


CYBERSECURITY GOVERNANCE: A SCOPING REVIEW

Talal Albalas^A, Amir Modjtahedi^B, Reza Abdi^C



ARTICLE INFO	<u>ABSTRACT</u>
<p>Article history:</p> <p>Received 08 August 2022</p> <p>Accepted 10 November 2022</p>	<p>Purpose: Security measures have become increasingly important due to the expansion of the cyber environments. National and international entities are exposing themselves to cybersecurity risks, and they are growing in number every day.</p>
<p>Keywords:</p> <p>Cybersecurity; Cyber Environment; Governance; Scoping Review Research.</p> <div data-bbox="172 909 480 1155" style="text-align: center;">  </div>	<p>Theoretical Framework: With a comprehensive cybersecurity plan, threats can be eliminated. Implementing this plan is possible by involving all stakeholders in the management processes because the idea of management is insufficient. To ensure cybersecurity, this study highlights the significance of cybersecurity and cybergovernance in the digital world.</p> <p>Design: The study findings and recommendations for cybersecurity governance were reviewed. A scoping review research model was used for this purpose.</p> <p>Findings: A basic and documentary research model related to research philosophy were developed for the application technique. The scope of the research includes publications from Scopus. Studies from the last ten years were downloaded using the selected keywords.</p> <p>Originality: The results show that despite research that has led to local cybersecurity governance solutions in several countries, a comprehensive governance framework has not yet been established. Instead, there is a hidden conflict over control of this region, not its governance.”</p> <p>Doi: https://doi.org/10.26668/businessreview/2022.v7i4.e629</p>

^A DBA Student. College of Business. Law and Social Science. Postgraduate Research Student. University of Derby, Derby - United Kingdom. E-mail: t.albalas1@unimail.derby.ac.uk Orcid: <https://orcid.org/0000-0001-9946-9674>

^B Senior Lecturer in Marketing and operation. College of Business. Law and Social Science. Senior Lecture in Marketing and Operations. University of Derby, Derby - United Kingdom. E-mail: a.modjtahedi@derby.ac.uk Orcid: <https://orcid.org/0000-0001-6028-877X>

^C Post graduate research supervisor. College of Business. Law and Social Science. Post-Graduate Research Supervisor. University of Derby, Derby- United Kingdom. E-mail: R.abdi@derby.ac.uk Orcid: <https://orcid.org/0000-0003-0603-9734>

GOVERNANÇA DA CIBER-SEGURANÇA: UMA REVISÃO DO ESCOPO

RESUMO

Objetivo: As medidas de segurança têm se tornado cada vez mais importantes devido à expansão dos ambientes cibernéticos. Entidades nacionais e internacionais estão se expondo a riscos de segurança cibernética, e eles estão crescendo em número a cada dia.

Estrutura teórica: Com um plano abrangente de segurança cibernética, as ameaças podem ser eliminadas. A implementação deste plano é possível envolvendo todas as partes interessadas nos processos de gestão porque a idéia de gestão é insuficiente. Para garantir a cibersegurança, este estudo destaca a importância da cibersegurança e da ciber governança no mundo digital.

Projeto: Os resultados do estudo e as recomendações para a governança da cibersegurança foram revisados. Um modelo de pesquisa de revisão de escopo foi utilizado para este fim.

Conclusões: Um modelo de pesquisa básica e documental relacionado à filosofia de pesquisa foi desenvolvido para a técnica de aplicação. O escopo da pesquisa inclui publicações da Scopus. Estudos dos últimos dez anos foram baixados usando as palavras-chave selecionadas.

Originalidade: Os resultados mostram que, apesar das pesquisas que levaram a soluções locais de governança de cibersegurança em vários países, ainda não foi estabelecida uma estrutura de governança abrangente. Em vez disso, existe um conflito oculto sobre o controle desta região, não sobre sua governança".

Palavras-chave: Ciber-segurança, Ambiente cibernético, Governança, pesquisa de revisão do escopo.

GOBERNANZA DE LA CIBERSEGURIDAD: UNA REVISIÓN DEL ALCANCE

RESUMEN

Objetivo: Las medidas de seguridad son cada vez más importantes debido a la expansión de los entornos cibernéticos. Las entidades nacionales e internacionales se exponen a los riesgos de ciberseguridad, y su número aumenta cada día.

Marco teórico: Con un plan integral de ciberseguridad se pueden eliminar las amenazas. La aplicación de este plan es posible implicando a todas las partes interesadas en los procesos de gestión, ya que la idea de gestión es insuficiente. Para garantizar la ciberseguridad, este estudio destaca la importancia de la ciberseguridad y la ciber gobernanza en el mundo digital.

Diseño: Se revisaron las conclusiones del estudio y las recomendaciones para la gobernanza de la ciberseguridad. Para ello se utilizó un modelo de investigación de alcance.

Resultados: Para la técnica de aplicación se desarrolló un modelo de investigación básico y documental relacionado con la filosofía de la investigación. El alcance de la investigación incluye las publicaciones de Scopus. Se descartaron los estudios de los últimos diez años utilizando las palabras clave seleccionadas.

Originalidad: Los resultados muestran que, a pesar de que la investigación ha dado lugar a soluciones locales de gobernanza de la ciberseguridad en varios países, todavía no se ha establecido un marco de gobernanza global. Por el contrario, existe un conflicto oculto por el control de esta región, no por su gobernanza".

Palabras clave: Ciberseguridad, Entorno cibernético, Gobernanza, Investigación de revisión del alcance.

INTRODUCTION

With the increasing use of the Internet, cyberspace is becoming more mobile and shareable. This change can be seen as both an advantage and a disadvantage in maintaining national security. People use data in cyber environments where there is a lot of information, in useful or harmful ways, in addition to economic and personal purposes. The idea of cybersecurity is important in this situation.

Cybersecurity refers to the procedures applied in protecting users in the cyber environment (Aslay, 2017). As threats in cyberspace become more frequent, sophisticated, and serious, the concept of cybersecurity is no longer limited to individuals or institutions but is

becoming a global issue. It has become imperative to create international legal principles for cyberspace that unite the world.

Today, in order to protect individual users, companies, organizations, and nations from cyber threats and cyberterrorism, new legal frameworks and procedures are being developed. However, the changes in legal standards and regulations, as well as tactics used in relation to information technology (IT), malware created, and methods developed are not aligned. In addition, it is impossible for the parties involved to agree on a working governance and communication strategy. Therefore, it is possible that resources are spent on the fight against cyber threats and the hegemony of the dominant players grows. This state of affairs makes it difficult to implement the necessary measures efficiently and effectively (Çözümler, 2019).

Management and governance processes have different organizational goals and structures. The role of governance is to balance the requirements, circumstances, and opportunities of stakeholders. It enables management and administration to make decisions and set priorities, as well as needs assessment to achieve attainable goals. At the same time, it ensures performance and adherence to organizational goals and direction to the extent that institutional structuring, complexity, and competencies allow, specific governance tasks can be delegated to individual units. On the other hand, management performs the tasks of organizing, creating, implementing, and monitoring in accordance with the recommendations and directives of the governing body. Management refers to the means by which decisions are put into practice, while governance encompasses the decision-making processes. This approach states that while the two are interdependent, they must be separate (Çözümler, 2019).

The terms Internet governance and cyber governance are sometimes used interchangeably. Recently, the idea of governance has become more prominent and has implications for governance systems around the world. Thus, the idea of cyber governance has evolved as a logical consequence in cyberspace. For cyber governance to be successful, human rights must also be upheld. These elements include transparency, and accountability within the governance idea. The concept of cyber governance is important today, and first world countries such as China and the US, which have a global influence on technology, are paying attention to it and conducting research in this area. Countries conducting national studies can represent them on international platforms by anticipating these studies. Who will have control over cyber environments is a concern that is on the global agenda, along with the idea of cyber governance (Savas & Karata, 2022)

The scoping review process is used because it is most appropriate in this situation. Through this review, the study seeks to address some of the following questions:

RQ1: What is the concept of cybersecurity and cybersecurity governance?

RQ2: What is the trend in the literature involving cybersecurity governance?

RQ3: What is the most productive country's cybersecurity governance?

RQ4: What are the most productive journals for cybersecurity governance?

RQ5: What are the most cited articles in cybersecurity governance?

The purpose of this study is to highlight the importance and function of the idea of governance in ensuring cybersecurity in all its forms. Since cyber governance is a relatively new idea, it should be understood by IT professionals as well as anyone else who has an interest in sharing data but is not a IT professional. This is where the idea of cyber governance should be developed to ensure that users behave in common sense online (Rahman et al., 2021).

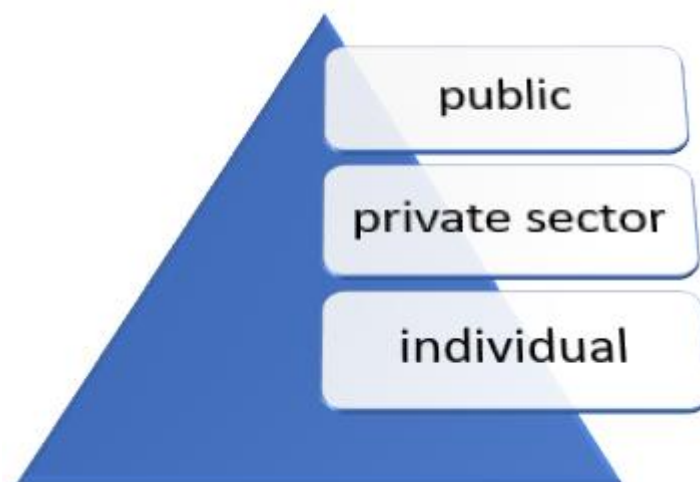
CONCEPTUAL FRAMEWORKS

Cyberspace

According to Bakanlıgı (2013), cyberspace is the environment consisting of networks connecting different information systems scattered all over the world and space. With advancement in technology, the cyber environments is a universe that encompasses all information systems and their users. While it is considered legitimate to refer to cyberenvironments as such in research (Blazevic et al., 2014). Figure 1 illustrates the elements of the cyber environment (Barnes & Pressey, 2011).

Digital data production technologies are used in the workplace, in public places, at home, during leisure time, in other words, at every stage of a person's life. All components of the cyber environment shown in the figure transport both business and personal data into cyberspace.

Figure. 1 Components of the cyber environment

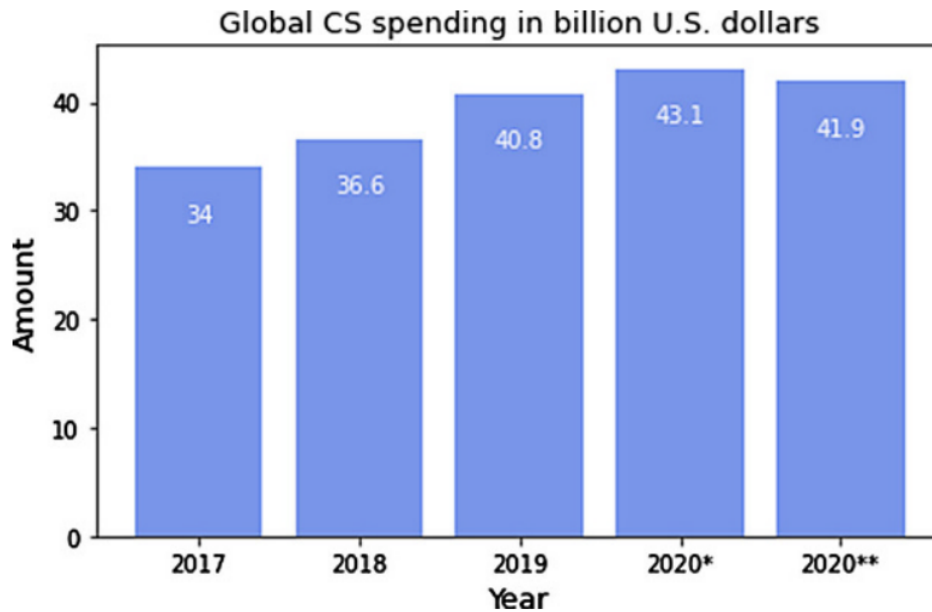


Cybersecurity

Regardless of their public, private, or personal background, users are expected to understand the importance of cybersecurity, which is one of the most important disciplines. People spend most of their time in a digital environment that has now merged with reality itself (Savas & Karata, 2022). For this reason, the dangers of the real world are also found in the digital environment. Almost every institution and every person has experienced a cyberattack, and the number of cybercrimes is constantly increasing. The importance placed on the concept of cybersecurity has increased significantly in recent years due to these attacks and crimes. One of the most important components of cybersecurity is data security in digital contexts. Cybercriminals damage users' business or personal data and systems by infiltrating computers using various techniques such as viruses, worms, Trojans, DDOS attacks, and deception. People need to take precautions to protect their data in cyber environments just as they do for their physical residences, offices, and workplaces. Organizations are trying to implement hardware- and software-based security solutions. They are also implementing workforce development measures to prevent human-caused security issues (Sava, S. & Topaloğlu, 2019). Ethics is another issue at the heart of cybersecurity practices. With so much important data now stored digitally by companies and individuals, potential vulnerabilities in cybersecurity can be quite problematic for both parties. A company or individual's privacy can be compromised. Company secrets can be leaked to the public. Cybersecurity risks can lead to the disclosure of personal information. These factors make the creation of sufficient security and its sustainability a moral issue in itself (Macnish & Ham, 2020).

One of the most important factors in this approach is improving user and employee knowledge. Most cyberattacks today are perpetrated by ignorant users. Humans are often referred to as the "weakest link" in security, as 88 percent of data breaches are due to human error, according to a 2021 Tessian analysis. 43 percent of workers admit to making a mistake in the workplace that negatively impacted their company's security or their security. 25 percent of workers admitted to clicking on a phishing emails in their workplace (Tessian, 2021). To prevent this, companies are investing heavily in cybersecurity, as Figure 2 shows (Statista, 2020).

Figure. 2 Global cybersecurity spending in the period 2017–2020.



The cost of cybersecurity to enterprises worldwide between 2017 and 2020 is shown in Figure 2. By mid-2020, investments have increased to nearly \$ 42 billion. Organizations around the world have had their employees work from home following the outbreak of the COVID - 19 pandemic. The fact that there has been an increase in cyberattacks since the COVID -19 epidemic supports the contention that this decentralization of an organization's IT ecosystem has created new vulnerabilities for criminal actors to exploit. For this reason, business leaders continue to prioritize cybersecurity to ensure business viability and data security (Statista, 2020). The value placed on cybersecurity globally can be understood through these investments.

Management and governance

Gathering resources and performing the task as per organizational structure and goal is another management strategy. The main considerations of this definition can be divided into four categories (Hitt, 2005):

- Management, which includes various activities and actions such as scheduling, decision making, and assessment, is the most important process for an organization.
- In order for management to function, resources are needed. By combining tangible and intangible resources, the goal is achieved. These resources include money, materials, labor, and knowledge.

- Management makes a deliberate effort to achieve its goals. The two key variables in this study are organizational management and human resource management.
- The establishment and functioning of the organization give management the opportunity.

The governance of a socio-political system is described as the structure or order that emerges through the combined efforts of all major actors (Swinton & Hedges, 2020). In terms of democratic ideology and the process of democratization, governance is one of the most controversial issues in recent years. International organizations such as the IMF, EU, OECD, and the World Bank brought governance to the forefront in the 1990s, and it quickly attracted much attention. Although governance spread quickly, it also became the subject of theoretical debates (Boerman, 2020). Participants in governance are actors in society. Governance can be considered as a mechanism of direction and control that develops through the interaction between social, political, and economic actors in a community. Consequently, governance is a process that results from the interaction of multiple actors (Bodeau, 2012).

In the modern society, the term "governance" describes a multifaceted system that comprises of the public sector, the corporate sector, non-governmental groups, and their networks and interactions with each other. It emphasizes the participation of a wide range of actors in the process, including nongovernmental groups, private entrepreneurs, and nonprofit organizations, as well as the institutions of central and local government (Pernice, 2018).

The triangle of participation, openness, and accountability preserves governance. Figure 3. This triangle can also be used to correlate social, economic, and political priorities. Economic development is combined in this agreement.

Figure. 3 scope of the governance

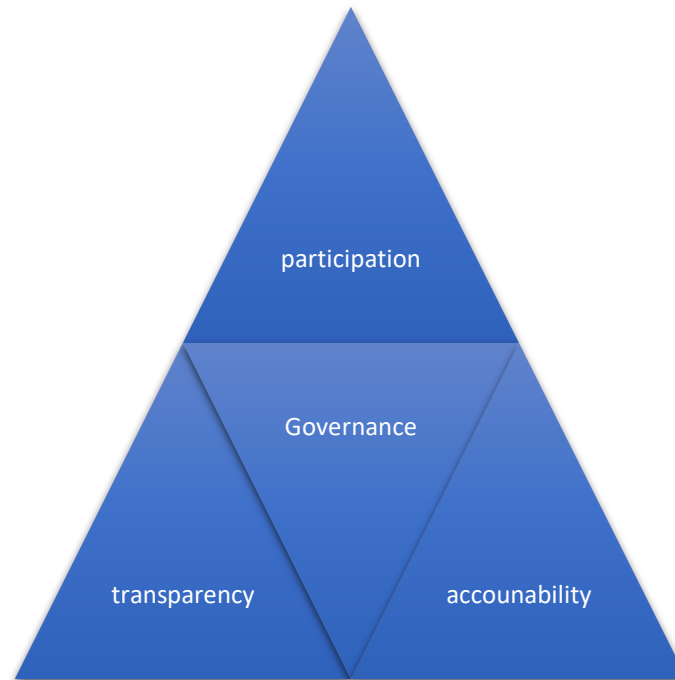
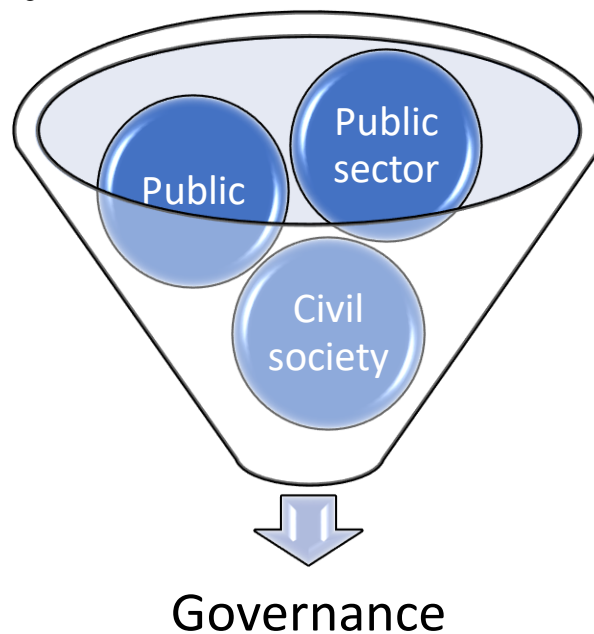


Figure. 4 Social, Economic, and Political Considerations.



The public sector, the commercial sector, civil society, and, the general public are all involved in governance (Figure 4). One of the actors in this process is public organizations, and one of their main concerns is to better serve their constituents. By upholding the rule of law, controlling socioeconomic conditions, creating social and physical infrastructure, and providing social safety nets, governance creates a coherent framework in developing and maintaining equality and justice. The second factor is the private sector, which includes private

companies in numerous industries. By promoting sources of employment and revenue, increasing production, and providing services and business standards, these groups promote economic development and growth (Xu et al., 2021). Thirdly, the civil society acts as the intermediary between the state and the individuals and provides the background for responsibility, equality, and freedom.

Cyber governance

Cyber governance is concerned with the decision making process within the cyber environment that ensures transparency and accountability within the digital environment (Savas & Karata, 2022). One of the most important issues in international relations in recent years has been cyber governance. International organizations have been looking for answers to the problems with cyber governance. The first steps in this direction were taken with the ratification of the Council of Europe's "Cyber Crime Convention" (Calderaro & Craig, 2020). Moreover, this field has adopted global standardization. For example, the ISO /IEC 38500:2015 standard describes organizational or corporate governance as a subset or area of IT governance. These procedures may be managed by internal IT professionals, external service providers, or internal business units (ISO, 2015). Even with these standards, there is still a lack of a framework standard that links cyber governance and cybersecurity as two distinct topics.

SEARCH STRATEGY

The scoping process is a five-step heuristic that includes defining the research topic, locating relevant studies, selecting studies, collecting data, and compiling, summarizing, and reporting results. Figure 1 illustrates the process used to gather evidence for this review. We filtered the “subject area” to social science, computer science, and business “subject category” to all, “region and country” to all, and the “type of publications” to articles and proceedings. Our scoping review covered the period from January 2012 to June 2022.

Table 1. Inclusion and exclusion criteria applied (32)

Inclusion criteria	Exclusion criteria
<ul style="list-style-type: none"> • Papers on cybersecurity governance • English language used • Time period: 2012–2022 	<ul style="list-style-type: none"> • Papers from cybersecurity governance • Book series • Conference Proceeding • Books

Study Selection

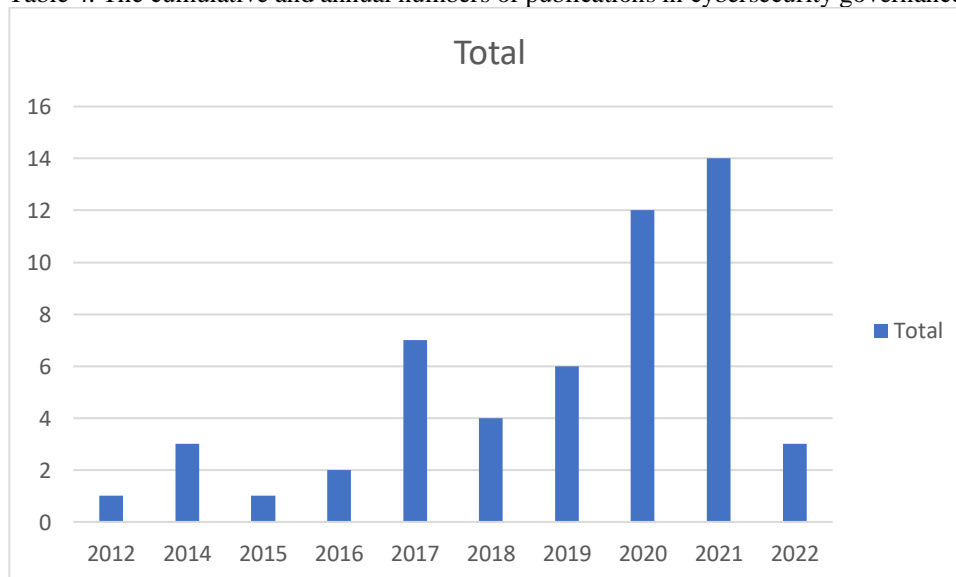
We searched only the Scopus database for our scoping search. This choice was made with at least three factors in mind. First, only a tiny fraction of the peer-reviewed content in Scopus, the largest repository, is in a language other than English (Adam et al., 2019). Data mining was conducted using the Scopus database to find all published studies on the topic. This database is often considered the most thorough compared to other databases because it contains research papers on a wide range of topics (e.g., Web of Science). According to (Abbas et al., 2021, 2022; Ali et al., 2021), Scopus is one of the most comprehensive databases of abstracts and citations for peer-reviewed literature. The Scopus database was selected since it allows searching for articles using predefined keywords, such as those in the title, abstract, or keywords. The sample size at this time was 32 articles. All of these articles were excluded from the final round because they did not address the topic of cybersecurity governance.

RESULT ANALYSIS AND FINDINGS

4.1 Charting the Data

To answer RQ2, First, we assessed the percentage of publications published in the last ten years. The distribution is shown in Figure 2. In 2021, articles increased almost eightfold compared to 2015 and 2016. This indicates that cybersecurity researchers are increasingly interested in thinking about and evaluating governance. Second, we examined the most frequently used expressions over the past decade in the context of the present studies by conducting a full-text analysis of all 32 articles.

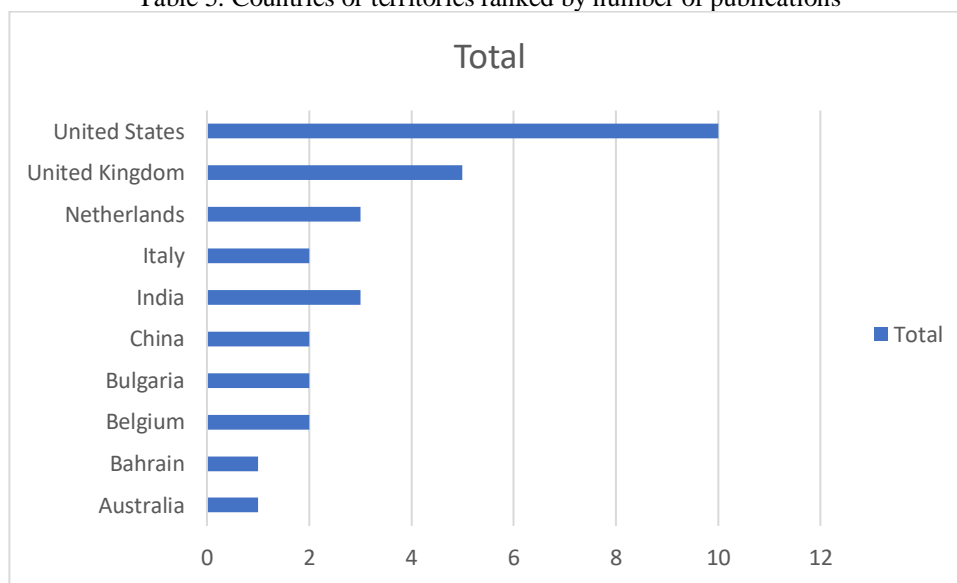
Table 4. The cumulative and annual numbers of publications in cybersecurity governance.



The most productive country for cybersecurity governance

To answer RQ3, The sample documents of this study included 10 countries or territories, of which 5 countries have published more than 2 articles and 5 countries or territories have published at least 2 articles. These countries or territories are listed in figure 5 which shows the total number of documents between countries or territories. It can be seen that the United States contributed the most publications (14) and citations among all the countries or territories. The second place goes with the UK have (6) publications, and the Netherlands and India with (4) publications. China, Bulgaria, and Belgium have (3) publications. Finally, Bahrain and Australia have the lowest publication (2) publications for each one of them.

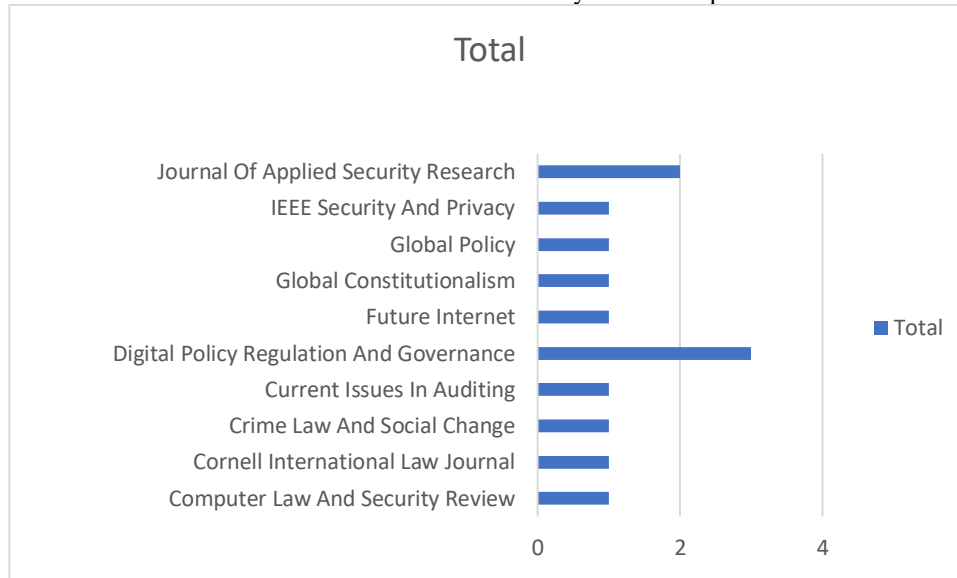
Table 5. Countries or territories ranked by number of publications



The most productive journals in cybersecurity governance

To answer RQ4, In this analysis, as illustrated in Table 6, shows that the most active journal comes from digital policy regulation and governance proceedings with (3 publications), followed by the Journal Of Applied Security Research (2 publications). Journal of IEEE Security And Privacy, Global Policy, Global Constitutionalism, Future Internet, Current Issues In Auditing, Crime Law And Social Change, Cornell International Law Journal, and Computer Law And Security Review comes with 1 publication within 2012-early 2022. The observations indicated that cybersecurity governance is gaining more attention in different fields.

Table 6. Countries or territories ranked by number of publications



The most cited articles in cybersecurity governance

To answer RQ5, The number of citations in the top 10 articles is shown in Table 2. It shows that some articles were the only ones mentioned in certain years. Numerous authors include the exchange of information in numerous areas. This significantly affects the number of citations, especially when cybersecurity outcomes are linked to ideas such as government and technology. Al-Sartawi from 2020, which has the most citations (28) of any year to date, is the most cited article. The second article, written by Shackelford in 2014, was cited (26) times. Other articles were cited on various topics. The fact that the publications provide information and identify the concepts of "cybersecurity" and "governance" as popular research areas in the community suggests that they are important.

Table 2. The most cited articles

Rank	Author	paper	Year	Citations
1	(Al-sartawi, 2020)	"Information technology governance and cybersecurity at the board level"	2020	28
2	(Shackelford et al., 2017)	"Beyond the new "digital divide": Analyzing the evolving role of national governments in Internet governance and enhancing cybersecurity"	2014	26
3	(Mueller, 2017)	"Is cybersecurity eating internet governance? Causes and consequences of alternative framings"	2017	17
4	(Terlizzi et al., 2017)	Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance	2017	8
5	(Calderaro & Craig, 2020)	"Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building"	2020	7
6	(Peng, 2018)	"Private" cybersecurity standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime"	2018	7
7	(Auffret et al., 2017)	"Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems"	2017	6

8	(Wolff, 2016)	“What we talk about when we talk about cybersecurity: Security in internet governance debates”	2016	6
9	(Carr & Lesniewska, 2020)	“Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance”	2020	5
10	(Pernice, 2018)	“Global cybersecurity governance: A constitutionalist analysis”	2018	5

DISCUSSION

The importance of policies and initiatives that set regional, global, and national standards for managing cyber environments continues to grow. There is still a democratic divide in how people use the Internet for civic engagement, even though the digital divide is narrowing as the Internet spreads (Fierro et al., 2020). Numerous studies have emphasized the use of a governance model under the concept of "governance" that includes a free-form and participatory technology that involves all stakeholders.

The literature review on cybersecurity governance has shown that states and international organizations have not yet made sufficient progress toward cybersecurity governance. The studies have generally dealt with widely held concepts and specific studies. This shows that cybersecurity governance is increasingly becoming more important with the increasing use of the Internet.

In our review of the literature, the study found that most previous studies were based on single or multi-country studies and were conducted mainly in developed and developing countries. The United States, the United Kingdom, the Netherlands, Italy, China, and India are single nations. This paper makes clear that we have attempted to provide the preliminary framework for evaluating the cybersecurity paradigm from a governance perspective. As far as we can tell, there have not been many attempts of this type in the recent literature. In the absence of prior research that would have provided us with further guidance, we were compelled to conduct a review study while keeping in mind the overarching research questions.

The results show that the last articles published argued different perspectives on cybersecurity governance. According to (Al-sartawi, 2020), his research combines two important areas, ITG and cybersecurity, to provide a new topic for the literature on the MENA region. Regulators, policymakers, and governments in the region are interested in this study. It would also be of interest to the global investment community. In addition, this report provides useful input that shareholders might find helpful in selecting board members or establishing technology/cyber committees. To control cyber threats and the resulting legal consequences of data breaches, companies should take a proactive approach and ensure against security breaches. In addition, organizations should conduct an annual risk self-assessment to understand their cyber environment and gain a comprehensive understanding of their risk

profile (Hoffmann et al., 2020). Because boards must first have a clear understanding of their organization's risk profile, they are then able to manage their risks. Similarly, Boyes (2015) argues that while organizations cannot completely prevent cyberattacks, they can create the necessary plans and procedures to thwart some attacks and mitigate the risks of others.

Moreover, the paper (Mueller, 2017) has shown how important Internet connectivity is to any notion of cyberspace. This highlights the close relationship between Internet governance and cybersecurity governance. It has been noted that cybersecurity governance may indeed diverge from Internet governance and push Internet governance in a more nationalistic or state-centric direction because of these close interdependencies. However, the opposite is also possible: cybersecurity governance can be significantly shaped by the models and standards created for Internet governance.

From technical and policy perspectives, Calderaro & Craig (2020) explain that Internet availability is growing across nations, regions, and socio-political contexts as a result of the continued expansion of connectivity infrastructure. The need to expand cyber capabilities beyond national contexts and to develop a transnational, coherent and coordinated governance approach to cybersecurity arises from the rapidly changing physical geography of the Internet. Cyber capacity initiatives are gaining prominence in international discussions in this situation, with the goal of helping developing countries in the Global South develop their cybersecurity strategy. The study addressed the main explanations for government initiatives to develop their cyber capabilities. The findings contradict cybersecurity theories originating in international relations (IR), which assume that nations build their cyber capabilities in response to challenges to their external security, domestic policies, or international norms.

From a financial services perspective, (Terlizzi et al., 2017) analyzed the five key controls and governance mechanisms that the financial services sector employs to protect data, namely (a) incorporating the National Institute of Standards and Technology framework into its cybersecurity governance model, (b) establishing policies governing the use of information assets, (c) establishing a code of conduct for its employees, (d) developing a corporate security culture, and (e) maintaining corporate security management.

From a global internet perspective, an article by (Shackleford & Craig, 2014) analyses Critical infrastructure regulations that have been proposed and implemented in China, the European Union, India, the United Kingdom, and the United States. It was conceivable to start the process of finding best practises that could result in standards and eventually be included into customary international law by contrasting and comparing these regulations. Finally, the article demonstrates that there is a continuum of state interests and opportunities to regulate

cyberspace that eliminates the "digital divide" and highlights the importance of focusing on international cooperation. The international community will not be able to agree on the future of Internet governance or advance cyber peace if this is not accomplished. Our society and daily lives are becoming increasingly dependent on the security of the Internet, and cybersecurity, due to the advancement of digitization and the use of especially the Internet of Things and artificial intelligence by industry, commerce, financial services, science and education, public administration, health care, and individuals. For this reason, the essay (Pernice, 2018) intends to examine the tools and procedures of cybersecurity governance in general, drawing lessons from Internet governance and taking a constitutional perspective. It builds on a system of inclusive global rulemaking that includes public engagement, shared accountability, and resilience. A new framework for global rule-making would emerge in line with the ideas of global constitutionalism as a democratic tool for people to address common problems in addition to and complementary to cybersecurity measures at the local, regional, national, and supranational levels. In addition, (Wolff, 2016) looks at how different stakeholders define and shape cybersecurity challenges in the context of governance discussions. He then analyses how these divergent views on security continue to generate new disputes.

The World Economic Forum has identified the "Fourth Industrial Revolution," which unifies the biological, digital, and physical domains. The introduction of the Internet of Things (IoT) is key to this revolution. As a result, new connections will emerge that will test established relationships and governance structures. Carr & Lesniewska (2020) note that improvements in global climate governance appear to provide a prototype for a consensus rules-based strategy within the current international system that pushes for cybersecurity governance. The importance of strong knowledge-sharing systems, particularly between the technical and policy sectors, is perhaps one of the most important lessons we can learn from climate governance.

RECOMMENDATIONS

The scale of life in cyberspace is best illustrated by the fact that even the number of users of major social media platforms is now in the hundreds of millions. Take Facebook, for example, with its estimated 2.5 billion users from around the world. With increasing technological advancements, there will be a scope that will push the boundaries of thinking about the dimensions of cyberspace. The struggle for management and control in these circumstances continues today, just as there have been conflicts between nations throughout history.

To conduct business and transactions securely, establish institutions, and sustain life in cyber environments, which is an essential aspect of existence, a common understanding and governance structure are needed. Individuals, individual institutions, or individual states cannot decide on this framework. We need the support of all international organizations that have legal and treaty obligations. There may be a technical deficit, even if the policies that these organizations decide for themselves are usually valid. Therefore, the concept of democracy should include the views of all interested parties.

The application of theory is another area where current research is inadequate. It is important to study and understand the various connections and interactions that exist between cybersecurity systems and their users using the right theories. Grounded theories can be a good starting point, as qualitative methods are prevalent in this area of study. In addition to interviews, ethnography or netnography could also be used to study human interactions. In this context, the usability of cybersecurity systems is also a neglected issue, and efforts need to focus on developing some standardized measurement methods to determine the perception of human security. At the academic level, multidisciplinary approaches are critical. By bringing together experts in computer science, engineering, economics, diplomacy, and law, we can deepen the technical and policy conversations in practice. The problem of our time will be how to do this successfully, and success will have a greater impact on global cyber (in)security than any technical advance by itself.

REFERENCES

- Abbas, A. F., Jusoh, A., Mas, A., Alsharif, A. H., & Ali, J. (2022). Bibliometrix analysis of information sharing in social media. *Cogent Business & Management*, 9(1). <https://doi.org/10.1080/23311975.2021.2016556>
- Abbas, A. F., Jusoh, A., Masod, A., Ali, J., Ahmed, H., & E, A. R. H. (2021). A Bibliometric Analysis of Publications on Social Media Influencers Using Vosviewer. *Journal of Theoretical and Applied Information Technology*, 99(23), 5662–5676.
- Adam, I., Jusoh, A., & Streimikiene, D. (2019). Scoping research on sustainability performance from manufacturing industry sector. *Problems and Perspectives in Management*, 17(2). [https://doi.org/10.21511/ppm.17\(2\).2019.10](https://doi.org/10.21511/ppm.17(2).2019.10)
- Al-sartawi, A. M. A. M. (2020). Information technology governance and cybersecurity at the board level. *Int. J. Critical Infrastructures*, 16(2), 150–161.
- Ali, J., Jusoh, A., & Abbas, A. F. (2021). Thirty- Eight Years of ‘ Wellbeing ’ Research : Bibliometric Analysis of Open Access Documents . *Studies of Applied Economics*, October, 1–11. <https://doi.org/10.25115/eea.v39i10.5412>

- Aslay, F. (2017). Siber Attack Methods and Current Situation Analysis of Turkey's Cyber Safety. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24–28.
- Auffret, J., Kelley, D., & Warweg, P. (2017). Cybersecurity Leadership : Competencies , Governance , and Technologies for Industrial Control Systems. *Journal of Interconnection Networks*, 17(1), 1–20. <https://doi.org/10.1142/S0219265917400011>
- Bakanlıđı. (2013). *National Cyber Security Strategy and 2013–2014 Action Plan*. Information Technologies and Communication Authority.
- Barnes, S. J., & Pressey, A. D. (2011). Who needs cyberspace? Examining drivers of needs in Second Life. *Internet Research*, 21(3), 236–254. <https://doi.org/10.1108/10662241111139291>
- Blazevic, V., Wiertz, C., Cotte, J., De Ruyter, K., & Keeling, D. I. (2014). GOSIP in cyberspace: Conceptualization and scale development for general online social interaction propensity. *Journal of Interactive Marketing*, 28(2), 87–100. <https://doi.org/10.1016/j.intmar.2013.09.003>
- Bodeau, D. (2012). Cyber security governance: A component of MITRE's cyber prep methodology. *Washington: MITRE Corporation., September*.
- Boerman, D. (2020). *Reporting on Cybersecurity Performance*. University of Twente.
- Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*, 5(4), 28–34. <https://doi.org/10.22215/timreview888>
- Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity : policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 0(0), 1–22. <https://doi.org/10.1080/01436597.2020.1729729>
- Carr, M., & Lesniewska, F. (2020). Internet of Things , cybersecurity and governing wicked problems : learning from climate change governance. *International Relations*, 34(3), 391 –412. <https://doi.org/10.1177/0047117820948247>
- Colquhoun, H. L., Levac, D., Brien, K. K. O., Straus, S., Tricco, A. C., Perrier, L., Kastner, M., & Moher, D. (2014). Scoping reviews : time for clarity in definition , methods , and reporting. *Journal of Clinical Epidemiology*, 67(12), 1291–1294. <https://doi.org/10.1016/j.jclinepi.2014.03.013>
- Cope, S., Leishman, F., & Starie, P. (1997). Globalization , new public management and the Futures of police management. *Intl Jnl Public Sec Management*, 10(6), 444–460.
- Çözümlemler, P. (2019). *Siber Güvenlik ve Savunma: Problemler ve Çözümlemler* (Vol. 06520).
- Culver, C. A. (2022). Manipulating Remittances: Strengthening Autocratic Regimes with Currency Overvaluation and Remittance Flows. *Remittances Review*, 7(1), 21–47.
- 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. *Technology in*

Society, 101432. <https://doi.org/10.1016/j.techsoc.2020.101432>

Hitt. (2005). *Management*. Prentice Hall Inc.

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, 44(2019), 655–662. <https://doi.org/10.1016/j.promfg.2020.02.243>

ISO. (2015). *Iso/iec 38500:2015 information technology | governance of it for the organization*.
Levac, D., Colquhoun, H., & Brien, K. K. O. (2010). Scoping studies : advancing the methodology. *Implementation Science*, 5(1), 1–9.

Macnish, K., & Ham, J. Van Der. (2020). Technology in Society Ethics in cybersecurity research and practice. *Technology in Society*, 63(December 2019), 101382. <https://doi.org/10.1016/j.techsoc.2020.101382>

Mueller, M. (2017). Is Cybersecurity Eating Internet Governance ? Causes and Consequences of Alternative Framings. *Digital Policy, Regulation and Governance*, 19(6), 415–428.

NATO. (2020). *Warsaw Summit Communiqué*. North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/official_texts_13316

Peng, S. (2018). “ Private ” Cybersecurity Standards? Cyberspace Governance , Multistakeholderism , and the (Ir) relevance of the TBT Regime. *Cornell International Law Journal*, 51(2).

Pernice, I. (2018). Global cybersecurity governance : A constitutionalist analysis. *Global Constitutionalism*, 7(1), 112–141. <https://doi.org/10.1017/S2045381718000023>

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human Factors in Cybersecurity : A Scoping Review Human Factors in Cybersecurity: A Scoping Review. *IAIT, July*. <https://doi.org/10.1145/3468784.3468789>

Sahi, A. M., Khalid, H., Abbas, A. F., & Khatib, S. F. A. (2021a). The Evolving Research of Customer Adoption of Digital Payment : Learning from Content and Statistical Analysis of the Literature. *J. Open Innov. Technol. Mark. Complex*, 1–25.

Sahi, A. M., Khalid, H., Abbas, A. F., & Khatib, S. F. A. (2021b). The evolving research of customer adoption of digital payment: Learning from content and statistical analysis of the literature. *Journal of Open Innovation: Technology, Market, and Complexity*, 7(4), 1–25. <https://doi.org/10.3390/joitmc7040230>

Sava, S., & Topaloğlu, N. (2019). Data analysis through social media according to the classified crime. *Turkish Journal of Electrical Engineering and Computer Sciences*, 27(1), 407–420. <https://doi.org/10.3906/elk-1712-17>

Savas, S., & Karata, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *Int. Cybersecur. Law Rev*, 3, 7–34.

Shackelford, S. J., Sulmeyer, M., Deckard, A. N. C., Buchanan, B., & Micic, B. (2017). From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and

What to Do about It. *Nebraska Law Review*, 96(2).

Shackleford, S., & Craig, A. (2014). Beyond the New ' Digital Divide ': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity. *World Conference on International Telecommunication*, 119(290).

Statista. (2020). *Spending on cybersecurity worldwide from 2017 to 2020*. Statista.

Swinton, S., & Hedges, S. (2020). *Cybersecurity Governance, Part 1: 5. Fundamental Challenges*. <https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html>

Terlizzi, M. A., Meirelles, F. D. S., & Alexandra, M. (2017). Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance. *Journal of Applied Security Research*, 12(2), 224–252. <https://doi.org/10.1080/19361610.2017.1277886>

Tessian. (2021). *The psychology of human error*. <https://www.tessian.com/research/the-psychology-of-human-error/>

Wolff, J. (2016). What we talk about when we talk about cybersecurity : security in internet governance debates. *INTERNET POLICY REVIEW*, 5(3), 1–13. <https://doi.org/10.14763/2016.3.430>

Xu, Z., Ge, Z., Wang, X., & Skare, M. (2021). Technological Forecasting & Social Change Bibliometric analysis of technology adoption literature published from 1997 to 2020. *Technological Forecasting & Social Change*, 170(March), 120896. <https://doi.org/10.1016/j.techfore.2021.120896>