Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance

Serkan Savaş · Süleyman Karataş

Abstract With the exponential increase of digital data in cyber environments, security measures have gained more importance. Cybersecurity threats are revealed by national and international units, and the number of these threats is increasing daily. The elimination of cybersecurity risks is possible with an effective cybersecurity strategy. Since the concept of management is not sufficient, the implementation of this strategy is possible with cyber governance, which includes all stakeholders in the management processes. This study emphasizes the importance and necessity of cyber governance in ensuring cybersecurity. The research and results for cybersecurity governance have been examined. A descriptive research model was used to this end. In terms of research philosophy, a basic research model and a documentary research model have been created with regard to the application method. The universe of the research consists of studies obtained from Web of Science, EBSCO, Scopus, Google Scholar, and TR Index. Studies from the last 5 years have been downloaded with the determined keywords. The result showed that although there are studies that produce local solutions for cybersecurity governance in different countries, a general governance framework has not been established as yet. On the contrary, there is a latent struggle to retain the management of this area, not its governance.

Keywords Cyberspace · Management · Cyber environment · Governance framework · Documentary research

Serkan Savaş
Faculty of Engineering, Department of Computer Engineering, Çankırı Karatekin University, 18100 Çankırı, Turkey
E-Mail: serkansavas@karatekin.edu.tr

Süleyman Karataş
İstanbul Başakşehir Special Education Practice School 3rd Stage, 34480 İstanbul, Turkey
E-Mail: suleymankaratas34@gmail.com
1 Introduction

With the widespread use of computer networks and the internet, cyberspace, which has become more mobile and shared, has started to turn into real-life itself. This transformation can be considered both the reward and the penalty of information age technology for national security. In cyber environments where intense data occurs, people inevitably use this data in a useful or harmful way, in addition to commercial and personal ways. Here, the concept of cybersecurity (CS) comes into play.

CS is described as “the set of tools, policies, security concepts, security assurances, guidelines, risk management approaches, activities, pieces of training, best practices and technologies used to protect the assets of institutions, organizations and users in the cyber environment” by Alkan (2012). The concept of CS no longer concerns only individuals or institutions, but also emerges as an international problem since threats in cyber environments are now more common, complex, and deeper. In cyber environments that make the world a single state, it has now become necessary to establish international law rules.

Today, new legal mechanisms and practices are developed to protect the rights and sovereignty of individuals, companies, institutions, and states against cyber threats and cyber terrorism. However, the changes in legal norms and legislation, as well as the strategies implemented in parallel with the information technology (IT) and the produced malware and techniques, are not in harmony with one other. Furthermore, the relevant stakeholders are not able to make decisions on an effective way of communication and governance. Thus, the resources can be wasted in the fight against cyber threats and the dominant actors are increasingly under the hegemony. This situation causes an inability to take necessary measures effectively and efficiently (Efe and Bensghir 2019).

The goals and organizational structures of management and governance processes differ from one other. Governance ensures that stakeholders’ needs, conditions, and options are balanced. It allows a determination of the management and administration in decision-making and prioritization, as well as a needs assessment to determine common institutional goals. At the same time, it ensures the observance of performance and compliance according to corporate purposes and orientation. Special governance responsibilities can be delegated to a number of specific units to the extent that institutional structuring, complexity, and capabilities allow. Management, on the other hand, fulfills the functions of planning, building, execution, and supervision according to the referral and direction made by the governance body. While governance concerns decision mechanisms, management refers to the implementation mechanism of decisions. According to this approach, although both take input from each other, they must be distinct. In other words, while governance is the mechanism that provides management and administration, management is the enforcement and action mechanism (Efe and Bensghir 2019).

Threats in cyberspace are increasing day by day; they harm institutions, individuals, and organizations. Since the concept of management is not sufficient alone to take measures to prevent these damages, the concept of governance, which includes all stakeholders in management processes, should be put into use. For this reason, the problem of putting the concept of cyber governance into a standard framework...
has emerged. In the concept of cyber governance, not only governments or institutions have roles, but also individuals and the private sector. Since each of these components has different purposes for using cyberspace, their definitions of roles in cyber governance are also different. International agreements, strategies, laws, metrics, and regulations must all be taken into account when establishing cyber governance standards, as they bring together such a diverse set of institutions and individuals with different roles. In addition, all of these arrangements must be performed in harmony. The regulations made should also cover data protection, security infrastructure, encryption, content protection, and all similar security sub-units that make up cyberspace. Since the scopes are so large, the rules determined should be kept wide while making the regulations. Therefore, informatics laws alone will not be enough. It is necessary to use the rules of international law for CS, to make decisions about problems and solutions, and to carry out detailed risk analyses.

Cyber governance is sometimes also used as internet governance. The concept of governance has recently been affecting management systems in the world and has come to the fore. Thus, as a reflection of this in cyberspace, the concept of cyber governance emerged as a natural result. To achieve success in cyber governance, it is necessary to provide features such as openness, transparency, participation, and accountability in the concept of governance, and human rights must also be protected. Today, countries such as the United States, Russia, and China, which steer technology in the world, attach importance to the concept of cyber governance and conduct studies in this direction. By foreseeing these studies, countries that carry out national studies will gain the ability to represent them on international platforms. Along with the concept of cyber governance, another issue that occupies the world agenda is who will control cyber environments.

Establishing an international legal standard for cyber governance is based on the universality of information law. However, today there are problems that information law cannot fully solve. The main ones include the following (Doğru 2016; Dülger 2004):

- Problems in commercializing electronic data.
- Responsibility of search engines and problems in internet law.
- Problems with the formation of the internet censorship network.
- Increase in crimes committed through social media.
- New generation peer bullying—the increase in cyberbullying.
- Failing to protect personal information in the digital environment.
- Violation of privacy and unauthorized access.
- There is no consensus on the definition and content of cybercrime, and classic criminal law is inadequate.
- With the widespread use of the internet, the common legal understanding determined by physical borders between countries is insufficient.
- There is no consensus on ethical rules in the digital world regarding intellectual property, user privacy, and information integrity.
- The technical, application, and legislative infrastructure of the e-signature is insufficient.
- Failure as yet to develop forensic informatics as an independent scientific discipline.
- The inability to prevent offenders from using computer systems for crimes such as money laundering and financing of terrorism through technology and the internet.
- Failing to prevent international cyber operations that cause all manner of rights violations.

Although new studies have been carried out in the field of IT law to overcome these problems, these studies have many theoretical, technical, and structural deficiencies. Cyber domains cover issues in all areas of civil society, military, social security, politics, economy, culture, technological development, security, and mobile technologies. For the management of all these different kinds of challenges, comprehensive rules must be found; written standards must be set and generally accepted. All institutions should be included in these processes and all employees in public and private institutions should grasp the importance of governance concepts. The elimination of CS risks is possible with the implementation of an effective CS strategy. The implementation of this strategy can be realized with the concept of cyber governance. Although the area covered by the concept of CS is cyberspace, the most important component of this concept is humans. Users should distinguish between security and insecurity in cyberspace and have technology literacy. Whether they are professional (business) users or personal users, all individuals are important for effective CS.

The aim of this study is to emphasize the importance and role of the concept of governance to ensure CS with all its elements. In addition, since the concept of cyber governance is a recent one, it is intended to be comprehended by both IT employees and all individuals who are not from this field but who are in any way a stakeholder of data sharing. Here, the concept of cyber governance should be designed to ensure that users in cyberspace act with a common consciousness. The plans, strategies, and technical studies that are only on paper will be insufficient in actual practice. This study and similar studies are important in terms of ensuring that the strategies determined to comply with national and international standards are accepted, understandable, compatible, and competent. With the work to be carried out and the planned training activities, cyber governance implementation will be provided and CS risks will be prevented.

2 Conceptual framework

2.1 Cyberspace

In the literature, cyberspace is sometimes called “cyber environment,” “cyber area,” and “cyber field” (and in public language even “virtual world”). Cyberspace means the environment that consists of information systems spread all over the world and space and the networks that connect them (Bakanlı 2013). While it is seen as appropriate to give this name to internet environments in research, cyber environments should be considered as a universe that includes all information systems and those...
who use these systems, especially with the spread of cloud computing and industry 4.0 technologies (Bıçakçı 2014). Components of the cyber environment are shown in Fig. 1 (Center 2014).

Technologies that produce digital data are used in the business world, in public spaces, at home, as well as in leisure activities—in short, at every stage of human life. Both corporate and personal data are transferred into cyberspace by all elements of the cyber environment specified in Fig. 1. The cyber environment has also been on the agenda on an international level and was defined as a new dimension by NATO in 2016, in addition to land, air, sea, and space. For this reason, it has also become an official operational area (NATO 2020).

### 2.2 Cybersecurity

The importance of CS is increasing every day and emerges as one of the most relevant disciplines required by all users, regardless of public, private, or personal background. The definition of CS according to the Maritime Transport and Communications Ministry of the Republic of Turkey (Bakanlığı 2013) is as follows: “Cybersecurity means the protection of the information systems that create the cyber environment from attacks, to secure confidentiality, integrity and accessibility of the information processed in this environment, the detection of attacks and CS incidents, the activation of reaction mechanisms against these detections and then returning the systems to their state before the CS incident”.

Cyber environments have now become real-life itself (Savaş and Topaloğlu 2019), and people spend most of the day in digital environments. For this reason, real-life threats can also be seen in digital environments. The number of cybercrimes is constantly increasing and almost every institution and every individual has been exposed to cyber attacks at some point. Due to these attacks and crimes, the importance given to the concept of CS has increased significantly in recent years. Data security in digital environments is one of the most important elements in providing CS. Cybercriminals who access computers with many different methods such as viruses, worms, Trojans, distributed denial-of-service (DDOS) attacks, and decoy methods damage users’ corporate or personal data and systems. In the same way that people take measures to keep their living spaces, homes, and workplaces safe, they also need to take measures to keep their data secure in cyber environments.

Companies around the world are trying to take software-based and hardware-based measures to ensure CS. In addition to these, measures are also taken in the di-

![Fig. 1 Components of the cyber environment](image)
mension of personnel training in order to prevent human-induced security problems. Another issue at the center of CS practices is ethics. Because important information of institutions and individuals is now recorded in the digital environment, possible CS issues can cause many problems for both. Corporate or personal privacy may be compromised. Corporate secrets can be exposed. CS risks may cause the disclosure of personal data. For these reasons, ensuring adequate security and making it sustainable is also an ethical problem itself (Macnish and van der Ham 2020).

Raising the awareness of users and employees is one of the most important factors in this regard. Currently, most cyber attacks are caused by people’s lack of knowledge. According to a Tessian report (2021), 88% of data breaches are caused by human error, so that humans are often considered as the “weakest link” in security. Nearly half of employees (43%) accept that they have made a mistake at work that had security repercussions for themselves or their company. One in four employees (25%) said they have clicked on a phishing email at work (Tessian 2021). To prevent this, businesses make enormous investments in CS, which is shown from a global perspective in Fig. 2 (Statista 2020).

Fig. 2 shows the CS expenditures of companies around the world between 2017 and 2020. The investments reached approximately 42 billion dollars in the middle of 2020. Since the outbreak of the COVID-19 pandemic, organizations worldwide have sent their employees into the home office for work. This decentralization of an organization’s IT landscape created new vulnerabilities for malicious actors to exploit, which is substantiated by IT professionals’ observation that there has been an increase in cyber attacks following the COVID-19 pandemic. As a result, cybersecurity remains a priority among business leaders to ensure operability of companies and data security (Statista 2020). From these investments, it is possible to understand the importance attributed to CS worldwide.

2.3 Management and governance

A different approach in terms of management is to bring resources together and perform the work in accordance with the organizational structure and purpose. The main factors discussed in this definition can be analyzed in four parts (Hitt 2005):
Management is the most important process for a business, including many activities and actions such as planning, decision-making, and evaluation. Resources are needed for the management to work. The goal is achieved by combining material and intangible resources. These resources include financial, material, workforce, and information. Management tries to work in a purposeful manner to achieve its goals. The two main factors in this study are human and organizational management. Management is provided by the establishment and operation of the organization.

Governance is defined as the structure or order created by the joint efforts of all relevant actors in a socio-political system (Bozkurt et al. 1998). In recent years, governance has been one of the most controversial issues in terms of democracy theory and the democratization process. In the 1990s, governance, which was brought to the agenda by international organizations such as the World Bank, the International Monetary Fund, the United Nations, the European Union (EU), and the Organisation for Economic Co-operation and Development (OECD), soon became the focus of great interest. While governance began to spread rapidly, it also became the subject of theoretical discussions (Ataay 2006). Governance is also seen as a process that is formed by interdependent positions and actors with conflicting and opposing interests, coordinating different network structures (Cope et al. 1997). Actors in society are partners for governance. For this reason, governance can be seen as a steering and control mechanism formed in the interaction of the economic, political, and social actors of the society. Therefore, governance is a process brought about by the interaction of different actors (Tekeli 1996).

Today, the term governance is used to express a complex system that includes the public administration, the private sector and non-governmental organizations, and the network and mutual interactions between them. In this process, the exis-

![Fig. 3](image_url) a Economic, social, and political priorities, and b scope of the governance
tence of a wide range of actors, including non-governmental organizations, private entrepreneurs, and non-profit organizations, as well as central government and local government organizations, as well as their inclusion in the management system, comes to the fore (Eryılmaz 2000).

Governance is preserved in a triangle of participation, transparency, and accountability (Fig. 3a). In addition, it is possible to reach a compromise on economic, social, and political priorities with this triangle. This compromise brings together economic development.

Governance covers the private sector, civil society, and in particular the public, which includes political organizations and public sector organizations (Fig. 3b). Public organizations, one of the actors, focus on how to serve their citizens more effectively in this process. Governance creates a framework for development and establishes the basis of equality, peace, and justice by maintaining the rule of law, regulating socio-economic conditions, developing social and physical infrastructures, and providing social security nets. The private sector as the second actor covers private businesses in various sectors. These organizations ensure economic development and growth by creating employment and income sources, developing production, trade and human resources, and through service provision and corporate standards (Başkanlığı 2003). The third actor within the scope of governance is civil society, which establishes the foundations of freedom, equality, and responsibility through organizing and educating communities by serving as the interface between the individual and the state, ensuring the participation of groups in society in economic and social life, facilitating political and social interaction, increasing solidarity, and nurturing cultures (Özer 2006).

2.4 Cyber governance

Cyber governance can be defined as the operation of decision-making processes in a way that increases participation, transparency, and accountability in taking measures related to cyberspace, together with the mechanism of international agreements, strategies, laws, measures, regulations, and standards that interlock in the best way (Efe and Bensghir 2019).

Cyber governance in international relations is one of the most prominent issues of recent years. International organizations have searched for solutions regarding the challenges of cyber governance. In this regard, first steps have been taken by signing the “Cyber Crime Convention” by the Council of Europe (Önok 2013). In addition, international standardization has been adopted in this area. For example, the ISO/IEC 38500:2015 standard provides guiding principles for members of governing bodies of organizations on the effective, efficient, and acceptable use of IT within their organizations. The standard applies to the governance of the organization’s current and future use of IT. This governance also covers the management processes and decisions related to the use of IT. Moreover, the ISO/IEC 38500:2015 standard defines the governance of IT as a subset or domain of organizational or corporate governance. These processes can be controlled by IT specialists within the organization, external service providers, or business units within the organization (ISO 2015). As mentioned, although there are some steps for cyber governance standardization and
CS standardizations, such as ISO 22301, ISO/IEC 27001, 27002, 27031, 27032, 27701, there is not yet a framework standard consisting of the combination of cyber governance and CS as two separate subjects.

3 Proposed strategy

The research strategy is to collect data and analyze it using systematic processes and tools. The data obtained in the study include cyber governance and CS governance (CSG) articles published on different academic databases. The present study, by analyzing this data, aims to examine the steps taken in the field of CSG around the world by investigating the scope and results of these publications, and to determine the steps taken so far in CSG, which is a new subject. In this way, a due diligence study was conducted on the steps to be taken to ensure CSG, the deficiencies identified, and the work that can be done in the future.

3.1 Research model

In this study, a descriptive research model, one of the qualitative research methods, is used. A basic research model for research philosophy and a documentary research model, which is based on data (text, pictures, etc.) compiled from existing sources such as libraries, archives, museums, and the internet (University 2020), has been created in terms of application method. The research model used in this study is shown in Fig. 4.

The research model used in this paper consists of studies obtained from Web of Science (WoS), EBSCO, Scopus, Google Scholar, and TR Index. The studies used in the research were recorded in academic databases and classified according to the research subject. The studies related to cyber governance and CSG from the last 5 years in the databases have been searched with the determined keywords. The

Fig. 4 Research model. EBSCO Elton B. Stephens Company, TR Turkish Republic
obtained studies are arranged according to the research subject and then in historical order. These studies were classified as follows:

- **Author(s)
  - Research year
  - The subject of the study**

and the findings are presented in the fourth part, results and discussion in the fifth part, and recommendations in the sixth part of the study presented in this paper.

### 4 Findings and review

Within the framework of the model prepared for the research, cyber governance and CSG studies from to the last 5 years in five different indexes were searched using the determined keywords, and a research database was created. The number of studies obtained is shown in Table 1.

As seen in Table 1, there are not many studies including cyber governance and CSG keywords in the Turkish literature as yet. Among the studies reached within the scope of the research, there are also duplicate studies found by different academic indexes. For this reason, a matrix chart was prepared for the studies obtained, and these duplicate studies were only examined once in the study. The matrix created is shown in Fig. 5.

In Fig. 5, the rows and columns show mutually the number of the same studies indexed by different indexes. If the color intensity in a cell in the matrix is high, it means that the number in that cell is high. When it is examined, it is concluded that out of 14 studies downloaded with the keyword “cyber governance” over WoS, 12 of them were also included in Scopus, 10 of them were downloaded via EBSCO, and four of them have also been listed in Google Scholar. It is also seen that there is one study reached with this keyword using the keyword “cybersecurity governance” on Google Scholar. Similarly, the numbers of the studies accessed from all academic survey indexes in the table are listed on the matrix.

|   | SY (TR a) | SGY (TR) | CG | CSG |
|---|-----------|-----------|----|-----|
| WoS | 0         | 0         | 14 | 8   |
| Scopus | 0        | 0         | 16 | 11  |
| EBSCO | 0         | 0         | 10 | 5   |
| TR Index | 0      | 0         | 1  | 0   |
| Google Scholar | 7    | 3         | 20 \(^b\) | 20 \(^b\) |

SY Siber Yöneti¸sim, SGY Siber Güvenlik Yöneti¸simi, CG cyber governance, CSG cybersecurity governance

\(^a\) TR Turkish language

\(^b\) Since there are many indexes such as web pages, results from repetitive sites, as well as books and patents on Google Scholar, 20 studies with the most citations and that appear in the first 10 pages were included in the research.
| WoS | Scopus | EBSCO | TRindex | Google Scholar |
|-----|--------|-------|---------|---------------|
| Siber Yönetişim | 0 | 0 | 0 | 0 |
| Siber Güvenlik Yönetişimi | 0 | 0 | 0 | 0 |
| Cyber Governance | 0 | 0 | 0 | 0 |
| Siber Yönetişim | 0 | 0 | 0 | 0 |
| Siber Güvenlik Yönetişimi | 0 | 0 | 0 | 0 |
| Cyber Governance | 0 | 0 | 0 | 0 |
| Siber Yönetişim | 0 | 0 | 0 | 0 |
| Siber Güvenlik Yönetişimi | 0 | 0 | 0 | 0 |
| Cyber Governance | 0 | 0 | 0 | 0 |
| Siber Yönetişim | 0 | 0 | 0 | 0 |
| Siber Güvenlik Yönetişimi | 0 | 0 | 0 | 0 |
| Cyber Governance | 0 | 0 | 0 | 0 |
| Siber Yönetişim | 0 | 0 | 0 | 0 |
| Siber Güvenlik Yönetişimi | 0 | 0 | 0 | 0 |
| Cyber Governance | 0 | 0 | 0 | 0 |
| Siber Yönetişim | 0 | 0 | 0 | 0 |
| Siber Güvenlik Yönetişimi | 0 | 0 | 0 | 0 |
| Cyber Governance | 0 | 0 | 0 | 0 |

Fig. 5 Database matrix. WoS Web of Science, EBSCO Elton B. Stephens Company, TRIndex Turkish Republic Index
4.1 Studies on cyber governance

When a search was carried out with the keyword “cyber governance,” seven studies were found only on Google Scholar. Two of these studies are book review articles and one is a workshop review. The remaining four studies are article studies conducted by the researchers. In the search made on WoS with the keyword “cyber governance,” 14 studies were found. As shown in Fig. 5, 12 of these studies are joint studies with Scopus, nine with EBSCO, and four with Google Scholar. Apart from the studies accessed from common databases, there are four different studies accessed via Scopus.

When the studies obtained with cyber governance keywords were examined, six different topics were formed. Although there are some studies that touch upon the subjects included in other themes in some section, the following main topics were determined in the general evaluation process:

- Cyber law studies and prevention of cybercrime
- Governance of cyberspace
- Cybersecurity policies
- Regional governance studies
- Reflections of cyber governance in the field
- Workshop, policy, and book review studies

The distribution of the studies on these themes was realized as shown in Fig. 6.

![Fig. 6 Distribution of cyber governance studies in themes](image-url)
On the theme of cyber law studies and prevention of cybercrime: The necessity of a legal framework and potential roadmap for international cyberspace legislation is stated as a common topic, which includes some basic issues of international cyberspace law such as global cyber governance, state sovereignty, internet freedom, enforcement of armed conflict laws, and international cooperation in combating cybercrime (Xinmin 2016). It is important to address CS problems with a multidisciplinary perspective by evaluating cyberspace and CS problems within the framework of international relations discipline and security approaches. A platform must be created to discuss cyber problems for developing a common understanding within the framework of the governance logic. Also, non-state actors, international organizations, and even individuals must be included in this platform (Çelik 2018).

To prevent spying and stop cyber conflicts, it is stated that international institutions and organizations can reduce the cyber trust gap by determining the rules of the game if the phrase is true (Fliegauf 2016).

In these studies, the importance of incompatibility with technologies in criminal law and the uncertainties in legal provisions that cannot be regulated simultaneously with the passage of time and the flow of life are also highlighted (Walker-Munro 2020). To take national precautions as necessary in cyberspace and to solve the problems in the field of informatics law, initially, security and reliability in electronic government must be ensured. It is also necessary to strengthen the software and hardware infrastructure related to informatics law by integrating tools and applications that will provide ease of work (Efe 2016).

Emphasizing that the lack of boundaries of cyber environments does not mean that it will not be included in a legal regulation framework, the importance of producing solutions with common sense instead of closing the internet and all countries to the outside world in order to ensure cyber sovereignty in security is explained. It was stated that international societies should establish a new cyber governance system based on cyber sovereignty and equality in sovereignty, mutual respect, democracy, and transparency and the governance activities will be the future of cyber sovereignty (Wenhong 2020). In addition, in order to create innovative cyberculture, the use of social governance and the formation of social groups should be calculated. To provide this calculation, social processes should be monitored digitally and expert evaluations should be carried out. In this way, a series of measures can be defined in order to eliminate the deteriorated and corrupt relations in society (Hacimahmud et al. 2017).

In studies on the theme of governance of cyberspace: In a study conducted by Bayrak (2018), it was discussed whether cyberspace would be managed by states or other actors. In addition to this discussion, it has also been investigated which states will have a say in governance and what kind of governance style they will adopt. In this study, it was also mentioned that states such as the United States (US), Russia, and China, which adopt that managing cyberspace means managing the physical world, causes governance problems rather than governance (Bayrak 2018). It is stated by Akyeşilmen (2018) that cyber governance also lacks governing institutions such as international law, international organizations, great powers, and diplomacy that alleviate anarchy at the global level. In order to better understand
the challenges of developing an integrated global cyber governance system, the cyber governance researches of countries from various regions of the world, both developed and developing, have been studied and their challenges are also explained (Greiman 2015). It is also stated in the studies that the debate on the governance of cyberspace should not be perceived as another conflict between “the West and the Rest,” but as a struggle to embrace and protect human rights in cyberspace (Liaropoulos 2015).

The values of corporate assets accessible in cyberspace, the intentions of hackers and criminals, the discourses between the governing body and the management, the dynamic relationships between the state of cyber risk and controls, and the balance between corporate value and cyber risk are the cyber governance elements that really need to be highlighted (Kikuchi and Okubo 2019). Therefore, it is difficult to create a common understanding of cyber governance. Since the CS discourse brings an understanding such as military or state security, the humanitarian aspect is seen as incomplete. However, the most effective mechanism for the governance of this place is stated as protecting human rights (Liaropoulos 2015). In the studies, the definition of good cyber governance has been made by human rights and multiple stakeholders. In this definition, it has been stated that good cyber governance requires greater accountability and transparency. For good cyber governance, more stakeholders should be reached through mobile devices and the internet and a human rights-based approach should be developed. Technology should be used as an element that promotes and protects human rights.

In cyber governance studies, multistakeholder governance models were examined and suggestions were made for their improvement. Greater transparency in decision-making with a veto ban, allocating financial resources to empowering disadvantaged stakeholders, and fairly allocating leadership positions are among these improvements. It has been stated that cyberspace must be managed through a combination of formal and informal approaches. This combination has been defined as a flexible, incremental, and sectoral approach to strengthening the rule of law in cyberspace through international agreement, efforts to build trust and consensus through the development, dissemination, and institutionalization of norms for responsible behavior in cyberspace (Jayawardane et al. 2015). The fact that states cannot secure cyberspace on their own forces them to develop cooperation mechanisms with each other and international organizations as well as with the private sector. This reality has raised a number of problems with the most effective governance model (Liaropoulos 2017). Although the solution to the problems in cyber environments is seen as prohibitions, it has been stated that the applied bans are ineffective in cyber environments. For this reason, it was stated that the problems encountered with the governance techniques to be applied in the future can be overcome by improving troubleshooting responsibilities (Raymond 2016).

**Studies conducted on the theme of cybersecurity policies:** Regional and international CS policies and their applications are explained. It has been stated that information warfare in cyber environments is a new and poorly understood threat to the international community that can be used more widely as a foreign policy tool in the future. Lei (2019) stated that by analyzing cases in countries such as Rus-
sia and North Korea, information warfare can be used by weaker states as a tool against stronger ones. The use of information warfare is expected to become more widespread due to the weakness of existing legal and normative frameworks. Kahraman et al. (2019) stated that the CS policy of the Council of Europe addresses the steps taken against cyber incidents for developed European countries. They also stated that Turkey has taken steps against cyber incidents by publishing cyber security policies in recent years. In these studies, it was stated that in order to intervene in information warfare operations and CS elements, there is a need for a governance model that can bring all these variables together under the same roof, without remembering that there are different disciplines, sectors, actors, and components. States can take action to promote relevant international governance and develop policy frameworks to protect themselves against information wars. It is emphasized that a problem with economic, social, political, technical, cultural, and legal dimensions without any distinction between formal and informal, state and private, can be successfully solved as long as all these components are handled together (Kahraman et al. 2019; Lei 2019).

Unlike the studies that bring international recommendations, based on regional studies, studies suggesting national CS models have also been carried out. While creating the national CS strategy, it is expected to cover cyberspace, CS, stakeholder engagement, capacity building, cyber governance, cybercrime, and cyber defense elements. In cooperation with these national strategies and in line with cyber governance and cyber law, the aim is to develop international CS strategies. Therefore, in a study, the CS strategies of 10 leading countries and intergovernmental organizations in cyberspace were analyzed comparatively (Sabillon et al. 2016). In the studies, not only policy recommendations were made on the basis of the state, but also sectoral policy models were developed. In the model, where the accountability and responsibilities of companies against cyber risks arising from the use of cyberspace are defined, the need to determine how ready they are to address cyber risks is explained (Von Solms 2016).

**Studies on the theme of regional applications of cyber governance:** These studies focus on the cyber governance understanding of different countries. Among these studies, research conducted in China stands out. The main features of China’s approach to the governance of internet information were explained by the researchers. It is stated that the dialectical relationship between internet freedom and internet order should be clarified and a people-oriented, bottom-up participatory approach should be adopted towards the ecological governance of internet information (Wang et al. 2020). Researchers have stated that China supports internet sovereignty, but the strategies applied to realize this sovereignty are diverse, fragmented, and underdeveloped (Zeng et al. 2017). Considering the extent of China’s participation in cyber environments, internet usage, and other digital statistics, the researchers, who show China’s presence in the governance of cyber environments as a natural justification, have built the basic principles of global cyber governance on cyber sovereignty-based pluralism. There are also differences between the understanding of cyber governance between China and other countries. For this reason, negotiations between
China and other states should be held to create an alternative for multilateralism, democracy, and transparency in global cyber governance (Cuihong 2018a, b).

There are three situations in cyber environments: stable, medium stable, and unstable. International cyber governance and cyber strategic stability have become two areas that have emerged in international studies. It is stated that the active participation of Chinese scientists in related studies will contribute to the knowledge base and theoretical framework of international cyber governance. In the study, it was stated that an international order that helps cyber strategic stability can only be developed through effective dialogue and joint work based on common interests and concerns among all international stakeholders, and this will shape the cyber strategies of individual countries (Zhou 2019).

Studies conducted in European countries have also participated in regional research. In studies conducted in the Netherlands, Denmark, Estonia, and the Czech Republic, cyber governance classification has been made. The Netherlands has created a participatory managed cyber environment characterized by trust and equity. The Czech and Estonian models have been compared to a cyber-management organization with a sanctioned role for national CS centers. Denmark has adopted a model of the lead agency. According to the research, national computer emergency response teams (CERT)/computer security incident response teams (CSIRT) need to be deployed inside or outside the intelligence community to basically shape information sharing arrangements and potential roles during cyber crises. In addition, cyber capacity can be centralized in a single unit or spread across different sectors (Boeke 2018). In another study on the analysis of the Netherlands’ understanding of cyber governance, it was stated that a national understanding alone is not a complete solution for cyber governance and that it cannot be insensitive to the international arena (Claver 2018).

Many governments are trying to exercise domination in cyberspace as they do in physical spaces. The fact that private companies dominate in this complex ecosystem is annoying for many policymakers, just as their citizens have unlimited internet access. Governments are struggling to keep up with the pace of technological change—technology is evolving faster than law-making efforts. In a Russian example, which is supported by demographic factors, it is explained that the internet environment is rapidly becoming more international and less west-centered. Also, it has been argued that the inseparable intertwining of the internal and external relations of the Russian Federation plays an important role in determining the policies of global cyber issues to a large extent (Nocetti 2015). In a Malaysian-based study that emphasizes that governments need a transformative cyber governance security model to protect the information of valuable government agencies, it is stated that in order to have an open, stable, and vibrant cyberspace, governments should be more resistant to cyber attacks and the state agencies should be able to protect all interests in cyberspace (Perumal et al. 2018).

On the theme of the reflections of cyber governance in the field: Here, studies that apply to the cyber governance strategy are examined. It has been observed that these studies are mostly applications in the financial sector, and cyber governance mostly focuses on securing critical interfaces in this sector (Menacho and Martin...
Although cyber governance plays a very important role in the business world, it has been noted that companies have difficulty determining the best policies and strategies to implement both internally and with their corporate partners. However, the relations between the business of a company and its stakeholders are primarily affected by cyber governance strategies (Ribeiro 2019). Therefore, a participatory method should be followed in the decision-making mechanisms of cyber governance in the financial sector.

According to research in the commercial sector in Jordan, it is stated that banks should conduct an analysis of their needs before making a change in their information and communication technology environment, their transactions and supplies, or after any event that affects their security. Improvements must be made in the CS policy and program to comply with artificial intelligence applications (Al-Tahat and Moneim 2020). With the increasing cloud computing systems, the risks of commercial banks related to the use of cloud accounting are also discussed. In addition to the need to adopt cyber governance as a fundamental reference to banking policies, the requirements of special departments for human resource management within the bank that will have a leading intellectual orientation to deal with modern trends in cyber governance are also described (Ali et al. 2020).

Social networks and cyber democracy tools offer important opportunities for individuals to develop an ideal democracy model as a new means of participation and representation of individuals in decision-making processes and management mechanisms. Concepts such as e-democracy, e-governance, mobile management, e-participation, e-voting, and e-politics enable people to participate in decision-making mechanisms within the framework of governance. Thus, the importance of internet-based applications in the participation and representation of individuals in management processes within the context of developments in the globalization process and information technologies, whose effects on political, social, and economic life are deeply felt and mutually supportive (Öztürk 2019).

Studies on the theme of the workshop, policy, and book review: Here, researchers have discussed the literary steps in cyber governance. Differences of opinion arose at the meetings of the United Nations (UN) State Experts Group, which would further clarify how international law regulates cyberspace. In a study that stated that there is a fragmented normative structure for information and communications technologies (ICT), researchers stated that non-state actors are likely to start to play a more central role in their efforts to bring legal clarity to their management within the framework of the concept of governance (Henriksen 2019). It is stated in a study that by creating a more integrated section on cyber attacks, cyber conflicts, and CS, examining the security dimension of cyberspace under a single heading has been presented as a solution that can overshadow the dominance of “security” (Söker 2018). In another study, researchers focused on cyberspace and international relations/theory, and discussed and negotiated to understand and make sense of cyberspace (Altiner and Çakır 2017).

In another study related to book reviews, the subject of cyber ethics was discussed and the aim was to explain the truths, mistakes, as well as good and bad behaviors in cyberspace. In this context, the core values and virtues of cyber technology...
and certain new challenges arising from cyber society are mentioned (Güler 2019). Similarly, a study compiling research and perspectives on data governance, consumer privacy, and project status reporting was conducted by Keil et al. (2019). In the research carried out on the CS and Protection of Personal Data agreement in Africa in 2014, 5 years after the acceptance of the agreement, only 14 of the 55 member states signed the document and seven of them ratified it. It was declared that 15 states must ratify the convention for it to be in effect. In the study, it was stated that Africa should work with its members to encourage the creation of cyber legislation and ratify the convention to protect its citizens while acting within the framework of the rule of law and respect for human rights (Turianskyi 2020).

The distribution of research and researchers within each theme is shown in Table 2 chronologically.

### 4.2 Studies on cybersecurity governance

When the cybersecurity governance (TR) keyword was scanned, only three studies on Google Scholar were found. One of these studies was also found in the cyber governance search and is examined in the previous section. The studies obtained with CSG keywords were examined, and four different themes were formed. Even

---

**Table 2** The distribution of research on six themes

| $N$ | CLS&PoCc | GoCs | CsP | RGS | RoCGitF | WP&BRS |
|-----|-----------|------|-----|-----|---------|--------|
| 1   | Efe (2016) | Greiman (2015) | Sabillon et al. (2016) | Nocetti (2015) | Menacho and Martin (2018) | Altuner and Çakır (2017) |
| 2   | Fliegauf (2016) | Jayawardane et al. (2015) | Von Solms (2016) | Boeke (2018) | Öztürk (2019) | Söker (2018) |
| 3   | Xinmin (2016) | Liapopoulos (2015) | Kahraman et al. (2019) | Zeng et al. (2017) | Ribeiro (2019) | Güler (2019) |
| 4   | Hacimahmud et al. (2017) | Raymond (2016) | Lei (2019) | Claver (2018) | Al-Tahat and Moneim (2020) | Henriksen (2019) |
| 5   | Çelik (2018) | Liapopoulos (2017) | – | Cuihong (2018a) | Ali et al. (2020) | Keil et al. (2019) |
| 6   | Walker-Munro (2020) | Akyesilmen (2018) | – | Cuihong (2018b) | – | Turianskyi (2020) |
| 7   | Wenhong (2020) | Bayrak (2018) | – | Perumal et al. (2018) | – | – |
| 8   | – | Kikuchi and Okubo (2019) | – | Zhou (2019) | – | – |
| 9   | – | – | – | Wang et al. (2020) | – | – |

*CLS&PoCc* cyber law studies and prevention of cybercrime, *GoCs* governance of cyberspace, *CsP* cybersecurity policies, *RGS* regional governance studies, *RoCGitF* reflections of cyber governance in the field, *WP&BRS* workshop, policy, and book review studies
though some studies also touch upon the subjects included in other themes in some sections of these studies, the following main topics were determined in the general evaluation process:

- Analysis and control of CS
- CSG
- CSG strategies and methodologies
- Reflections of CSG in the field

The distribution of the studies on these themes was realized as shown in Fig. 7.

**In the studies on the analysis and control of CS:** The cyber role of internal auditors and internal audits in the context of CS and cyber hygiene has been evaluated. Cyber hygiene can be defined as the set of activities that must be carried out in order to ensure and maintain the digital security of an organization or individual. To prevent organizations from becoming victims of a cyber attack, cyber hygiene strategies are required. For this hygiene to mature, cyber hygiene should be considered as personal hygiene and integrated into the institution in this way (Güler and Arkin 2019). As mentioned before, the weakest link in CS is the human. The most important reason for being affected by cyber attacks is also the human. For this reason, providing personal cyber hygiene is as important as providing organizational cyber hygiene, because ensuring cyber hygiene is not only the responsibility of information specialists but also of all employees. To realize a secure ecosystem in the age of information society, it is necessary to develop the measures taken, increase the
importance given to the field, and improve the legal regulations. For the efficiency of CS strategies, it is also necessary to focus on public–private partnerships (PPP), which is one of the common denominators. PPP is exemplified in the approach of countries such as the EU, Japan, Turkey, and the US (Aldemir and Kaya 2020; Min et al. 2015).

In the study conducted by Mačák (2016), it was argued that the issue of CS increased by the reluctance of states to involve themselves in the making of international law and the allegations that international law failed to address the modern challenges posed by the rapid development of information and communication technologies. It has been mentioned that attempts are being made to fill this gap with a series of non-state-driven norms, such as Microsoft’s cyber norms proposal or the Tallinn Guide project. The researchers stated that it will be decided shortly whether international law will lead to the collapse of interstate cyberspace management or whether legal approaches will be recalibrated (Mačák 2016).

**Studies on the governance of cybersecurity:** These studies have suggested that the need for state institutions to expand their horizontal coordination mechanisms is increasing, because cyber threats are becoming more complex every day. This need is followed by the increasing demand for criminological research into the managerial aspects of CS networks (Rondelez 2018). The philosophical concept of distributed authority has changed the nature of power by increasing the spread of the information age from governments to non-state actors (such as companies, civil society, and academia) (Pontbriand 2020). The governance aspects of CS have been investigated in businesses that are multidisciplinary by nature, and the use of various cybernetics models has been proposed in national CS risk management processes for continuous and good CS management by taking advantage of multidisciplinary cooperation, speech, target guidance, and dynamic feedback control aspects of cybernetics (Tatar et al. 2016; Vinnakota, 2016).

**Studies on the theme of CSG strategies and methodologies:** In these studies, the aim is to make the CSG framework functional. In this context, how to protect against CS threats and vulnerabilities is explained (Machado 2015). It has been stated that the difficulties in CS will vary with the social science perspective and social science perception. To this end, steps should be taken to develop a range of community building and support mechanisms that can simultaneously support a micro-based approach to expose research and community elements to each other (Whyte 2018). Corporate officials and the board of directors have potential roles and responsibilities in data governance. Issues and challenges related to CSG are also discussed in the studies (Thuraisingham 2019). It is stated that although CS has become a part of our daily life and concerns, it has not yet been fully adopted as a disciplinary field in Europe for in-depth research. It is also stated that the EU is an important actor in CS and should contribute to filling this gap by questioning what forms of governance it uses in this field (Carrapico and Barrinha 2018). For organizations, various models called the Cybersecurity Governance Maturity model have been proposed and the results have also been evaluated (de Bruin and von Solms 2015; Von Solms 2016).
Regarding the theme of CSG’s reflections in the field: In one of the studies, the difficulties of CSG in the energy sector were shown, and current CS standards were explained. It is stated how CSG will be applied to systems and what the requirements for this application are (Lam 2016).

Protecting intellectual capital is a CS risk. Capital boards and senior management teams need to outline CS risks to understand their CS responsibilities and accountability (Renaud et al. 2019). In the age of information security, while providing basic protection against common attacks is sufficient, in the age of CS, organizations need to implement smart, innovative, and efficient controls to detect and prevent advanced and emerging cyber attacks. In the past, information security was more concerned with the security of data in physical environments. However, CS has led to the emergence of a security concept covering digital environments. Thus, a new dimension has been added to information security, which requires not only the security of data in physical environments, but also the security of data in digital environments. CS activities now require enterprise-wide governance efforts that involve all employees, not just IT departments or designated individuals. In addition, digital technologies are now included in business strategies and work in harmony. CS strategies should likewise be included in working strategies (Spremić and Šimunic 2018).

The WannaCry software attack is an example of contemporary CS issues as an ICT-mediated epidemic. This epidemic has shown how incompatible CS events are with traditional national security policy and democracy. It also drew attention to how security rings should be formed (Christensen and Liebetrau 2019). Countries take steps in this regard and determine convergent and divergent models according to the changing balances in the world (Eldem 2020).

The distribution of research and researchers within each theme is shown in Table 3 chronologically.

| N  | A&CoCs       | GoCs          | CsGS&M          | RoCsGitF       |
|----|--------------|---------------|-----------------|----------------|
| 1  | Min et al. (2015) | Tatar et al. (2016) | De Bruin and von Solms (2015) | Lam (2016)     |
| 2  | Mačák (2016)  | Vinnakota (2016) | Machado (2015)  | Spremić and Šimunic (2018) |
| 3  | Güler and Arkın (2019) | Rondelez (2018) | Von Solms (2016) | Christensen and Liebetrau (2019) |
| 4  | Aldemir and Kaya (2020) | Pontbriand (2020) | Carrapico and Barrinha (2018) | Renaud et al. (2019) |
| 5  | –             | –             | Whyte (2018)    | Eldem (2020)   |
| 6  | –             | –             | Thuraiasingham (2019) | –             |

A&CoCs analysis and control of cybersecurity, GoCs governance of cybersecurity, CsGS&M cybersecurity governance strategies and methodologies, RoCsGitF reflections of cybersecurity governance in the field.
5 Results and discussion

The use of cyber environments is spreading day by day. Especially with the widespread use of the internet and social media, cyber environments have become “the real-life itself.” With this increase in usage, threats in cyber environments are also increasing and both institutions and individuals are harmed by these environments. This damage can sometimes be material as well as moral or even reputational. Considering all these factors, the need to establish management mechanisms in cyber environments has arisen, just as there are management mechanisms in real life. This management action is not just about hardware protocols and structures.

The need for policies and strategies in which national and international standards are set for the management of cyber environments is constantly increasing in importance. As the digital divide shrinks with the growing penetration of the internet, a democratic divide remains in the way people use the internet for civic engagement (Fierro et al. 2020). A management model has become even more important in recent years; it has been emphasized in many studies that this should be done within the framework of the concept of “governance” that includes a libertarian and participatory technique in which all stakeholders are involved. The research on “cybersecurity governance” conducted within the scope of this study, and which can be defined as a subset of the concept of cyber governance, has also shown that the world agenda is increasingly placing more emphasis on this governance issue.

The literature review on CSG has shown that the steps taken by governments and international organizations towards CSG are not yet at a sufficient level. The subject of the studies has generally been on “general concept definitions” or included “country-based studies.” This shows that CSG, which is closely related to the whole world and will become more important with the increasingly widespread use of the internet, social media, the internet of things (IoT), cloud computing, and industry 4.0 needs the integrity of policies, rules, and strategies valid worldwide, not specific solutions. In a few studies, issues such as economy, education, and energy systems are covered, and again, these studies do not cover a common policy on the concept of CSG.

The result of the study has shown that although there are studies that produce local solutions for this issue in different countries around the world, a general governance framework has not yet been established. Although some international organizations try to create a framework, these plans are not fully accepted. Moreover, it has emerged as a result that states such as the US and China, which can be seen as pioneers in technology, are in an invisible struggle against the governance of cyberspace.

CSG, which is the focal point of the study, is almost expected in the queue of transactions since those cyber governance techniques are not fully implemented yet.

CS concerns all individuals and organizations with access to a network, including public, private sector, and individual users. All real-life threats also exist in cyber environments. Just as people want to secure their homes, workplaces, and living spaces, they should secure the data they use with ICT tools. The concept of CS is a concept that can be realized in the cooperation of all units. At this stage, the concept
of governance comes into play. All units and all elements involved in cyberspace have their duties and roles in ensuring CS. These tasks are given as an example:

- A manufacturer should not open the door to unauthorized access to information that should not be accessed by finding a gap in the equipment that was developed.
- A manager should not sign decisions that will create security weaknesses to the policies to be determined and implemented.
- A user must ensure personal cyber hygiene, receive the necessary training provided by a company, and comply with the measures taken.

Based on these sample tasks, the scope and framework of policies that should be implemented for CSG can be drawn. The CSG to be determined should be within the following scope:

- **It must be generally valid:** The determined policies must be valid for all institutions, individuals, and devices in cyber environments. Since all individuals, institutions, and devices are included in the elements that make up cyber environments, the policies that bring them together should have general validity. The results of this research showed that different countries are trying to produce solutions within themselves. In fact, in these studies, it has been observed that policies sometimes even change from one sector to another. For this reason, CSG should be seen as an area where common rules should be applied for all institutions, individuals, and devices, rather than seeing it as an individual (national/corporate) competition area.

- **It must be internationally recognized:** It must be of a type of policy that all states accept and implement, not one or a few. Another result of the study is that the researches are generally country- or sector-based studies in the current situation. In addition, the existence of a secret general governance struggle between countries should not be ignored. These situations may harm the adoption of the policies determined by different countries. For this reason, especially worldwide policymaking institutions need to step in and determine CSG policies, similar to other standards accepted by the whole world, instead of a country- or institution-based approach.

- **It must be adaptable:** The policies determined should be adaptable to the issues in the sub-domain of cyber environments (e.g. CS, cloud computing, IoT, etc.). The number of components in cyber environments is continuously increasing and therefore new subset areas are constantly being formed. In this rapidly developing digital world, instead of frequently updating the policies, it is necessary to prepare policies that are far-sighted, more comprehensive, and adaptable to subsets in cyber environments. Cyber environments are formed in hierarchical structures. Similarly, the policies determined should have a hierarchical structure. In general, they should be designed in a structure that gets narrower as one goes down to the private sector, and they should adapt to the needs of all sub-domains.

- **It must be participatory:** It is necessary to provide participants representing all of the public, private sector, and individual users to the policies to be determined. As stated in the study, there is participation in the nature of governance. Management systems in the world have recently been shifting to more of a governance model.
Since one of the most important formation elements of cyber environments is interaction, it is not appropriate to prepare the policies to be determined in these areas separately from the representatives of the public or private sector and individual representatives, at the desk or behind secret doors.

- **It must be inclusive**: The policies determined should be policies that cover all institutions, organizations, and users—and not a single group. It was also observed in this study that certain sectors were involved in determining policies suitable for them. The fact that these studies set an example means that many different sectors or institutions take initiatives to determine policies for themselves. This situation is against the nature of the general valid policies and will also contradict the physical structure and fiction of the cyber environments that interact with the whole world.

- **It must be developable**: CSG must be able to adapt to changing situations with the development of technology. Cyber environments, where life without the internet can no longer be imagined and which are used by people for almost every purpose such as business, social, education, and entertainment (Savaş et al. 2015) are created by rapidly developing and changing technologies, both in software and hardware. Policies determined for governance also need to keep up with this change.

- **It must be binding**: CSG must be binding against all elements using cyber environments and must be able to impose sanctions. Sanctions are also needed for the determined policies to be accepted and binding. Just as certain sanctions are applied to ensure the applicability of real-life rules, similarly, sanctions will be needed to carry out policies in cyber environments. For this reason, while the studies are carried out, not only the rules should be established, but also the sanctions to be applied to adhere to them should be planned. These sanctions can range from limiting access to real-life fines and prison sentences. For this, national and international patrols can be established. Real-life security forces can be adapted to digital environments and the framework of existing teams can be expanded. In fact, artificial intelligence and machine learning algorithms can be used for these processes.

The scope of the framework to be determined for CSG can be expanded to cover the basic elements above, and the content of each scope item can be determined with more precise lines.

### 6 Recommendations

The fact that even the number of users of important social media sites today is expressed in hundreds of millions can exemplify the life dimension in cyber environments. For example, considering Facebook, which has approximately 2.5 billion users from all countries, it will not be odd to think of the internet environment as a single state without a flag. When many innovative technologies such as IoT, artificial intelligence, the metaverse and robotic applications, mobile technologies, and cloud computing are added to internet usage, a scope that will force the limits of the mind about the dimensions of cyberspace will emerge. Just as there have
been ongoing struggles between states and even between states of the same nation throughout history, the struggle for management and governance in these environments also maintains its existence. There is an invisible struggle for superiority here. The consequences of this affect all users.

There is a need for a common understanding and governance framework to securely carry out business and transactions, establish institutions, and continue life in cyber environments, which is an indispensable area of life. This framework is not one that can be determined by individuals, individual institutions, or individual states. The support of the world’s regulatory and binding international organizations is needed. Of course, although the policies to be determined by these institutions on their own are generally valid, it is also possible that there is a technical inadequacy. Therefore, opinions from all stakeholders should be taken into the concept of democracy, including universities, the public, the private sector, and individual users. Technology centers should be involved. Only with such solutions can permanent and future-oriented steps be taken.

Conflict of interest S. Savaş and S. Karataş declare that they have no competing interests.

References

Akyeşilmen N (2018) Cyber good governance: a new challenge in international power politics? Siber Polit Derg 3(5, 6):2–21 (http://cyberpolitikjournal.org/index.php/main/article/view/37)

Al-Tahat S, Moneim OA (2020) The impact of artificial intelligence on the correct application of cyber governance in Jordanian commercial banks. Int J Sci Technol Res 9(3):7138–7144

Aldemir C, Kaya M (2020) Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları. Kamu Yönetimi Polit Derg 1(1):6–27 (https://dergipark.org.tr/tr/pub/kaypod/issue/56116/726431)

Ali OAM, Matanreh AJ, Almalkawi A, Mohamed H (2020) The impact of cyber governance in reducing the risk of cloud accounting in Jordanian commercial banks-from the perspective of Jordanian auditing firms. Mod Appl Sci 14(3):75–89. https://doi.org/10.5539/mas.v14n3p75

Alkan M (2012) Siber Güvenlik ve Siber Savaşlar: Bilgi Güvenliği Derneği TBMM İnternet Komisyonu Sunumu. T. İ. Komisyonu,

Altun M, Çakır F (2017) Siber Uzay ve Uluslar Arası İlişkiler/Teorisi. Cyberpolitik J 2(3):180–187

Ataay F (2006) Türkiye’de yönetim ve “sivil toplum” tartışmaları üzerine bir değerlendirme. Memleket Siyaset Yönetim 1(1):121–140

Bakanlı́ği TCDÜH (2013) National Cyber Security Strategy and 2013–2014 Action Plan. Information Technologies and Communication Authority. https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf. Accessed 05.12.2020

Bayrak S (2018) Büyük güçlerin siber yönetim mücadelesi. Cyberpolitik J 3(5,6):47–60

Başkanlığı ABDD (2003) İyi yönetim temel unsurları. T.C. Maliye Bakanlığı,

Boeke S (2018) National cyber crisis management: different European approaches. Governance 31(3):449–464. https://doi.org/10.1111/gove.12309

Bozkurt Ö, Ergun T, Sezen S (1998) Kamu Yönetimi Sözluğu. T ODAIE Yayınları,

de Bruin R, von Solms SH (2015) Modelling cyber security governance maturity. 2015 IEEE International Symposium on Technology and Society (ISTAS).

Bıçakcı S (2014) NATO’nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. Uluslararası İlişkiler Derg 10(40):100–130

Carrapico H, Barrinha A (2018) European Union cyber security as an emerging research and policy field. Eur Polit Soc 19(3):299–303. https://doi.org/10.1080/23745118.2018.1430712

Center NCIR (2014) Basic Information on Cyber Security. U.-TRCERT,

Christensen KK, Liebetrau T (2019) A new role for ‘the public’? Exploring cyber security controversies in the case of WannaCry. Intell Natl Secur 34(3):395–408. https://doi.org/10.1080/02684527.2019.1553704

Claver A (2018) Governance of cyber warfare in the Netherlands: an exploratory investigation. Int J Intell Secur Public Aff 20(2):155–180. https://doi.org/10.1080/23800992.2018.1482435
Cope S, Leishman F, Starie P (1997) Globalization, new public management and the enabling state: futures of police management. Intl Jnl Public Sec Management 10(6):444–460

Cuihong C (1997) Globalization, new public management and the enabling state: Futures of police management. Intl Jnl Public Sec Management 10(6):444–460

Cuihong C (2018a) China and global cyber governance: main principles and debates. Asian Perspect 42(4):647–662

Cuihong C (2018b) Global cyber governance: China’s contribution and approach. China Q Int Strateg Stud 04(01):55–76. https://doi.org/10.1142/S2377740018500069

Doğru M (2016) Siber Hareketin Uluslararası Hukuk Çerçevesinde Analizi XVIII. Akademik Bilişim Kongresi, Aydın (https://ab.org.tr/ab16/bildiri/106.pdf)

Dülger MV (2004) Avrupa Konseyi ve Avrupa Birliği Düzenlemlerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayınaması Karşısı Yapılan Düzenlemler. İstanbul Barosu Derg 4:95–103

Efe A (2016) Bilişim Hukuku Alanındaki Sorunlar ve Risklerin Mevzuat Boyutuyla Analiz ve Çözümlemesi. Türk Nöterler Birliği Hukuk Derg 3(1):175–209

Efe A, Bensghir KT (2019) Siber Güvenlik İçin Siber Yönetişim. In: Siber Güvenlik ve Savunma Problemleri ve Çözümleri. Grafiker Yayınları, , pp 325–378

Eldem T (2020) The governance of Turkey’s cyberspace: between cyber security and information security. Int J Public Adm 43(5):452–465. https://doi.org/10.1080/01900692.2019.1680689

Eryılmaz B (2000) Kamu Yönetimi (Vol. İstanbul)

Fierro P, Aroca P, Navia P (2020) How people access the internet and the democratic divide: Evidence from the Chilean region of Valparaiso 2017, 2018 and 2019. Technol Soc 63:101432. https://doi.org/10.1016/j.techsoc.2020.101432

Fliegauf MT (2016) In cyber (governance) we trust. Glob Policy 7(1):79–82

Greiman V (2015) Cybersecurity and Global Governance. J Inf Warf 14(4):1–14

Güler B (2019) Modern information technology | governance of it for the organization. https://www.iso.org/standard/62816.html. Accessed 08.12.2020

Jayawardane S, Larik J, Jackson E (2015) Cyber governance: Challenges, solutions and lessons for effective global governance

Kahraman S, Kutlu O, Dinçer S (2019) Avrupa Birliği’ne Uyum Sürecinde Türkiye’nin Siber Güvenlik Politikalarının Analizi. In: ASSAM Uluslararası Hakemli Dergi, pp 1–14

Keil M, Culnan M, Dinev T, Xu H (2019) Data governance, consumer privacy, and project status reporting: Remembering H. Jeff smith. Inf Syst Front 21(6):1207–1212

Kikuchi M, Okubo T (2019) Cyber governance complex in firms. Proceedings of the 2nd International Conference on Control and Computer Vision.

Lam J (2016) IIET: Cyber security in modern power systems—Protecting large and complex networks. IET Cybersec Mod Power Syst. https://doi.org/10.1049/ic.2016.0044

Lei H (2019) Modern information warfare: analysis and policy recommendations. Foresight 21(4):508–522. https://doi.org/10.1108/FS-06-2018-0064

Liaropoulos AN (2017) Cyberspace governance and state sovereignty. In: Democracy and an open-economy world order. Springer, Berlin Heidelberg, pp 25–35 https://doi.org/10.1007/978-3-319-52168-8_2

Liaropoulos A (2015) A human-centric approach to cybersecurity: securing the human in the era of cyber-phobia. J Inf Warf 14(4):15–24

Machado MN (2015) Cyber Security Governance: Securing the European Union’s Cyber Domain. L. U. F. o. G. a. G. Affairs, Macnish K, van der Ham J (2020) Ethics in cybersecurity research and practice. Technol Soc 63:101382. https://doi.org/10.1016/j.techsoc.2020.101382

Mačák K (2016) Is the international law of cyber security in crisis? 2016 8th International Conference on Cyber Conflict (CyCon).

Menacho VSJ, Martin A (2018) Cyber governance and the financial services sector: the role of public-private partnerships

Min K-S, Chai S-W, Han M (2015) An international comparative study on cyber security strategy. Int J Secur Its Appl 9(2):13–20. https://doi.org/10.14257/ijisia.2015.9.2.02
NATO (2020) Warsaw Summit Communiqué. North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/official_texts_133169. Accessed 05.12.2020

Nocetti J (2015) Contest and conquest: Russia and global internet governance. Int Affairs 91(1):111–130

Önok M (2013) Avrupa Konseyi Siber Suç Sözləşməsi İşğinda Siber Suçlarla Mücədele Uluslararası İşbirliliği. Marmara Univ Hukuk Fak Hukuk Arastırma Derg 19(2):1299–1270

Özler MA (2006) Yöneti̇sim üzerine notlar. Sayı˙stay Dergisi (63):59–89. Retrieved from https://dergipark.org.tr/tr/pub/sayistay/issue/61520/918910

Öz türk C (2019) Demokrasiyi Hacklemek: Siber Demokrasi Araçları. Electron Turk Stud. https://doi.org/10.29228/TurkishStudies.22957

Perumal S, Pitchay SA, Samy GN, Shamugam B, Magalingam P, Albakri SH (2018) Transformative cyber security model for Malaysian government agencies. Int J Eng Technol 7(4.15):87–92. https://doi.org/10.14419/jiet.v7i4.15.21377

Pontbriand K (2020) Distributed authority as a guiding set of principles for transnational cyber security governance. International Conference on Cyber Warfare and Security.

Raymond M (2016) Managing decentralized cyber governance: the responsibility to troubleshoot. Strateg Stud Q 10(4):123–149

Renauk K, Von Solms B, Von Solms R (2019) How does intellectual capital align with cyber security? JIC 20(5):621–641. https://doi.org/10.1108/JIC-04-2019-0079

Ribeiro SLMR (2019) How Cyber Governance Influences Relationships Between Companies. Doctoral. NOVA Information Management School, Lisboa

Rondelez R (2018) Governing cyber security through networks: an analysis of cyber security coordination in Belgium. Int J Cyber Criminol 12(1):300–315. https://doi.org/10.5281/zenodo.1467929

Sabillon R, Cavaller V, Cano J (2016) National cyber security strategies: global trends in cyberspace. Int J Comput Sci Softw Eng 5(5):67–81

Savaş S, Topaloğlu N (2019) Data analysis through social media according to the classified crime. Turk J Electr Eng Comput Sci 27(1):407–420. https://doi.org/10.3906/elk-1712-17

Savaş S, Topaloğlu N, Güler O (2015) Türkiye’deki Uydu Alımaçları veführen Okulların Terra Texture Çevresinin Belirlenmesi: Bir Anket Uygulaması. Bilisim Teknol Derg 8(2):51. https://doi.org/10.17671/btd.20505

Söker Ç (2018) Disiplinerlararası Bir Yaklaşımla: Siber Politika & Siber Güvenlik. Cyberpolitik J 3(5, 6):140–143

Spremić M, Šimuníc A (2018) Cyber security challenges in digital economy. Proceedings of the World Congress on Engineering.

Statista (2020) Spending on cybersecurity worldwide from 2017 to 2020. Statista. https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/. Accessed 10.12.2020

Tatar U, Karabacak B, Gheorghe A (2016) An assessment model to improve national cyber security governance. 11th International Conference on Cyber Warfare and Security: ICCWS2016.

Tekeli İ (1996) Yönetim Kavramı Yanısıra Yöneti̇sim Kavramının Gelişmesinin Nedenleri Üzerine. Sosyal Demokr Degisim 3:45–54

Tessl (2021) The psychology of human error. https://www.tessl.com/research/the-psychology-of-human-error/. Accessed 10.11.2021

Thuraisingham B (2019) Cyber Security and Data Governance Roles and Responsibilities at the C-Level and the Board. 2019 IEEE International Conference on Intelligence and Security Informatics (ISI).

Turianskiy Y (2020) Africa and Europe: cyber governance lessons. Policy Insights 77:1–13

University D (2020) Research and Report Writing Techniques. http://akademik.duzce.edu.tr/Content/Dokumanlar/secancerin/Dosya/1da91783-2989-4d19-825b-a6894bd523c5.pdf (Accessed 15 Nov 2020)

Vinnakota T (2016) A second order cybernetic model for governance of cyber security in enterprises. 2016 IEEE 6th International Conference on Advanced Computing (IACC).

Von Solms B (2016) Towards a cyber governance maturity model for boards of directors. Bus Manag Rev 7(4):26–33

Walker-Munro B (2020) Cyber-governance, systemic governance and disruption of the criminal law. U Queensland LJ 39(2):225–252. https://doi.org/10.38127/uqlj.v39i2.5023

Wang C, Cheng L, Pet J (2020) Exploring the cyber governance discourse: a perspective from China. Int J Leg Discours 5(1):1–15. https://doi.org/10.1515/ijld-2020-2025

Wenhong X (2020) Challenges to cyber sovereignty and response measures. Mirovaia Ekon Mezhdunarodnye Otnoshenia 64(2):89–99

Whyte C (2018) Crossing the digital divide: Monism, dualism and the reason collective action is critical for cyber theory production. Polit Gov 6(2):73–82. https://doi.org/10.17645/pag.v6i2.1338
Xinmin M (2016) Key issues and future development of international cyberspace law. China Q Int Strateg Stud 2(01):119–133. https://doi.org/10.1142/S2377740016500068
Zeng J, Stevens T, Chen Y (2017) China’s solution to global cyber governance: unpacking the domestic discourse of “Internet sovereignty”. Polit Policy 45(3):432–464. https://doi.org/10.1111/polp.12202
Zhou H (2019) Strategic stability in Cyberspace: a Chinese view. China Q Int Strateg Stud 5(01):81–95. https://doi.org/10.1142/S2377740019500088
Çelik S (2018) Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım. Acad Rev Humanit Soc Sci 1(2):110–119

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.