ARTICLE

Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice

NEZİR AKYEŞİLMEN

Selçuk University, Türkiye
ORCID No: 0000-0001-8184-5280

ABSTRACT *The threat of malicious actors is a growing fear among all cyberspace stakeholders, particularly states, who are primarily responsible for national security, including the protection of critical infrastructure. Taking into consideration the major cyberattacks of the last three decades and their impacts on international society, a comprehensive strategy is needed to defend cyberspace against malware and to provide a safe and free cyber ecosystem. Türkiye, like many countries, has developed cyber strategies to respond to such threats in the last decade. This paper addresses a set of interrelated cybersecurity issues; central among them is the question, "Is Türkiye's cybersecurity strategy properly devised to cope with the new security environment in the anarchic world of cyberspace?" Türkiye's national cybersecurity strategy has undergone several changes since 2013, each representing an attempt to address the evolving cybersecurity landscape. These strategies have been successful in some areas, such as Türkiye's legal, capacity-building, and organizational structure, but have been less successful in terms of technical measures. This article applies a macro-analysis framework that encompasses both quantitative and qualitative research to analyze Türkiye's cybersecurity strategies in theory and practice. The findings of this analysis suggest that Türkiye is still vulnerable to a possible major cyber-attack.*

Keywords: Technology, Cyber-attacks, Cybersecurity, Türkiye, Cooperation

Insight Turkey 2022
Vol. 24 / No. 3 / pp. 109-134

Received Date: 27/5/2022 • **Accepted Date:** 14/9/2022 • **DOI:** 10.25253/99.2022243.8

Introduction

Today, we are becoming ever more dependent on cyber technology. More than five billion people are connected to the internet, and every day, more than 10 billion gigabytes (GB) of information is produced online.[1] The number of active devices connected to the internet is expected to exceed 24 billion by 2030.[2] Business transactions, trade, finance, entertainment, communication, politics, security, and many more processes are becoming increasingly digitized.

Digitalization has brought new advantages and comfort to our lives, yet it also has led to new risks and threats. Every day, more than 250,000 web pages are hacked.[3] According to Checkpoint –a cybersecurity solutions provider to governments and private companies globally– on average, 70 million cyber-attacks take place each day.[4] The cybercrime market reached $6 trillion worldwide in 2021.[5] New technologies such as cloud computing, blockchain, big data, mobile technology, the Internet of Things (IoTs or IoE), and now the metaverse are increasing our dependency on the digital domain and complicating the landscape of cyber threats. In a recent article on 'cyber anarchy,' Joseph Nye remarks: "The world has experienced cyberattacks since the 1980s, but the attack surface has expanded dramatically; it now includes everything from industrial control systems to automobiles to personal digital assistants."[6] The 'Morris worm' of 1987, mafia boy's attacks on transnational companies in 2000, the distributed denial-of-service (DDoS) attacks on Estonia in 2007, Stuxnet's strike against Iranian nuclear facilities in 2010, Wikileaks disclosures in 2011, and alleged Russian interference in the U.S. presidential elections of 2016 indicate the steadily increasing intensity of cyber incidents in international politics.

The fact that concepts such as cyber-attacks, cyber-crimes, cyber conflicts, and even cyber warfare have become a part of our daily conversations in recent years shows that the hyper-anarchic world of cyberspace is increasingly becoming a threatening place. As Nye puts it, "The relentless bad news stories paint a picture of an ungoverned online world that is growing more dangerous by the day– with grim implications not just for cyberspace itself but also for economies, geopolitics, democratic societies, and basic questions of war and peace."[7] All these destructive processes have forced cyberspace stakeholders, especially states, to take precautions to ensure cybersecurity; indeed, in the last decade, cybersecurity has become one of the top issues on national and international security agendas worldwide.

This paper explores Türkiye's national cybersecurity strategy documents, policies, strategies, measures, and organizational structures. The primary research question it seeks to answer is: Is Türkiye's cybersecurity strategy

properly devised to cope with the new security environment in the hyper-anarchic world of cyberspace?

Research on Türkiye's national cybersecurity strategies has focused primarily on the country's military and offensive capabilities with a 'negative' security approach

In the last decade, research on Türkiye's national cybersecurity strategies has focused primarily on the country's military and offensive capabilities with a 'negative' security approach, i.e., a focus on Türkiye's capacity to deter or prevent cyberattacks by establishing cybersecurity. The present paper aims to analyze Türkiye's national cybersecurity strategy with a holistic approach that encompasses all necessary policies, strategies, measures, and processes from a legal, technical, organizational, and capacity-building perspective that considers cooperation among stakeholders from a positive security understanding, i.e., one that not only focuses on preventing cyber-incidents but also on efforts to maintain freedoms in cyberspace. The purpose of this research is to reveal the weaknesses and strengths of Türkiye's national cybersecurity strategy and to develop policy proposals and recommendations to improve it.

Research Methodology and Research Questions

This study applies both quantitative and qualitative research methods. The analysis and outcomes of the study will be based on primary and secondary sources including national cybersecurity strategy documents, legal and administrative regulations, and the literature. Macro Analysis will be applied in the evaluation of Türkiye's NCSSs and policies that will cover the followings:

i. Consistency among all national cyber strategy plans, documents, regulations, laws, and directives.
ii. Türkiye's capacity to protect its cyberspace and critical infrastructure.
iii. Literature on the effectiveness of national cyber strategies in cyberspace.
iv. The possibilities of cooperation on cybersecurity issues.
v. Power is dedicated to different cybersecurity institutions.
vi. Policy proposals and legal regulations.

The research questions are designed to assess whether Türkiye's cybersecurity strategy and architecture is responsive to current challenges and threats. Does Türkiye have the proper/adequate national and international tools, regulations, standards, and policies to counter today's cyber threats? How could Türkiye's current security regimes, policies, and institutions be transformed to ensure cybersecurity?

Literature Review

If this paper had been written 10 years ago, we would start with the challenges posed by the scarcity of literature available on the subject. The main advantage of analyzing the proposed research questions today is that not only is there an abundance of information, but the overwhelming majority of the relevant literature is available online and is easily accessible through digital media, academic journals, and corporate and government webpages. The challenge today lies not in the scarcity of literature, but in deciding what is credible in the abundant literature.[8] The research available on the topic at hand may be classified into three sections: Defining cybersecurity, the evolution of cybersecurity in International Relations (IR), and the architecture of Türkiye's cybersecurity structure and strategies. An exploration of these areas within the literature is provided below to contextualize the work of the present study.

Cyber(in)security: The Most Controversial Concept of Cyberspace

Cyberspace –the space in which cybersecurity is enacted– is itself a contested term. It has no widely accepted definition in contemporary literature. Different approaches have been developed by various experts, institutions, and disciplines for understanding this term, which in broad strokes refers to a highly complex, global domain. The concept of cyberspace was first introduced by William Gibson in his famous science fiction novel *Neuromancer* in 1984. Gibson describes cyberspace as a complex global network of computers co-created/shared by billions of users from all around the world.[9] Since then, several definitions that expand upon Gibson's initial concept have been proposed. One study claims to have found 28 different definitions of cyberspace in the previous decade. Each definition prioritizes one dimension of cyberspace, such as hardware, software, protocols, network, information, the user, interconnectedness, the internet, etc. Each study puts forward a working definition that serves or carries out the interests of its developer. Based on the plethora of definitions, Kramer claims that "definitions should be used as an aid to policy and analysis and not as a limitation of them."[10] It exceeds the scope of this paper to analyze all of the definitions developed in other studies; instead, it will elaborate on a few of the most useful and move on to discussions of cybersecurity.

Defining Cyberspace: Is It a Space?

What does the concept of cyberspace bring up first in your mind? Is cyberspace a place, a region, or a space? Is it possible to design it, present its map or represent it physically? Is it even possible to define it? "For some geographers, cyberspace is a dynamic discourse which (re)embodies social reality by giving a meaning to structures and social processes and an identity to users, despite the absence of tangible borders."[11] Many people perceive cyberspace as a vir-

tual domain, and this is not wrong. However, in addition to its virtual dimension, cyberspace requires physical infrastructure –a physical, global network that is made up of computers, wires, satellites, servers, modems, etc.– all of which make the virtual network possible, and all of which are necessarily located somewhere on earth. This complex structure supports and defines the protocols that users accept as components of this world. Eric Schmidt, CEO of *Google*, notes the complexity of the cyber world by claiming, "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."[12] Various experts and notable institutions have attempted to figure out and map the different dimensions of the cyber world and make it understandable for everyone –with varying levels of success.

Highly complex and globally interconnected, cyberspace is a multidimensional domain with numerous layers and unique features in which ever more complicated processes and operations take place within the cyber-ecosystem

Kuehler puts forward a definition that encompasses hardware, software, and information layers. In his words, cyberspace is "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."[13] The European Union Agency for Cybersecurity (ENISA, formerly known as the EU Agency for Network and Information Security), has developed a similar but shorter definition of cyberspace: Cyberspace is the time-dependent set of tangible and intangible assets, that store and/or transfer electronic information."[14] For NATO, "Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks."[15]

Türkiye has introduced three different but closely interrelated definitions of cyberspace in its national cybersecurity strategy documents published in the last 10 years. Türkiye's National Cybersecurity Strategy Document (NCSD) and 2013-2016 Action Plan define cyberspace as, "The environment which consists of information systems that span across the world including the networks that interconnect these systems."[16] The country's NCSD 2016-2019 adds some new elements, describing the domain as, "The numeric environment composed of information systems spread over the entire world and space, the networks interconnecting these systems or independent information systems."[17] The most recent NCSD and Action Plan of 2020-2023 defines cyberspace as, "systems and services connected either directly or indirectly to the internet, telecom-

In cyberspace, the offense is always a step ahead of the defense

munications and computer networks."[18] The definition contained in the 2016-2019 strategy plans seems to be more comprehensive and accurate compared to the others. Since cyber technology is constantly evolving and changing, naturally, the elements of the definitions will also change over time.

Highly complex and globally interconnected, cyberspace is a multidimensional domain with numerous layers and unique features in which ever more complicated processes and operations take place within the cyber-ecosystem. To fully understand cybersecurity, each characteristic of cyberspace needs to be evaluated. First of all, unlike physical space, cyberspace is a fabricated domain. Moreover, human beings are active actors both within and in cyberspace; they contribute to the expansion of cyberspace every moment. Usaf remarks, "cyberspace is constructed by man [sic] and constantly under construction. It changes from moment to moment."[19]

The second basic feature of cyberspace is its anarchic structure. It is a decentralized, polycentric space. It is not only anarchic in the sense of physical international relations, but it also lacks governing institutions such as international law, international organizations, diplomacy, great powers, etc. For this reason, Choucri describes the cyber domain as hyper-anarchic. Cyber features make possible a world of high conflict and violence worldwide in the absence of sovereign control or any centralized authority. We refer to this feature as one of *cyber anarchy.*[20] In other words, "Cyberspace is devoid of governance systems, there are no regulatory norms or practices, and there are no mechanisms for tracking "damages" –and little incentives to do so."[21] Another characteristic feature of cyberspace is the dominance of private actors; as Choucri notes, "the state system is weak, and the private sector (for-profit, not-for-profit, legal, and illegal) dominates."[22] Nye concisely explains most of these characteristics: "Among the special characteristics of the new cyber-domain are the erosion of distance (oceans no longer provide protection), the speed of interaction (much faster than rockets in space), the low cost (which reduces barriers to entry), and the difficulty of attribution (which promotes deniability and slows responses)."[23] A such, cyberspace is widely accepted as the fifth operational domain[24] "in addition to the traditional four of land, sea, air, and space."[25]

Cybersecurity: Whose Security?

Commenting on the worried look of a cheetah waiting with its young cubs at a lion 30 meters away in a documentary broadcast on Animal Planet TV, the presenter said, 'No baby is safe in the savannah, since no one here can be sure

> of its neighbor's true intentions.' The same is valid indeed, for cyberspace. Because... it eliminated distances and made everybody neighbors to everybody. Therefore, referring to the documentary, 'no user is safe in cyberspace. Because in this domain, nobody is even sure who his neighbor is, let alone the intention of the neighbor.[26]

The quotation above perfectly explains the vulnerability of the security situation in cyberspace. Threats are always in place, and they are real and imminent. Therefore, Claude Shannon cautions, "assume that the enemy knows the system, and treat every host, server, and connection as potentially hostile."[27] This approach is known as "zero trust" in the cybersecurity community.[28]

Various definitions of cybersecurity have been developed for different national cybersecurity strategy documents, by various international organizations and experts. Cyberspace and its related terms, such as cybersecurity, cyber ethics, cyber politics, cyber conflict, and cyber warfare, are highly controversial, uncertain, and vague concepts. Cybersecurity is an even more contested and complicated term than cyberspace and is similarly hard to define. Indeed, it means different things to different actors, including states, international organizations, private companies, and even users. Craigen *et al*. claim:

> Cybersecurity is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative… The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges.[29]

For practical use, the International Telecommunication Union (ITU) has developed a comprehensive and self-explanatory definition for cybersecurity that encompasses almost every aspect of cybersecurity: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."[30] The ITU's definition is one of the most commonly found in the literature. The ITU also describes exactly the assets that cybersecurity protects:

> Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[31]

> In all three of its NCSDs, Türkiye uses a very similar, broad definition of cybersecurity: "Protection of information systems forming cyberspace from attacks, assuring confidentiality, integrity, and availability of information/data processed in this environment, detection of attacks and cybersecurity incidents, activation of counter-response mechanisms, and recovering systems to conditions prior to the cybersecurity incident."[32]

This NCSDs definition focuses not only on the protection of systems from cyber-incidents; it also stresses the three main objectives of cybersecurity, known as the confidentiality-integrity-availability (CIA) triad: "Availability, Integrity, which may include authenticity and non-repudiation and Confidentiality."[33]

The definition proposed by Michael Veale and Ian Brown is very similar to Türkiye's, focusing on the protection of information systems and countermeasures against cyber-attacks:

> Cybersecurity covers the broad range of technical, organizational, and governance issues that must be considered to protect networked information systems against accidental and deliberate threats. It goes well beyond the details of encryption, firewalls, anti-virus software, and similar technical security tools.[34]

Veale and Brown rightly point out that "Understanding cybersecurity is a moving target, just like understanding computing and society. Exactly what is being threatened, how, and by whom are all in flux."[35] Therefore, definitions change from person to person, from study to study, and from time to time.

Despite changes in definitions and different approaches developed by different actors in cyberspace, however, all definitions include the elements of fighting against harmful actions, preventing cyber-attacks, and enabling system recovery. These definitions generally correspond with a negative security understanding. There are rare references to freedom and human rights in cybersecurity definitions and/or strategies.

The Emergence of Cybersecurity in IR

The evolution of cybersecurity in IR focuses on the major cyber-attacks and cyber conflicts that have shaped the emergence of cybersecurity at the national and international levels.[36] Cyberspace was developed for sharing information, and transparency was its primary characteristic for almost 20 years, from 1969 to 1988, when the Morris worm –the first harmful malware– was created and released to the network.[37] In other words, the first two decades of the internet

were free from malware and thus it was considered free and safe. The notion of cybersecurity itself first started with the Morris worm. And although cyberspace, which is a product of the Cold War, was set up primarily to contribute to physical security, over time, it generated a new security concern: Cybersecurity.[38]

Global cybersecurity has been an agenda item for states in the last 10 years in international relations

In cyberspace, the offense is always a step ahead of the defense: "the offense has the upper hand. The Internet was designed to be collaborative and rapidly expandable and to have low barriers to technological innovation; security and identity management were lower priorities."[39] Along with the expanding need for cybersecurity, its mechanisms developed gradually from the individual level to the national and global level from the late 1980s to the present. Several major cyber-attacks and cyber conflicts shaped this process in international relations.

From Morris Worm to Mafia Boy (1988 to 2000)

A turning point occurred in the history of cybersecurity on November 2, 1988. Academics at leading U.S. universities declared that all their computers had either slowed down or stopped working and they faced difficulty in accessing information. It is claimed that more than 10 percent of computers in the U.S. (approximately 6,000-60,000) lost their functionality.[40] This malware attack was named for its developer, Robert Tappan Morris,[41] a graduate student at Cornell University.

Being the first of its kind, the Morris worm,[42] had a deep impact on computer and internet security. In its wake, various Computer Emergency Response Teams were created and people started to be more careful and thoughtful about security in cyberspace. "Some people even term the episode as the big bang of cybersecurity."[43] The worm was a wake-up call regarding computer and internet security for administrators, professionals, and users.[44] "Soon after the Morris worm incident, the U.S.' Defense Advanced Research Projects Agency (DARPA) provided funding for the Computer Emergency Response Team (CERT), which has since served as a clearinghouse for security-vulnerability information. Although CERT provides no panacea, it has become a trusted source of information about security flaws and fixes for a variety of software."[45]

The Morris worm led to the emergence of cybersecurity at the individual level in the 1990s and shaped the perception of security as a necessity in cyberspace. Thus, cybersecurity became viewed more widely in terms of personal

computer/internet security at that time and was limited to the protection of personal data/information or at most that of small communities around the world. Within a short time of the Morris worm, a large number of viruses/worms and other malicious software of different types and with different effects were developed. Thus, as a result of DDoS attacks on some global companies by a 15-year-old Mafia Boy, the landscape of cybersecurity changed dramatically with the beginning of the 21st century.

From Individual to Institutional: Cybersecurity in the 2000s

Michael 'Mafia Boy' Calce was just 15 years old when he managed to shut down several major websites of global companies, including Dell, Amazon, *Yahoo!*, *CNN*, E-Tarde, Buy.com, and eBay, in a series of denial-of-service (DoS) attacks in 2000.[46] "At the time, *Yahoo* was the biggest search engine in the world."[47] The monetary amount of damage caused by the Mafia boy's attack is estimated at roughly between $1-3 billion.[48] This attack transformed the course of cybersecurity from individual to institutional, organizational, and network levels. Private companies started to be more cautious about the security of their assets in the cyber domain. The massive elaboration and publication of the incident in the media helped disseminate fear about the notion of cybersecurity worldwide. This trend continued throughout the first decade of the 21st century. And yet again, the offense took charge: the DDoS attacks on Estonia (2007) and Stuxnet (2010) on Iran's nuclear facility entirely changed the landscape and perception of cybersecurity.

Cybersecurity as a Component of National and International Security

Until the 2010s, states –newcomers in cyberspace– largely considered the cyber realm a matter of low politics, along with trade, entertainment, the environment, etc. In other words, cyberspace was perceived by states in general among the secondary issues that are not related to security, strategy, and military issues. As Chocuri notes, "By contrast, high politics is about national security, core institutions, and decision systems that are critical to the state, its interests, and its underlying values. We now see cyberspace shaping the domain of high politics, and high politics shaping the future of cyberspace."[49]

Since the DDoS attacks against Estonia in 2007, Israel's control of the Syrian radar system (2007 and 2011), Russia's use of cyberattacks alongside physical attacks in Georgia in 2008 (now known as hybrid war), and finally, in 2010, Stuxnet, a malicious computer worm –accepted as the first cyber weapon– deployed against Iran's nuclear facilities, states began to perceive cybersecurity as a national security problem.[50] Wikileaks (2011), the Snowden Case (2013), and the Russian intervention in the 2016 U.S. presidential elections are among the

major incidents that prompted policymakers to consider cyberspace a realm of conflict, security, and war. In 2009, then-President Barack Obama announced a new U.S. strategy to address the threat posed/by cyberspace, stating, "It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation."[51] Other leaders also warned society about ongoing cyber threats. Mike Mullen, Chairman of the Joint Chiefs of Staff, claimed in 2011, "The single biggest existential threat out there, I think, is cyber." The following year, Martin Dempsey noted that "a cyberattack could stop our society in its tracks." Former Defense Secretary Leon Panetta sternly warned in 2012 of an impending "digital Pearl Harbor,"[52] and proclaimed in 2013 that cyber was "without question, the battlefield for the future."[53] States began to perceive the cyber domain as vital for national and international security and to develop tools and policies to protect the nation and its assets from cyber threats.

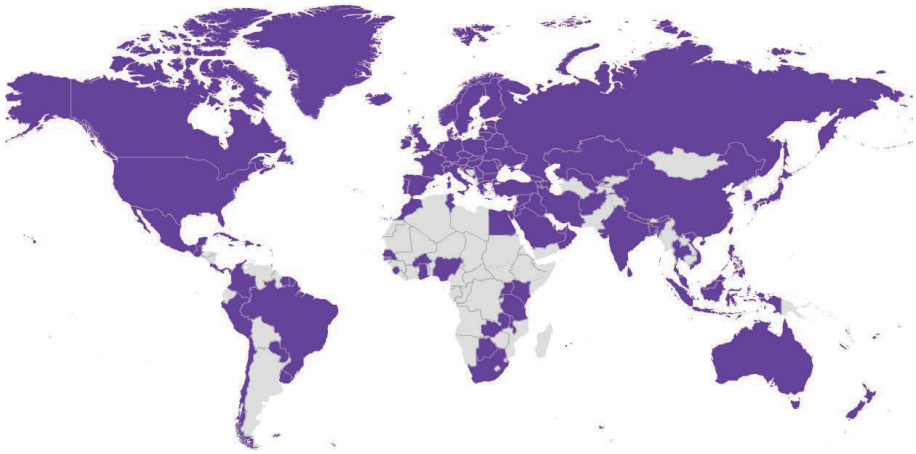
Although its legal regulations are comprehensive from a negative security standpoint, its legal apparatus seems weak in terms of envisaging rights and freedoms online

Development of National Cyber Security Strategies

After the 2007 DDoS attacks on Estonia and the Stuxnet attack of 2010, efforts to establish national and international cybersecurity measures emerged in earnest. International organizations such as the ITU, NATO, the OECD, and ENISA started to develop cybersecurity programs and guides to help their members ensure cybersecurity. The ITU stated that the objective of its cybersecurity program is to make cyberspace safer for everyone. It offers its members "opportunity and tools to increase cybersecurity capabilities at the national level, in order to enhance security and resilience, build confidence and trust in the use of ICTs– making the digital realm more safe and secure for everyone."[54] States began developing National Cyber Security Strategies (NCSS), a set of policies, tools, and applications that governments apply to make national cyberspace freer and safer. According to the ITU, an NCSS "outlines a framework for organizing and prioritizing efforts to manage risks to our cyberspace or critical information infrastructure."[55] NATO draws a more comprehensive framework: "A national cybersecurity strategy should enable government entities to identify strategic objectives, translate this vision into coherent and implementable policies, pinpoint the resources necessary for achieving such objectives and provide guidance for the use of these resources and distinguish how the NCSS is linked to other related strategies."[56]

Most governments started to develop their NCSS documents over the past decade. Today, only a few countries have no NCSS. Figure 1 illustrates the prevalence of NCSSs worldwide.

Map 1: Global Map of NCSS



Source: *National Cybersecurity Strategies Repository*[57]

Türkiye developed its first NCSS document in 2013 and has produced three to date. The NCSS currently in effect covers the years 2020-2023.[58] The following section analyzes these documents.

Global Cybersecurity and Cyber Power Outlook: Where Does Türkiye Stand?

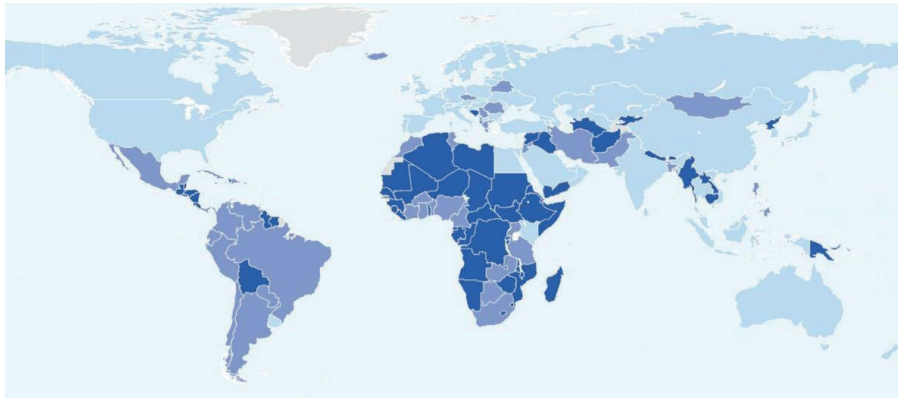
Türkiye's cybersecurity strategies will be discussed in this section after a global outlook has been presented. Discussions will be based on a macro-analysis of the five pillars used by the ITU in its Global Cybersecurity Index (GCI).[59] Each pillar has several indicators; Türkiye's strategy for addressing each pillar and its implementation of this strategy in practice will be evaluated based on these indicators.

Global cybersecurity has been an agenda item for states in the last 10 years in international relations. States initially struggled to establish cybersecurity, but they also started to increase their power in the cyber domain through different means and strategies. Cyber power is assessed based on both the offense and defense capability of states in cyberspace.

The ITU has been publishing its GCI since 2015 and has produced four so far (in 2015, 2017, 2018, and 2020). The GCI is not a cybersecurity index per se, but a cybersecurity 'commitment' index due to the methodology of data obtained from its 193 member states. It is based on a questionnaire consisting of 150 questions; in recent indexes, the ITU has also started to obtain data from open sources. The GCI measures member states' cyberse-

curity commitments across five pillars: legal measures; technical measures; organizational measures; capacity development measures; and cooperation measures.[60]

Map 2: Heat Map of National Cybersecurity Commitment



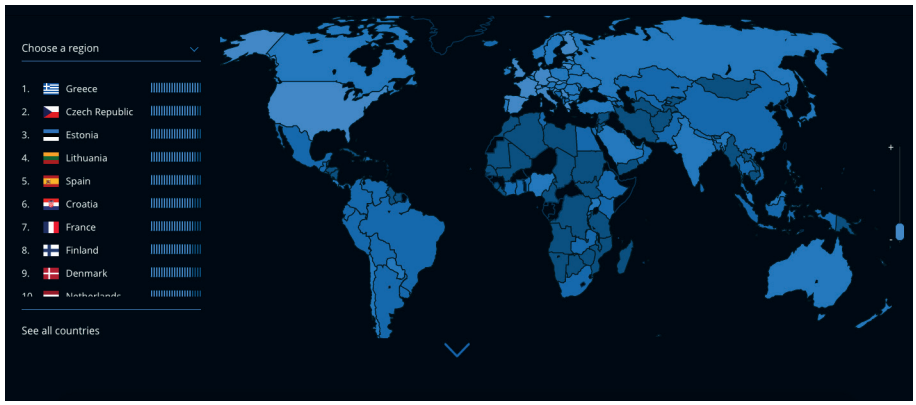
Source: *Global Cybersecurity Index 2018*[61]

Türkiye is currently ranked number 11 with a score of 97.49.[62] Its cybersecurity performance has increased, rising from 43rd place in 2017 to 11th place in 2020.

It should be stressed that the GCI measures commitment to cybersecurity, not cybersecurity itself. Its high score merely indicates that Türkiye is strongly committed to cybersecurity. Commitment is a positive sign for cybersecurity, but the real determinant is action. Data from the National Cyber Security Index (NCSI) and National Cyber Power Index (NCPI), presented below, will illustrate whether this commitment is reflected in action or not.

The NCSI is prepared by the E-governance Academy (an Estonia-based consultant company for digital transformation) and measures governments' cybersecurity capabilities. It is based on 12 indicators, including cybersecurity policy development, cyber threat analysis and information, cyber incident response, digital services protection, and military cyber operations.[63] The NCSI measures a country's "level of cyber security and identifies the main fields of priority that need to be tackled in order to improve the status of cyber security. The index also provides an overview of countries' preparedness to prevent and fight cyber-attacks and crimes."[64] According to its assessment, the top ten countries best prepared to defend against cyber-attacks are Greece (96.10), Lithuania (93.51), Belgium (93.51), the Czech Republic (92.21), Estonia (90.91), Germany (90.91), Portugal (89.61), Spain (88.31), Poland (87.01) and Finland (85.71). Türkiye is ranked 57th in the NCSI with a score of 54.55.[65]

Map 3: Cybersecurity Capability of the States



Source: *E-governance Academy*[66]

NCPI[67] on the other hand measures the cyber capability of 30 countries based on seven national objectives that countries pursue using cyber means. These are:

i. Surveilling and monitoring domestic groups;
ii. Strengthening and enhancing national cyber defenses;
iii. Controlling and manipulating the information environment;
iv. Foreign intelligence collection for national security;
v. Commercial gain or enhancing domestic industry growth;
vi. Destroying or disabling an adversary's infrastructure and capabilities;
vii. Defining international cyber norms and technical standards.[68]

Based on these objectives, the NCPI specifically measures countries' intent and capabilities for surveillance, defense, control, intelligence, commerce, offense, and norms.[69] According to the NCPI, to become a cyber power, countries require: "Capabilities to achieve their intended objectives. Cyber capabilities relate to the creation, control, and communication of electronic and computer-based information infrastructure, networks, software, and human skills. Therefore, countries invest in a wide range of resources including areas such as military cyber capabilities, cyber defense, and surveillance, as well as human capacity, institutional strengthening, and domestic policy."[70]

The top ten most comprehensive countries with the highest level of intent and capabilities across these seven objectives in 2022 are the U.S. (43), China (34), Russia (23), the United Kingdom (19), Australia (18), the Netherlands (17), Vietnam (16), ROK (16), France (15), Iran (14). Türkiye is ranked 2^{3rd} among 30 countries with a score of 9.[71] Türkiye's ranking in each sub-section is surveillance (9th), defense (15th), information control (17th), intelligence (22nd), commerce (24th), offense (25th), and norms (24th).[72] Compare to the 2020 in-

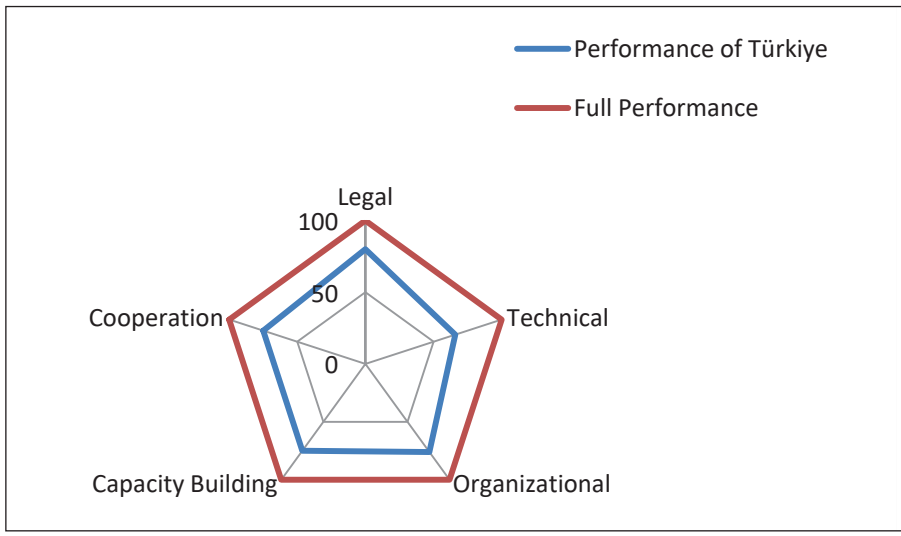
dex capabilities of Türkiye have increased in surveillance, defense, information control, intelligence, and commerce while decreased in offense and norms.[73]

Türkiye's performance has shown a steady increase in both ITU's GCI and Belfer Center's NCPI, yet has remained unchanged in E-Governance Academy's NCSI index in the last several years. Below, the relevant data of each index has been analyzed over the five pillars of GCI which tries to get an overall view of Türkiye's cybersecurity performance.

Türkiye's Cybersecurity Landscape

The literature on Türkiye's cybersecurity covers an analysis of existing legal and administrative regulations that shape the country's policy and strategy documents. Türkiye's overall performance in cybersecurity, as shown in Figure 1, is around 75/100. That is a level of good performance, albeit not perfect. As discussed in greater detail below, Türkiye needs to improve some of the indicators in all five pillars. The weakest link seems to be the technical pillar, while the strongest performance is shown in legal measures. The other three pillars fall in between, but they also need to be developed to improve Türkiye's national cybersecurity.

Figure 1: Cybersecurity Capacity of Türkiye



Source: *Developed by the author based on inferences from the five pillars developed by the ITU*

This article will next analyze the strengths and weaknesses of Türkiye's cybersecurity strategy based on the five pillars of the ITU's GCI: legal measures, technical measures, organizational structure, capacity building, and cooper-

Capacity building is about raising awareness, providing training, education, incentives, and campaigns for developing a cybersecurity culture among all internet users or digital citizens

ation. ITU's GCI pillars have been preferred for analysis since they are comprehensive enough and proper tools to measure the cyber capacity of an actor. Türkiye's position in the world has been underlined in the previous section. After a structured evaluation of Türkiye's strategies, its opportunities, and the threats it faces will be addressed.

Legal Regulations

The cost of cybercrimes worldwide is estimated to have exploded from $1 billion[74] in 2020 to as high as $6 billion in 2021.[75] Cyberspace is an attractive domain and a hub for criminals because committing a crime in cyberspace is cheap, lucrative, and low-risk. In order to provide a free and safe cyber area, the law is an effective instrument. Therefore, governments need to regulate this domain via legal processes. Legal measures authorize governments "to set up basic response mechanisms through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law."[76] Regulations include identifying "illicit activities in cyberspace, together with the definition of the necessary procedural tools to investigate, prosecute and enforce such legislation; the establishment of cybersecurity baselines and compliance mechanisms for a set of national stakeholders; and procedures to ensure consistency with international obligations."[77] For an effective legal framework, stakeholder cooperation, particularly at the international level, is needed. So far, little progress has been made at that level due to disagreements between nation-states about regulations in cyberspace. The realm of cyber law is thus limited to national regulations, which are less effective than cooperation in regulating a global network.

Türkiye began to develop cyber law regulations in the early 1990s. Its most comprehensive regulation on national cybersecurity initiatives is Cabinet Decision No. 2012/3842 issued in June 2012. The Turkish government has also issued stand-alone regulations, such as the Electronic Communication Law (No. 5809), the Electronic Signature Law (No. 5070), the Law on Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications (No. 5651), the Law on Regulation of E-Trade (No.6563) and the Personal Data Protection Law (No. 6698). Changes to existing legislation have also been made to address cyberspace, including the Turkish Criminal Code (No. 5237) and Turkish Trade Law (No. 6102).[78]

Türkiye has enacted comprehensive legislation to address legal regulations in cyberspace. Yet the purpose of legal measures is not only to issue regulations

but also to implement and enforce them. According to international monitoring frameworks, Türkiye has been performing well in the legal dimension. According to the GCI 2020, Türkiye has performed perfectly in terms of its legal endeavors and scores 20 points out of 20.[79] However, Türkiye's score on the NCSI 2020 is roughly 80 points out of 100.[80] The NCPI's surveillance and commerce sections cover legal regulations; Türkiye's average score on this index is around 60 out of 100.[81] i.e. (100+80+60)/3=80. Thus, Türkiye's overall legal performance based on the assessment of these three sources is about 80/100.

Türkiye seems to be quite successful in the protection of personal data and the fight against cybercrime but relatively is weak in cyber incident response, cyber threat analysis, and cyber crisis management.[82] Although its legal regulations are comprehensive from a negative security standpoint, its legal apparatus seems weak in terms of envisaging rights and freedoms online.

Technical Measures

This pillar covers technical infrastructure for combating technical cyber risks and incidents, including CERTs, certification, technical mechanisms, capabilities deployed to address spam, and child online protection. As the GCI underlines, "Without suitable technical skills to detect and respond to cyber-attacks, countries remain vulnerable."[83] The development of national software and hardware is vital for cybersecurity since cybersecurity is consumed not only by bad hackers but also by nation-states and IT companies. i.e., all stakeholders in cyberspace pose a threat and conduct cyber-attacks. Thus, national cybersecurity and technical products play a primary role in national cybersecurity.

Türkiye has developed its own CERTs,[84] certification frameworks, and child online protection[85] legislation and mechanisms. CERTs or Computer Incident Response Teams (CIRTs) "are responsible for taking measures to ensure information security of a specific sector or a particular institution; protecting a specific sector or institution against cyberattacks; taking measures to lower the damage in case of an attack; reacting against possible attacks; ensuring information flow with different partners, and ensuring 24/7 preparedness and availability."[86]

Türkiye's technical performance is relatively weaker compared to its legal performance. The GCI 2020 ranks Türkiye at 19.54/20 (~98), while the NCSI 2020 places the country at 50/100 in the effectiveness of its CIRT, cyber safety and security (50/100), and cyber threats analysis unit (20/100). Thus Türkiye's NCSI score for technical capability is 120/3 = 40/100. Its NCPI 2020 defense score is 30, while the highest state has 50 points (for the sake of simplification both numbers 30/50 were doubled to get the same level as other indices); hence, it can be extrapolated that Türkiye's overall performance is 66/100.

Organizational Measures

Organizations and administrative regulations include the NCSS documents that govern and coordinate national cybersecurity activity/initiatives. Organizational measures, therefore, measure the national strategies and organizations implementing cybersecurity. The lack of proper organizational set-up can lead to ineffective coordination and result in insecurity. This pillar requires comprehensive aims and objectives established by the government, along with an all-inclusive plan for implementation, delivery, and measurement. National agencies must be present to implement the strategy and evaluate the outcome. Without a national strategy, governance model, and supervisory body, efforts in different sectors become conflicted, preventing efforts to obtain an effective harmonization in cybersecurity development.[87]

Türkiye has developed three NCSS documents since 2013. The National Cybersecurity Strategy and Action Plan 2020-2023 delineates eight strategic objectives:

i. Protecting Critical Infrastructures and Increasing Strength;
ii. Developing National Capacity;
iii. Organic Cyber Security Network;
iv. Security of Next Generation Technologies;
v. Fighting Cybercrime;
vi. Development and Support of Domestic and National Technologies;
vii. Integration of Cyber Security into National Security;
viii. Developing International Cooperation.[88]

Unfortunately, the most recent report does not include a publicized Action Plan, an omission that is understood as a breach of transparency in cyberspace. In the two previous NCSS documents, the implementations, organizations, and action plans were made public.[89]

Several organizations play a role in the implementation of Türkiye's NCSS. The Ministry of Transport and Infrastructure is responsible for the preparation and governance of "cyber security activities at the strategic level with the National Cyber Security Board (established in 2013) and National Computer Incident Response Team (National CIRT) directed by the *Bilgi Teknolojileri ve İletişim Kurumu* (BTK), the Information and Communication Technologies Authority."[90] Other organizations involved in cybersecurity include National and Sectoral CERTs, the National Cybersecurity board, the Digital Transformation Office of Presidency, the Presidency of Defense Industries, the Scientific and Technological Research Council (TUBİTAK), the Police Department branch of Cyber Crime Prevention, the Personal Data Protection Authority (KVKK), the Ministry of National Defense, the Turkish Armed Forces (TSK) and the Presi-

dency of National Intelligence Organization (MİT).[91] Şentürk, Çil, and Sağıroğlu argue that "One of the most important issues [in enacting cybersecurity] is the designation of one single central authority that will be responsible for overall national cybersecurity. This authority should harmonize all the efforts and activities of other organizations that have cybersecurity tasks such as accreditation, auditing, standards, specification, and protection of both public and private systems as well as critical infrastructures."[92]

Cyberspace is not dominated by states; indeed, it is a multi-stakeholder domain

The Ministry of Transport and Infrastructure is Türkiye's national coordinator of cybersecurity, but there are some concerns about its effectiveness and its capability to organize all the relevant institutions. Powerful national coordinators are usually responsible to the highest authority in the government structure. But instead of having an institution responsible directly to the President, such as the Presidency Digital Transformation Office, this task is given to a ministry in Türkiye.

The GCI ranks the Turkish government's performance in the organizational setting at 17.96/200; according to the NCSI, Türkiye's cybersecurity policy development is 86/100, its military cyber operations is 17/100 and the protection of personal data is 100/100; Türkiye's overall average is 76/100.

Capacity Building

Capacity building is about raising awareness, providing training, education, incentives, and campaigns for developing a cybersecurity culture among all internet users or digital citizens. Today, more than half of the world's population, almost 5.3 billion people, are internet users. Every day, more than seven billion searches are done on Google, more than 10 billion GB of information is shared online, and more than 250,000 web pages are hacked.[93] According to Checkpoint, more than 60 million cyber-attacks take place on average every day.[94] The user or individual is the weakest link in cybersecurity, open to social engineering cyber-attacks such as fishing and spam messages. Therefore, "cybersecurity capacity building is key as it contributes to reducing issues such as digital divide and cyber risks."[95] Capacity building is measured through "the number of research and development, education and training programs and certified professionals and public sector agencies."[96]

Türkiye has launched several initiatives for raising awareness, conducted research and development (R&D) programs, developed formal and informal training courses, provided technical education, and launched quite a few campaigns. According to GCI 2020, Türkiye's capacity development score is 20/20. Türkiye's NCSI 2020 ranking in terms of educational and professional develop-

ment, which includes a number of programs in university as well as in primary and secondary schools, is 50/100. Therefore, Türkiye's average score in capacity building is 75/100.

Cooperation

Cyberspace is not dominated by states; indeed, it is a multi-stakeholder domain. It is populated with powerful private actors with more capability than even states. Therefore, states need to cooperate with non-state actors, including private companies, international organizations, Information Technology (IT) Non-Government Organizations (NGOs), and experts to ensure national security in cyberspace. Because the internet is a global network, ensuring security requires global cooperation. Thus, there is a need for cooperation at the international level among states and all other stakeholders: "The security of the global cyber ecosystem cannot be guaranteed or managed by any single stakeholder, and it needs national, regional, and international cooperation to extend reach and impact."[97] Cooperation includes public-private partnerships, bilateral and multilateral agreements, public-public partnerships, private-private partnerships, and best practices. As the GCI urges, "Greater cooperation can enable the development of much stronger cybersecurity capabilities, helping to deter repeated and persistent online threats and enable better investigation, apprehension, and prosecution of malicious agents."[98]

The Turkish government has already cooperated with private actors on certain projects. "As an example of national cooperation, a project to counter spam e-mail was launched in 2009 by the BTK with the participation of many public and private institutions."[99] Türkiye also engages in international cooperation through its membership in NATO and partnership with the Council of Europe, for example. Türkiye's initiatives for cooperation at the national and international level are scored by the GCI 2020 as 20/20, and by the NCSI as 50/100, based on the country's contribution to global cybersecurity including its cooperation activities. Therefore, Türkiye's average performance in terms of cooperation is 75/100.

Conclusion and Recommendations

The quantitative and qualitative analysis conducted here reveals that Türkiye addresses cyberspace in its security calculus as the fifth operational domain alongside land, sea, air, and space. With its physical, virtual, logical, and informational dimensions, cyberspace is too complicated to be fully understood by a single discipline. Instead, a multi-disciplinary approach is needed to comprehend and address it. Indeed, cyberspace is so complex that it is the only thing created by human beings that is not understood by them. Subsequently, even though cyberspace has been a fact of our lives for more than 50 years;

a comprehensive theory of cyberspace has not been developed.

If the institutions involved in providing cybersecurity do not share information, insecurity will be the natural outcome

States long considered cyberspace an issue of low politics. It is only a decade ago that states came to recognize it as a matter of high politics –a crucial one for security, military, and strategic issues. Resultantly, cybersecurity now occupies a secure position as a top global agenda item. Cybersecurity is now integrated into national security visions and plans across the globe. Just as the term cybersecurity is multidimensional, cybersecurity in action takes place on multiple levels: individual, societal, state, and global. The weakest link in cybersecurity remains the individual user. Therefore, cybersecurity capacity building on the individual and societal levels is essential for national and global cybersecurity.

Based on the findings and analysis of the paper, the following recommendations are proposed for each main pillar used in the GCI index:

Regarding legal measures, Türkiye is relatively weak in cyber incidents response, cyber threat analysis, and cyber crisis management. Thus, it needs to further develop legal regulations on improving cooperation and coordination in the cyber community. Türkiye also needs to focus more on rights and responsibilities online to encompass a positive rather than merely negative security understanding. Developing legal measures contributes to a country's readiness in cybersecurity, but proper implementation as well as the establishment of normative dimensions of regulations, including human rights and responsibilities, is much more vital.

Whereas the technical dimension is concerned, Türkiye is also relatively weak in cyber incident response, cyber safety and security, cyber threat analysis, and cyber crisis management. Thus, it needs to strengthen its national and sectoral CIRTs and develop more technical education for professionals.

In terms of organizational setting, Türkiye must determine a powerful coordinating institution with a comprehensive mandate directly responsible to the president. A clear-cut hierarchy among cybersecurity institutions is also needed. Türkiye badly needs an institution of sufficient scale and authority to develop and implement a centralized cybersecurity strategy. A more transparent national cybersecurity strategy is a must. Since cyberspace is based on transparency, information-sharing with the public and the inclusion of private actors on cybersecurity teams is indispensable. Keeping an Action Plan secret, as is the case in NCSS-2020, is not a solution but a source of insecurity. Major cyber-attacks on critical infrastructures or state institutions need to be

publicized to develop countermeasures. Otherwise, reoccurrence, as we have seen many times, is inevitable. But the key concept here is cooperation and information-sharing. If the institutions involved in providing cybersecurity do not share information, insecurity will be the natural outcome. Thus new strategies should propose new mechanisms and incentives for sharing information across public institutions and between the public and private sectors.

Regarding capacity building, more formal and informal training courses, cybersecurity education in primary and secondary schools, and cybersecurity programs in universities must be developed. R&D on cybersecurity should be encouraged and supported at all levels. The participation of universities, private companies, and NGOs in cybersecurity training and campaigns should be promoted and supported. Public institutions should benefit from the expertise at all levels without any discrimination based on ethnicity, religion, gender, or philosophical/political views.

Last but not least, in terms of cooperation measures, more public-private partnerships and bilateral and multilateral agreements should be formalized. Partnership at the national and international levels with absolute transparency is the key to success. The three NCSSs developed in the last decade have been theorized on the need for public-private entities to work together to counter threats, but in practice, there has been little cooperation. For instance, there are no representatives from non-state actors neither among Cybersecurity Board members nor in Türkiye's regulatory and supervisory Institutions. Public and sectoral CIRT teams also lack private participation.[100] Only a strong public-private partnership that promotes information sharing and facilitates coordinated responses to risks and threats can keep Türkiye's cyber ecosystem safe. Not only public-private but also international cooperation is inevitable for ensuring security in cyberspace. Since cyberspace is a global, anarchic domain, it requires global cooperation at every level among all stakeholders. ■

Endnotes

1. "Internet Live Stats," retrieved March 12, 2022, from https://www.internetlivestats.com/.

2. Silviu Stahie, "IoT Devices to Number 24.1 Billion by 2030, New Research Shows," *Bitdefender*, (May 25, 2020), retrieved April 24, 2022, from https://www.bitdefender.com/blog/hotforsecurity/iot-devices-number-24-1-billion-2030-new-research-shows.

3. "Internet Live Stats."

4. "Live Cyber Threat Map," *Checkpoint*, retrieved March 12, 2022, from https://threatmap.checkpoint.com/.

5. Steve Morgan, "Cybercrime Damages $6 Trillion By 2021," *Cyber Security Ventures*, retrieved May 14, 2022, from https://cybersecurityventures.com/annual-cybercrime-report-2017/#:~:text=Cybersecurity%20Ventures%20predicts%20cybercrime%20damages,in%20size%2C%20sophistication%20and%20cost.

6. Joseph S. Nye, "The End of Cyber-Anarchy? How to Build a New Digital Order," *Foreign Affairs,* Vol. 101, No. 1 (January/February 2022), retrieved March 24, 2022, from https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy, p. 3.

7. Nye, "The End of Cyber-Anarchy?"

8. William K. Tirrell, "United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?" Unpublished Ph.D. thesis, *Faculty of the U.S. Army Command and General Staff College*, (2012), pp. 7-8.

9. William Gibson, *Neuromancer*, (New York: Ace Science Fiction, 1984), retrieved May 1, 2022, from https://kupdf.net/download/william-gibson-neuromancer_59fbef8ce2b6f5126218562c_pdf.

10. Franklin D. Kramer, "Cyberpower and National Security," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security*, (Washington, D.C.: Potomac Book, 2009), retrieved May 1, 2022, from https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210, p. 4.

11. Hugo Loiseau, "Social Sciences and Studies on the Internet and Cyberspace," *Chaire Cyber*, (2013), retrieved May 3, 2022, from https://www.chaire-cyber.fr/IMG/pdf/r1_1_hugo_loiseau_territorialite_dans_le_cyberespace_3_draftv1.pdf.

12. Alessandro Finamore, "Analysis, Characterization and Classification of Internet Traffic," *Iris Polito*, (2012), retrieved May 3, 2022, from https://iris.polito.it/handle/11583/2497191.

13. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Kramer, Starr, and Wentz (eds.), *Cyberpower and National Security*, p. 27.

14. "ENISA Overview of Cybersecurity and Related Terminology," *ENISA*, (September 2017), retrieved May 1, 2022, from, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, p. 6.

15. Melissa E. Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security," in Alexander Klimburg (ed.), *National Cybersecurity Framework Manual,* (Talinn: NATO CCD COE Publication, 2012), retrieved May 1, 2022, from https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf, p. 8.

16. "National Cybersecurity Strategy and 2013-2016 Action Plan," *Ministry of Transport, Maritime Affairs and Communications of the Republic of Türkiye,* (2016), retrieved May 1, 2022, from https://www.btk.gov.tr/uploads/pages/2-0-1-cyber-security-strategy-and-action-plan-2013-2014-5a3412df707ab.pdf, p. 8.

17. "National Cybersecurity Strategy and 2013-2016 Action Plan," p. 7.

18. "National Cybersecurity Strategy and Action Plan 2020-2023," *Ministry of Transport, Maritime Affairs and Communications of the Republic of Türkiye*, 2020, p. 10. The same definition was used by the *ITU* in 2011. See, "ITU National Cybersecurity Guide," *ITU*, (2011), retrieved May 1, 2022, from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf, p. 5.

19. Lary D. Welch Usaf, "Cyberspace: The Fifth Operational Domain," *IDA*, retrieved May 1, 2022, from https://apps.dtic.mil/sti/pdfs/AD1124078.pdf, p. 3.

20. Nazli Choucri, *Cyberpolitics in International Relations,* (Cambridge: MIT Press, 2012), p. 234.

21. Choucri, *Cyberpolitics in International Relations,* p. 236.

22. Choucri, *Cyberpolitics in International Relations,* p. 236.

23. Nye, "The End of Cyber-Anarchy?"

24. Usaf, "Cyberspace," p. 2.

25. Nye, "The End of Cyber-Anarchy?" p. 3.

26. Nezir Akyeşilmen, *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik,* (Ankara: Orion Kitapevi, 2018), p. 107.

27. Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs,* Vol. 99, No. 4 (August 25, 2020), retrieved May 16, 2022, from https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

28. Nakasone and Sulmeyer, "How to Compete in Cyberspace," p. 2.

29. Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, "Defining Cybersecurity," *Technology Innovation Management Review,* (October 2014), retrieved April 25, 2022, from https://www.timreview.ca/article/835, p. 13.

30. "Definition of Cybersecurity," *ITU*, retrieved April 25, 2022, from https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

31. "Definition of Cybersecurity."

32. "NCSSD of Türkiye 2016-2019," p. 10.

33. "Definition of Cybersecurity."

34. Michael Veale and Ian Brown, "Cybersecurity," *Internet Policy Review*, Vol. 9, No. 4 (2020), retrieved April 25, 2022, from https://policyreview.info/pdf/policyreview-2020-4-1533.pdf, p. 2.

35. Veale and Brown, "Cybersecurity."

36. Throughout the paper, International Relations (IR) with capital letters is used to refer to the discipline of IR, while international relations in lower case refers to trans-borders relations between states.

37. Hilarie Orman, "The Morris Worm: A Fifteen-Year Perspective," *Security & Privacy,* (September/October 2003*)*, retrieved May 3, 2022, from https://www.cs.umd.edu/class/fall2019/cmsc818O/papers/morris-worm.pdf, p. 35.

38. Akyeşilmen, *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik*, p. 59.

39. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs,* Vol. 89, No. 5 (September/October 2010), retrieved May 4, 2022, from https://www.law.upenn.edu/live/files/6465-12-lynn-defending-a-new-, p. 99.

40. Shemakov, "The Morris Worm," p. 1.

41. Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, and Thomas Santoro, "The Cornell Commission: On Morris and the Worm," *Communication of the ACM*, Vol. 2, No. 6 (June 1989), retrieved May 4, 2022, from https://www.cs.cornell.edu/courses/cs1110/2009sp/assignments/a1/p706-eisenberg.pdf, p. 706.

42. "A worm is a program that can run by itself and can propagate a fully working version of itself to other machines. It is derived from the word tapeworm, a parasitic organism that lives inside a host and saps its resources to maintain itself. In contrast, "A virus is a piece of code that adds itself to other programs, including operating systems. It cannot run independently–it requires that its 'host' program be run to activate it. As such, it has a clear analog to biological viruses–those viruses are not considered alive in the usual sense; instead, they invade host cells and corrupt them, causing them to produce new viruses." See, Eugene H. Spafford "The Internet Worm Program: An Analysis," Purdue Technical Report CSD-TR-823, Purdue University (1988), retrieved May 4, 2022, from https://spaf.cerias.purdue.edu/techreps/823.pdf.

43. Akshay Jajoo, "A Study on Morris Worm," (2021), retrieved May 4, 2022, from https://www.researchgate.net/publication/357046348_A_study_on_the_Morris_Worm.

44. Orman, "The Morris Worm," p. 35.

45. Orman, "The Morris Worm," p. 40.

46. Linda Rosencrane, "Teen Hacker 'Mafiaboy' Sentenced," *Computer World*, (2001), retrieved May 4, 2022, from https://www.computerworld.com/article/2583318/teen-hacker--mafiaboy--sentenced.html.

47. Rebecca Hersher, "Meet Mafiaboy, the 'Bratty Kid' Who Took Down the Internet," *NPR*, (February 2015), retrieved May 4, 2022, from https://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet.

48. Charles Nesson and Anita Ramasastry, "Cybercrime," *Cyber Harvard*, (June 2002), retrieved May 4, 2022, from https://cyber.harvard.edu/studygroup/cybercrime.html.

49. Choucri, *Cyberpolitics in International Relations,* p. 2.

50. Akyeşilmen, *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik,* pp. 119-120.

51. Susan Hennessey, "Deterring Cyberattacks: How to Reduce Vulnerability," *Foreign Affairs,* Vol. 96, No. 6 (November/December 2017), retrieved May 4, 2022, from https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks, p. 41.

52. John Muller, "The Cyber-Delusion Digital Threats Are Manageable, Not Existential," *Foreign Affairs,* Vol. 101, No. 2 (March 22, 2022), retrieved May 4, 2022, from https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion, pp.1-2; Laurence J. Trautman, "Is Cyberattack the Next Pearl Harbor?" *North Carolina Journal of Law and Technology,* Vol. 18, No. 2 (December 2016), retrieved May 4, 2022, from https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article= 1326&context=ncjolt, p. 233.

53. John Muller, "The Cyber-Delusion" *CATO Institute* (March 22, 2022), retrieved May 4, 2022, from https://www.cato.org/commentary/cyber-delusion.

54. "Facilitating a Trusted Cyberspace for All," *ITU*, (2022), retrieved May 4, 2022, from https://www.itu.int/itu-d/sites/cybersecurity/.

55. "ITU National Cybersecurity Strategy Guide," *ITU*, (September 2011), retrieved May 4, 2022, from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf, p. 100.

56. "National Cyber Security Strategy Guidelines," *NATO*, (2013), retrieved May 4, 2022, from https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf, p. 6.

57. "National Cybersecurity Strategies Repository," *ITU,* retrieved May 4, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

58. "National Cybersecurity Strategy and Action Plan 2020-2023," *Ministry of Transport, Maritime Affairs and Communications of the Republic of Türkiye*, p. 10.

59. "Global Cybersecurity Index 2020," *ITU*, (2021), retrieved May 5, 2022, from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

60. "Global Cybersecurity Index 2020," pp. 6-7.

61. "Global Cybersecurity Index 2018," *ITU*, retrieved May 7, 2022, from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. p. 13.

62. "Global Cybersecurity Index 2020," p. 25.

63. "Description of Indicators," *NCSI,* retrieved May 7, 2022, from https://ncsi.ega.ee/indicators/. All NCSI indicators are based on (1) Cyber security policy development; (2) Cyber threat analysis and information; (3) Education and professional development; (4) Contribution to global cyber security; (5) Protection of digital services; (6) Protection of essential services; (7) E-identification and trust services; (8) Protection of personal data; (9) Cyber incidents response; (10) Cyber crisis management; (11) Fight against cybercrime; (12) Military cyber operations.

64. "The National Cyber Security Index Ranks 160 Countries' Cyber Security Status," *E-estonia*, retrieved May 7, 2022, from https://e-estonia.com/the-national-cyber-security-index-ranks-160-countries-cyber-security-status/.

65. "Turkey," *NCSI,* retrieved May 7, 2022, from https://ncsi.ega.ee/country/tr/.

66. *E-governance Academy*, retrieved May 7, 2022, from https://ncsi.ega.ee/.

67. NCPI is published by Belfer Center at Harvard Kennedy School, retreived from https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

68. Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach, "National Cyber Power Index 2020," (2020), retrieved May 7, 2022, from https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf, p. 1.

69. Julio Voo, *et al.*, "National Cyber Power Index 2020," p. 10.

70. Julio Voo, *et al.*, "National Cyber Power Index 2020," p. 37.

71. Julio Voo, *et al.*, "National Cyber Power Index 2020," p. 10.

72. Julio Voo, *et al.*, "National Cyber Power Index 2022," p. 10.

73. Julio Voo, *et al.*, "National Cyber Power Index 2022," p. 11-12.

74. Barclay Ballard, "Cybercrime Apparently Cost the World Over $1 Trillion in 2020," *Techradar*, (February 15, 2021), retrieved May 8, 2022, from https://www.techradar.com/news/cybercrime-cost-the-world-over-dollar1-trillion-in-2020.

75. Benn Russell, "Cybercrime to Top $6 Trillion in 2021, According to Cybersecurity Ventures," *NBCDFW*, (May 19, 2020), retrieved May 8, 2022, from https://www.nbcdfw.com/news/tech/cybercrime-to-top-6-trillion-in-2021-north-texas-security-firm-says/2636083/.

76. "Global Cybersecurity Index 2018," p. 3; "Global Cybersecurity Index 2017," p. 4.

77. "Global Cybersecurity Index 2018."

78. All relevant law regulations can be found on the webpage of the Institution of Communication and Information Technologies (BTK), *Mevzuat*, retrieved May 8, 2022, from https://www.btk.gov.tr/kanunlar.

79. "Global Cybersecurity Index 2020," p. 128.

80. "Turkey," *NCSI*, (2020), retrieved May 8, 2022, from https://ncsi.ega.ee/country/tr/.

81. Julio Voo, *et al.*, "National Cyber Power Index 2020," p. 12.

82. "Turkey," *NCSI*.

83. "Global Cybersecurity Index 2018," p. 3; "Global Cybersecurity Index 2017," p. 4; "Global Cybersecurity Index 2020," p. 6.

84. Emin Daşkın, "The Turkish Cyber Security Strategy: Structure, Legislation, and Challenges," *Journal of Intelligence and Cyber Security,* Vol. 2, No. 1 (June 2019), pp. 15-17.

85. Daşkın, "The Turkish Cyber Security Strategy," p. 19.

86. Daşkın, "The Turkish Cyber Security Strategy," p. 16.

87. "Global Cybersecurity Index 2020," p. 8; "Global Cybersecurity Index 2017," p. 4; "Global Cybersecurity Index 2018," p. 3.

88. "National Cybersecurity Strategy and Action Plan 2020-2023," p. 6.

89. "National Cybersecurity Strategy and Action Plan 2013-2014," *Ministry of Transport, Maritime Affairs and Communications of the Republic of Türkiye*, (2013), retrieved May 8, 2022, from https://www.btk.gov.tr/uploads/pages/2-0-1-cyber-security-strategy-and-action-plan-2013-2014-5a3412df707ab.pdf, pp. 21-46.

90. Ensar Şeker and İhsan Burak Tolga, "National Cyber Security Organisation: Turkey," *CCDCOE*, (2018), retrieved May 8, 2022, from https://ccdcoe.org/uploads/2018/10/CS_organisation_TUR_112018_FINAL.pdf, p. 9.

91. Şeker and Tolga, "National Cyber Security Organisation," pp. 10-15.

92. Hakan Şentürk, C. Zaim Çil and Şeref Sağıroğlu, "Cyber Security Analysis of Turkey," *International Journal of Information Security Science,* Vol. 1, No. 4 (2012), retrieved May 8, 2022, from https://dergipark.org.tr/tr/pub/ijiss/issue/16066/167876, p. 118.

93. "Internet Live Stats."

94. "Live Cyber threat Map."

95. "Global Cybersecurity Index 2020," p. 13; "Global Cybersecurity Index 2017," p. 4.

96. "Global Cybersecurity Index 2018," p. 3; "Global Cybersecurity Index 2017," p. 4.

97. "Global Cybersecurity Index 2020," p. 19; "Global Cybersecurity Index 2017," p. 4.

98. "Global Cybersecurity Index 2018," p. 3; "Global Cybersecurity Index 2017," p. 4.

99. Şentürk, *et al.*, "Cyber Security Analysis of Turkey," p. 120.

100. "National Cybersecurity Strategy and 2013-2016 Action Plan," *Ministry of Transport, Maritime Affairs and Communications of the Republic of Türkiye*, pp. 24-26.