Bank, and Denizbank.[110]
- On November 11, 2012, the muftiate's website was hacked by the PKK.[111]
- The Ordu regional government website was hacked by the PKK on February 16, 2014.[112]
- Pictures of imprisoned PKK leader Abdullah Öcalan and the terrorist organization PKK were shared after the PKK cyber-attacked the Lig TV channel's Twitter account on August 23, 2015.[113]
- A report published in 2017 stated that a hacker group called "Dragonfly" targeted Turkey's energy infrastructure.[114]

[107] Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," RAND Corporation, 2001, pp. 239-288, http://faculty.nps.edu/dedennin/publications/ActivismHacktivismCyberterrorism-NetworksAndNetwars.pdf (Access 15.10.2021).

[108] *T24*, "Devletin Sırlarını Çalan Pkk Kuryesi Çıktı," 19.11.2008, http://t24.com.tr/haber/devletin-sirlarini-calan-pkk-kuryesi-cikti,17138 (Access 15.10.2021).

[109] Memurlar.net, "Maliye'nin Web Sitesi Hacklendi," 10.11.2011, https://www.memurlar.net/haber/209719/maliye-nin-web-sitesi-hacklendi.html (Access 15.10.2021).

[110] *Habertürk*, "Devlere Facebook'ta PKK Saldırısı!" 27.07.2012, https://www.haberturk.com/ekonomi/makro-ekonomi/haber/762468-devlere-facebookta-pkk-saldirisi (Access 15.10.2021).

[111] *Sözcü*, "PKK Müftülük'ü Hack'ledi," 11.11.2012, https://www.sozcu.com.tr/2012/gunun-icinden/pkk-muftuluku-hackledi-111761/ (Access 15.10.2021).

[112] Ordumanset, "Ordu Valiliği Sitesine Pkk Saldırısı," 16.02.2014, http://www.ordumanset.net/m-haber-4017.html (Access 15.10.2021).

[113] *Haberler.com*, "Lig TV, Twitter Hesabı Hacklendi!" 23.08.2015, https://www.haberler.com/lig-tv-twitter-hesabi-hacklendi-7621613-haberi/ (Access 15.10.2021).

[114] Alper Başaran, *Yaklaşan Felaketin Habercileri Siber Kıyamet*, İstanbul, Arion Yayınevi, 2017, p. 21.

- On August 16, 2018, due to the anniversary of the PKK's first offensive (15 August 1984--Eruh Raid), the PKK hacker unit seized a public hotline and sent SMS to citizens' mobile phones with the declaration: "Down with Fascism, Long live August 15 spirit, Long live leader APO, Long live PKK. "[115]
- Cyber-attacks against Turkey's banking system were carried out in 2019. Garanti BBVA was most affected by this cyberattack using the Distributed Denial of Service (DDoS) technique.[116]
- On September 22, 2020, DDoS attacks were carried out against the Education Information Network (EBA) of the Ministry of National Education (MEB). [117]

As can be seen above, when we consider attacks carried out by terrorist organizations in Turkey so far, the visible side of the attacks is hacking the websites of several official institutions, taking them out of service for a few hours or days, or disclosing certain information. In addition, it has been proven in many reports that organizations such as IBDA-C, DHKP-C, and especially PKK are among the terrorist organizations operating in the cyber environment against Turkey.[118]

Conclusion and Suggestions

Our goal in this chapter has been to analyze Turkey's cyber security policies by explaining key concepts, the changing security perspective after the Cold War, Turkey's related institutions and legislations, and some crime statistics and information about cyber-attacks against Turkey. Overall, Turkey did its homework to establish institutions and create necessary legislation for securing cyber space on behalf of citizens. However, there is still a long way ahead. Technological progress continues, and malicious actors can take advantage of those advances to as much or greater effect than can states and well-intentioned people.

There are some institutions and organizations that are authorized in Turkey's struggle against cybercrimes. While the BTK is the leading authority, the Cyber Security Council that belongs to the Ministry of Transport and Infrastructure, the General Directorate of Security-Combating Cybercrimes Department, the Turkish Armed Forces, TSK Cyber Defense Command, and The Scientific and

[115] *Mynet*, "Telefonlarına Gelen Mesajı Görenler Şoke Oldu! PKK'dan Toplu SMS," 16.08.2018, https://www.mynet.com/telefonlarina-gelen-mseaji-gorenler-soke-oldu-pkk-dan-toplu-sms-110104335942 (Access 15.10.2021).
[116] Necdet Çalışkan, "Türkiye Ddos Saldırısı Altında! Garanti ve Türk Telekom'dan Açıklama Geldi," *Habertürk,* 28.10.2019, https://www.haberturk.com/son-dakika-garanti-ve-turk-telekom-na-siber-saldiri-aciklamamasi-haberler-2535014-teknoloji (Access 15.10.2021).
[117] *DW Türkçe,* "MEB: EBA'daki Sorun Siber Saldırı ve Yoğunluk Kaynaklı," 23.09.2020 (Access 15.10.2021).
[118] Gabriel Weiman, "How Modern Terrorism Uses The Internet," United States Institute of Peace, March Special Report, Washington, 2004, pp. 1-12, https://www.usip.org/sites/default/files/sr116.pdf (Access 15.10.2021).

Technological Research Council of Turkey are other prominent actors responsible for combating cybercrime, developing cyber security technologies and preparing security plans. Therefore, we can assert that the Republic of Turkey aims to develop cyber security policies by activating multiple institutions.

With the acceleration of digitalization in the 2000s, there has been an increase in cyber-attacks against Turkey. This increase necessitated legal and institutional regulations. In this context, the previously published National Cyber Security Strategy, 2013-2014 Action Plan and 2016-2019 National Cyber Security Strategies have all contributed to the way Turkey navigates cyberspace. Turkey determined its National Cyber Security Strategy and Action Plan on December 29, 2020, which covers the new period between 2020 and 2023. Thus, Turkey has taken a pro-active role to ensure its cyber security. Despite coordinated policy among key institutions, Turkey is struggling to emerge as an effective player in the domain of cyber security. However, to be able to reduce these attacks, the country might also try to establish more peaceful relations with its neighbors and other states, as well as neutralize the threat of militant domestic groups by implementing fresh strategies to solve the problem.