Smart Society : Community Service and Empowerment Journal
Volume 6, Issue 2, 223-241.
e_ISSN: 2807-5757
https://www.journal.foundae.com/index.php/smartsoc/index

Cybersecurity Policy Research in the Social Sciences: A Systematic Literature Review and Bibliometric Analysis

Refa Andrean Tri P.*
Sebelas Maret University
INDONESIA

Ismi Dwi Astuti Nurhaeni
Sebelas Maret University
INDONESIA

Faizatul Ansoriyah
Sebelas Maret University
INDONESIA

Article Info

Article history:

Received: March 18, 2026
Revised: June 15, 2026
Accepted: June 27, 2026

Keywords:

Bibliometric Analysis;
Conceptual Model;
Cybersecurity Policy;
Social Sciences;
Systematic Literature Review.

Abstract

The global digital transformation has positioned cybersecurity policy as a strategic issue within the social sciences rather than merely a technical concern. Although cybersecurity has been widely examined in technical, engineering, and information systems domains, studies that systematically map cybersecurity policy research from a social science perspective remain limited and fragmented across governance, regulatory, institutional, and socio-political dimensions. Therefore, a comprehensive synthesis is needed to better understand the development, intellectual structure, and future directions of cybersecurity policy scholarship within the social sciences. This study aims to map the development of cybersecurity policy research, identify publication patterns based on countries, institutions, sources, and publication types, and synthesize the key determinants and social dimensions associated with cybersecurity policy. The study employs a Systematic Literature Review and a bibliometric analysis of 70 Scopus-indexed articles published up to March 17, 2026. The findings reveal a substantial increase in cybersecurity policy research over the past decade, particularly in studies related to governance, regulation, and geopolitical issues, reflecting a growing multidisciplinary orientation. The thematic synthesis and literature analysis identify five key determinants of cybersecurity policy and several social, political, and economic dimensions frequently associated with cybersecurity governance. These findings are integrated into a conceptual model developed from literature synthesis and bibliometric mapping to illustrate the relationships among the identified determinants and associated dimensions. This study contributes to enriching the cybersecurity policy literature from a social science perspective and provides directions for future research and policy development.

To cite this article: Tri P., R. A., Nurhaeni, I. D. A., & Ansoriyah, F. (2026). Cybersecurity Policy Research in the Social Sciences: A Systematic Literature Review and Bibliometric Analysis. *Smart Society: Community Service and Empowerment Journal, 6*(2), 223-241. https://doi.org/10.58524/smartsociety.v6i2.1275

INTRODUCTION

According to the United Nations E-Government Survey, the adoption of digital governance and digital public services has expanded substantially across countries over the past decade, with governments increasingly integrating digital technologies into public administration, service delivery, and citizen engagement. This rapid expansion of digital governance has transformed the way governments, institutions, and societies interact in the contemporary era. Alongside these developments, cybersecurity issues have increasingly become a major concern within the social sciences because digital systems are now closely connected to governance processes, public administration, economic activities, and citizen participation (Veale & Brown, 2020). The growing dependence on digital infrastructure has also encouraged broader discussions regarding the role of

* **Corresponding author:**
Refa Andrean Tri P, Sebelas Maret University, INDONESIA. ✉ refa.andrean@student.uns.ac.id

public policy, institutional resilience, and governance capacity in addressing cyber-related risks (Carrapico & Farrand, 2020).

The increasing intensity of global cyber threats demonstrates that cybersecurity is no longer limited to technical system protection, but has become a multidimensional governance challenge. Cyberattacks targeting public institutions, financial systems, and digital public services continue to increase in complexity and scale across countries. Recent global reports indicate a sustained rise in cyber incidents, with ransomware attacks, data breaches, and attacks on critical infrastructure becoming increasingly frequent and sophisticated. For example, the IBM Cost of a Data Breach Report 2024 reported that the global average cost of a data breach reached USD 4.88 million, the highest level recorded to date, highlighting the growing economic and operational consequences of cyber threats. These developments demonstrate that cybersecurity is no longer limited to technical system protection but has become a multidimensional governance challenge (Farrand et al., 2024; Holt et al., 2023). Recent studies also show that cybercrime and vulnerabilities in digital infrastructure generate substantial economic, institutional, and social consequences (He, 2024; Ribeiro et al., 2025). In the public sector, weak cybersecurity governance may reduce public trust, disrupt service delivery, and weaken the effectiveness of digital transformation initiatives (Kosasih et al., 2025). These conditions indicate that cybersecurity policy has become an increasingly strategic issue in ensuring the sustainability of digital governance systems.

The urgency of cybersecurity policy studies has become even more relevant in the context of sustainable development and digital governance transformation. Cybersecurity governance contributes directly to the achievement of the Sustainable Development Goals (SDGs), particularly SDG 9 and SDG 16. In relation to SDG 9, which emphasizes resilient infrastructure, innovation, and technological development, effective cybersecurity governance helps protect critical digital infrastructure, ensure the reliability of digital services, and support the secure adoption of emerging technologies. Strong cybersecurity frameworks reduce vulnerabilities that may disrupt digital innovation and economic activities, thereby strengthening the sustainability of digital transformation initiatives. Furthermore, cybersecurity governance contributes to SDG 16, which promotes effective, accountable, and inclusive institutions, by enhancing the security, integrity, and reliability of digital public services. Effective cybersecurity policies support institutional resilience against cyber threats, protect sensitive public data, strengthen public trust in government systems, and improve the capacity of public institutions to deliver secure and accountable services. As digital governance continues to expand, cybersecurity policy has become increasingly important for ensuring both sustainable technological development and resilient public institutions.

The ability of governments and institutions to develop adaptive cybersecurity policies is increasingly essential for maintaining institutional stability, protecting digital infrastructures, and supporting sustainable public service transformation in the digital era (Mishra et al., 2022; Sterlini et al., 2020). Consequently, cybersecurity policy discussions require broader social science perspectives that consider governance dynamics, institutional adaptation, behavioral dimensions, and public policy responses.

Previous studies have examined cybersecurity from various perspectives, including cybersecurity regulation and legal frameworks (Fuster & Jasmontaite, 2020; Verhelst & Wouters, 2020), national cybersecurity governance (Baezner, 2020; Kaponig, 2020), cybersecurity behavior and organizational compliance (Okigui et al., 2024; Saeed, 2023), cyber resilience (Shkolnyk et al., 2025), and cybersecurity policy development (Mishra et al., 2022). In addition, several studies have utilized bibliometric and review approaches to map cybersecurity-related research trends and thematic developments (Barcellos-Paula et al., 2025; Ben Mamia et al., 2025). These studies provide important insights into the development of cybersecurity discussions across disciplines.

However, the existing literature still demonstrates several important limitations. First, many previous studies predominantly focus on technical, organizational, or sector-specific cybersecurity issues rather than examining cybersecurity policy as a broader social science research domain (Lang, 2025). Second, existing bibliometric studies predominantly focus on cybersecurity research from information technology, engineering, and information systems perspectives. For example, previous reviews have shown that the most frequently examined themes are network security, cyber threats, information security, technical risk mitigation, and cyber defense mechanisms, while comparatively limited attention has been given to cybersecurity policy, governance, regulatory frameworks, and

public administration issues (Barcellos-Paula et al., 2025). As a result, studies that specifically map cybersecurity policy discussions within public policy and governance scholarship remain relatively limited, leaving important questions regarding institutional adaptation, policy development, and governance responses insufficiently explored. Third, prior studies have not sufficiently integrated systematic literature synthesis and bibliometric mapping to comprehensively identify the intellectual structure, thematic evolution, theoretical implications, and future research directions of cybersecurity policy studies in the social sciences (Gan et al., 2022; Oliveira & Baldi, 2022). As a result, the research landscape on cybersecurity policy remains fragmented across disciplines, with studies differing substantially in their thematic focus, theoretical foundations, methodological approaches, and contextual settings (Lang, 2025) Existing research is dispersed across fields such as computer science, information systems, law, public policy, governance, and international relations, often examining cybersecurity from isolated perspectives. Consequently, limited integration exists among technical, institutional, regulatory, and socio-political dimensions, resulting in a fragmented understanding of how cybersecurity policy is developed, implemented, and evaluated across different governance contexts.

Considering these limitations, a more comprehensive synthesis is necessary to better understand the development trajectory and research direction of cybersecurity policy studies in the social sciences. A systematic mapping of the literature is important not only to identify dominant themes and publication trends, but also to reveal underexplored issues within cybersecurity policy research. Existing studies have largely concentrated on technical security measures, cyber threats, regulatory frameworks, and national cybersecurity strategies, while comparatively less attention has been devoted to policy agility, institutional adaptation, sociotechnical governance, and behavioral dimensions (Afshari-Mofrad et al., 2024; Ben Mamia et al., 2025). These areas remain underexplored because they require interdisciplinary perspectives that integrate governance, organizational, technological, and social considerations, which are often examined separately across different fields of study. Nevertheless, these issues are increasingly important in the contemporary digital environment. Policy agility is essential for enabling governments to respond effectively to rapidly evolving cyber threats, institutional adaptation influences the capacity of organizations and public institutions to implement cybersecurity measures, sociotechnical governance highlights the interaction between technological systems and governance arrangements, and behavioral dimensions help explain how human attitudes, awareness, and compliance affect cybersecurity outcomes. Therefore, a comprehensive mapping of the literature is needed to better understand how these interconnected dimensions contribute to the development and effectiveness of cybersecurity policy. Such efforts are essential for strengthening evidence-based policymaking and encouraging interdisciplinary collaboration in addressing increasingly complex cybersecurity challenges.

Accordingly, this study aims to examine the landscape and development trajectory of cybersecurity policy research within the social sciences and to assess its sustainability as a future research agenda. This study also seeks to identify dominant research themes, intellectual structures, and emerging policy discussions related to cybersecurity governance. The research questions addressed in this study are as follows:

RQ1: Is the exploration of cybersecurity policy a subject that has potential significance for future social science research?
RQ2: How is the current allocation of research investigations related to cybersecurity policy in the study of social sciences?
RQ3: What are the theoretical and practical implications from the perspective of cybersecurity policy research in the field of social sciences in the future?

This study contributes academically by strengthening discussions on cybersecurity policy within public policy and digital governance scholarship, particularly regarding adaptive governance, institutional resilience, and evidence-based policymaking in the digital era. Practically, the findings are expected to support policymakers, researchers, and public institutions in developing more adaptive and collaborative cybersecurity governance strategies. In addition, this study offers several novel contributions compared with previous review and bibliometric studies on cybersecurity. Existing bibliometric reviews have predominantly focused on technical cybersecurity, information systems, business cybersecurity, or human-factor security issues, while relatively limited attention

has been given to cybersecurity policy as a distinct area of inquiry within the social sciences. Unlike previous studies, this research specifically examines cybersecurity policy from governance, public policy, and institutional perspectives. Furthermore, by integrating Systematic Literature Review (SLR) and bibliometric analysis, this study not only maps publication trends and intellectual structures but also synthesizes key determinants, identifies broader social dimensions associated with cybersecurity policy, and develops a conceptual model based on literature synthesis and bibliometric evidence. These contributions provide a more comprehensive understanding of the evolution, thematic development, and future research agenda of cybersecurity policy studies within the social sciences.

Literature Review

In social science scholarship, cybersecurity policy is increasingly understood not merely as a technical regulatory instrument, but as a multidimensional governance issue shaped by institutional arrangements, political interests, and socio-digital transformations. Existing studies show that cybersecurity policy reflects how states construct authority, coordinate actors, and manage risks within the digital environment (Fuster & Jasmontaite, 2020; Napetvaridze & Chochia, 2019). From the perspective of governance theory, cybersecurity policy involves complex interactions among governments, private sectors, institutions, and society in responding to rapidly evolving cyber threats (Kaponig, 2020; Malatji et al., 2021). This perspective positions cybersecurity governance as part of adaptive and collaborative governance frameworks, where policy effectiveness depends not only on legal regulation, but also on institutional coordination capacity and inter-organizational cooperation.

The relevance of institutionalism in cybersecurity policy analysis can also be observed through the role of state capacity and institutional adaptation in managing cyber risks. Previous studies suggest that cybersecurity governance is closely related to digital state capacity, particularly in terms of regulatory responsiveness, institutional resilience, policy coordination, and strategic resource allocation (Mishra et al., 2022; Ribeiro et al., 2025). In this regard, cybersecurity policy is not simply intended to protect digital systems, but also to strengthen the legitimacy and effectiveness of governance institutions in the digital era. Therefore, the development of cybersecurity policy can be understood as part of broader transformations in public policy and digital governance structures.

A number of studies further emphasize that the formation and transformation of cybersecurity policy are strongly influenced by threat construction and political momentum. Major cyberattacks often function as critical junctures that encourage institutional reform and redefine the role of the state in digital security governance (Gao, 2024; Napetvaridze & Chochia, 2019). The increasing economic and political consequences of cybercrime also shape policy priorities, national security agendas, and public resource allocation (He, 2024; Ruvin et al., 2020). However, previous literature tends to frame cyber threats predominantly through security and technical lenses, while relatively limited attention has been given to how cyber threats are socially and politically constructed through governance narratives, institutional discourse, and policy negotiations. As a result, cybersecurity policy discussions often overlook broader socio-political dimensions that influence policymaking processes.

From a socio-political perspective, cybersecurity policy effectiveness is also shaped by the interaction between public opinion, organizational culture, and institutional compliance. Public perceptions of cyber threats significantly influence public acceptance of stricter cybersecurity regulations, including state intervention and surveillance mechanisms (Snider et al., 2021). At the same time, organizational culture and institutional awareness determine how cybersecurity policies are implemented in practice. Several studies reveal that the existence of formal cybersecurity regulations does not automatically guarantee effective implementation because policy outcomes are strongly influenced by resource availability, institutional commitment, awareness levels, and compliance cultures (Norris et al., 2018; Okigui et al., 2024; Wadesango & Maveneka, 2025). This indicates that cybersecurity policy effectiveness should be understood as a socio-institutional process involving interactions among governance capacity, organizational behavior, and public legitimacy, rather than merely as the implementation of normative regulatory frameworks.

The challenges of cybersecurity governance become more complex in developing countries, where institutional capacity, technological infrastructure, and resource availability are often uneven.

For example, studies in Indonesia highlight challenges related to fragmented institutional coordination, regulatory uncertainty, and limited cybersecurity capacity in supporting digital governance initiatives (Imran et al., 2024). Similarly, research in South Africa identifies difficulties in implementing cybersecurity policies due to resource constraints, uneven technological readiness, and institutional limitations across critical sectors (Malatji et al., 2021). These challenges illustrate how gaps in institutional capacity and cybersecurity preparedness may hinder the effective implementation of cybersecurity policies, reduce organizational resilience, and increase vulnerability to evolving cyber threats. Therefore, cybersecurity policy discussions require contextual perspectives that consider differences in governance capacity, institutional maturity, and socio-political conditions across countries.

Several studies indicate that developing countries frequently face difficulties in implementing adaptive cybersecurity policies due to limited technical expertise, fragmented institutional coordination, financial constraints, and dependence on external technologies (Imran et al., 2024; Malatji et al., 2021). In addition, the rapid expansion of digital public services in many developing countries is not always accompanied by adequate cybersecurity readiness and governance mechanisms. This condition creates vulnerabilities that may weaken public trust and reduce the effectiveness of digital transformation initiatives. Therefore, cybersecurity policy discussions require contextual perspectives that consider differences in governance capacity, institutional maturity, and socio-political conditions across countries.

Furthermore, cybersecurity policy develops within broader contexts of global interdependence and international political dynamics. Regional cooperation, public–private partnerships, and cross-border institutional collaboration have become increasingly important in strengthening cyber resilience and collective digital security governance (Baezner, 2020; Kaponig, 2020). Cybersecurity issues are also closely associated with geopolitical competition, technological sovereignty, and strategic contestation among states (Farrand et al., 2024; Górka, 2022). Consequently, cybersecurity policy can be understood not only as a technical or administrative policy domain, but also as an evolving arena of governance where political interests, institutional adaptation, global cooperation, and digital power relations continuously interact. From this perspective, cybersecurity governance represents an integral component of contemporary digital governance transformation within the social sciences.

Based on the previous discussion, cybersecurity policy can be understood as a multidimensional governance construct shaped by institutional, technological, legal, behavioral, and geopolitical factors. Prior studies have proposed various defining dimensions that determine the effectiveness and orientation of cybersecurity policy implementation. A synthesis of these defining factors is presented in Table 1.

Table 1. Defining Factors That Determine Cybersecurity Policy

No	Defining Factors That Determine Cybersecurity Policy	References
1	Cybersecurity policies include comprehensive regulation, data and network protection, privacy assurance, cybercrime countermeasures, and effective response capacity to increased cyber threats.	(Mishra et al., 2022)
2	Cybersecurity policies include comprehensive regulations, periodic security evaluations, proactive governance, infrastructure assessments, capacity investments, and guidelines that are aligned with international standards.	(Ribeiro et al., 2025)
3	Cybersecurity policies include a strong national strategy, information system protection, cyber attack prevention, strengthening security posture, and workforce development through education and career incentives.	(Holt et al., 2023)
4	Cybersecurity policies include clarity of roles and responsibilities, incident response plans, access controls, data protection, and efforts to maintain the integrity and confidentiality of digital assets.	(Alhumud et al., 2023)
5	Cybersecurity policies include a regulatory framework that ensures data confidentiality, integrity, and availability, stakeholder collaboration, privacy protection, and organizational implementation and compliance.	(Okigui et al., 2024)
6	Cybersecurity policies include proactive measures to deal with technological change, a comprehensive understanding of system and data protection, adaptive governance, and innovative strategies against digital threats.	(Charlet & King, 2020)
7	Cybersecurity policies include regulatory sovereignty and control, reducing dependence on external technologies, strengthening supply chains, and integrating security, economic, and geopolitical considerations.	(Farrand et al., 2024)

8	Cybersecurity policies include legal mechanisms and cost incentives, user-based prevention, collaboration between stakeholders, and the management of interdependent risks and evolving digital vulnerabilities.	(Wang et al., 2020)
9	Cybersecurity policy includes a comprehensive legal framework, strategic action plans, the establishment of specialized agencies, and adaptive responses to cyber threats to maintain national security.	(Napetvaridze & Chochia, 2019)
10	Cybersecurity policies include internal–external security integration, cross-sector collaboration, preventive and proactive approaches, and solidarity-based preparedness, detection, response, and recovery mechanisms.	(Sterlini et al., 2020)

Source: Processed by Researcher 2026

METHOD

This study employed a Systematic Literature Review (SLR) combined with bibliometric analysis to comprehensively examine the development of cybersecurity policy research within the social sciences. The SLR approach was used to systematically identify, evaluate, and synthesize relevant studies, while bibliometric analysis was utilized to map publication trends, intellectual structures, collaboration patterns, and thematic developments within the research field (Barrington et al., 2024; Soni, 2025). Specifically, this study applied performance analysis and science mapping approaches in bibliometric analysis. Performance analysis was conducted to identify publication productivity, influential authors, sources, and publication trends, whereas science mapping was used to visualize relationships among keywords, authors, and research themes through network analysis (Gan et al., 2022; Mering, 2017).

The bibliometric analysis was conducted using VOSviewer version 1.6.20, which enables the visualization of co-authorship networks, keyword co-occurrence, citation relationships, and thematic clustering within scientific publications (Al Husaeni & Nandiyanto, 2022; Malmqvist et al., 2019). The use of bibliometric mapping is particularly relevant for identifying the intellectual structure and research dynamics of cybersecurity policy studies in the social sciences.

This study adopted the PRISMA framework to ensure transparency, systematic procedures, and reproducibility in article identification and selection processes (Barrington et al., 2024; Soni, 2025). The PRISMA stages consisted of identification, screening, eligibility assessment, and inclusion. During the identification stage, articles were retrieved from the Scopus database on March 17, 2026. Scopus was selected as the primary database because it provides broad multidisciplinary coverage, high-quality indexed publications, standardized metadata, and strong compatibility with bibliometric software compared to several alternative databases such as Web of Science or Dimensions (Al Husaeni & Nandiyanto, 2022; Gan et al., 2022). In addition, Scopus is widely recognized in bibliometric studies due to its consistency in citation indexing and metadata export features.

The search strategy was designed using Boolean operators to improve transparency and reproducibility in the literature retrieval process. The search query applied in the Scopus database was:

> TITLE-ABS-KEY (“cybersecurity policy” OR “cyber governance” OR “digital security policy” OR “cyber regulation”)

The keyword “cybersecurity policy” was selected as the primary search focus because it directly represents governance and policy dimensions within cybersecurity discussions. However, several related terms such as “cyber governance,” “digital security policy,” and “cyber regulation” were also included to broaden search coverage and minimize the exclusion of conceptually relevant studies. The search was limited to publications within the Social Sciences subject area to maintain consistency with the focus of this study.

The publication period was restricted to 2015–2026 because significant developments in cybersecurity governance, digital transformation, and global cyber policy discussions accelerated after 2015, particularly following the rapid expansion of digital public services, increasing cybercrime incidents, and the growing international emphasis on digital governance frameworks (Carrapico & Farrand, 2020; Mishra et al., 2022). Therefore, the selected period was considered appropriate for capturing contemporary developments in cybersecurity policy research.

The inclusion criteria applied in this study consisted of: (1) articles focusing on cybersecurity policy-related discussions, (2) publications categorized within the Social Sciences subject area, (3) English-language publications, (4) open access publications, and (5) publications indexed in Scopus until March 17, 2026. The open access criterion was applied to ensure full accessibility, transparency, and consistency during the article evaluation and metadata verification processes. Although this criterion may reduce broader publication coverage, it supports data completeness and reproducibility in bibliometric analysis.

To ensure transparency and reproducibility in the article selection process, this study systematically documented each PRISMA stage, including identification, screening, eligibility assessment, and final inclusion. The detailed flow of the article selection process is presented in Figure 1.

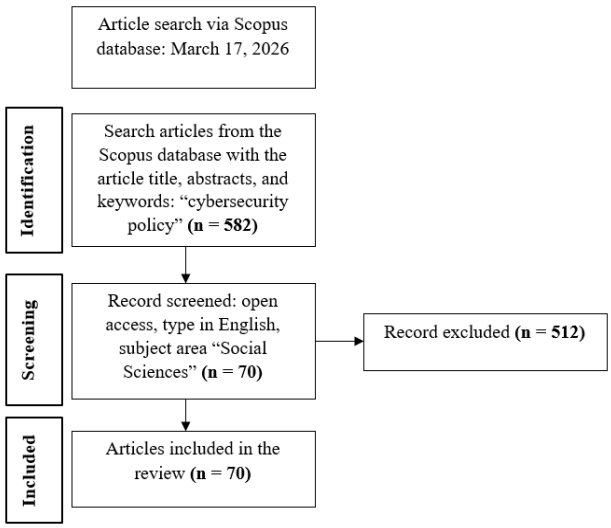

Figure 1. Systematic Literature Review information flow using PRISMA charts

Based on the PRISMA process illustrated in Figure 1, the initial search in the Scopus database produced 582 publications related to cybersecurity policy studies. During the screening stage, records were filtered based on open access status, English-language publication type, and relevance to the Social Sciences subject area. As a result, 512 records were excluded for not meeting the inclusion criteria, leaving 70 articles eligible for further analysis. The remaining publications subsequently underwent eligibility assessment through abstract examination, keyword relevance checking, and thematic evaluation to ensure alignment with cybersecurity policy discussions within the social sciences perspective. Consequently, a total of 70 articles were included as the final dataset in this study.

Metadata cleansing and standardization processes were conducted before bibliometric visualization to ensure consistency and accuracy in the dataset. Duplicate records, inconsistent author naming formats, institutional affiliation variations, and keyword inconsistencies were manually reviewed and standardized to reduce mapping bias and improve analytical reliability (Al Husaeni & Nandiyanto, 2022). This process is important in bibliometric studies to ensure more accurate visualization of collaboration networks, citation structures, and thematic clusters.

To strengthen validity and reliability, the article selection and screening processes were conducted through repeated cross-checking of metadata, abstracts, keywords, and thematic relevance. In addition, the inclusion and exclusion criteria were consistently applied throughout the screening process to minimize selection bias and maintain data reliability. A quality assessment stage was also conducted by evaluating article relevance, thematic consistency, journal indexing quality, and alignment with the objectives of the study, ensuring that article selection was not based solely on administrative criteria.

The analytical procedures in this study were aligned with each research question. RQ1 was addressed through publication trend analysis and keyword development mapping to evaluate the sustainability and future relevance of cybersecurity policy studies in the social sciences. RQ2 was analyzed through co-occurrence analysis, thematic clustering, citation mapping, and collaboration

network visualization to identify the distribution and intellectual structure of research investigations. Meanwhile, RQ3 was addressed through interpretative synthesis of the literature findings to identify theoretical implications, governance perspectives, and practical policy directions emerging from cybersecurity policy studies.

RESULTS AND DISCUSSION

RQ1: Is the exploration of cybersecurity policy a subject that has potential significance for future social science research?

To understand the development trend of cybersecurity policy research over time, Figure 2 presents the annual distribution of publications indexed in the Scopus database during the 2015–2026 period.

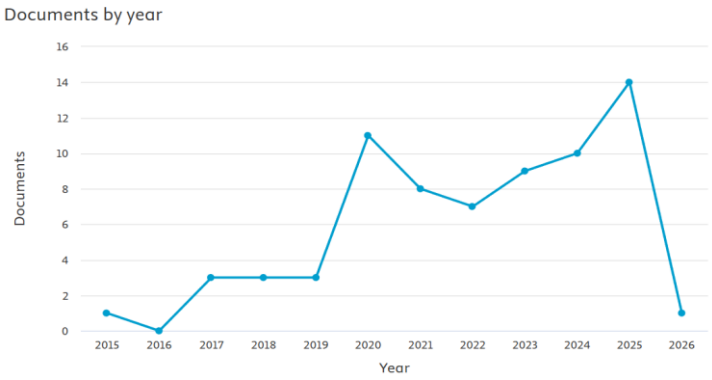

Figure 2. Number of Cybersecurity Policy Research per Year
Source: Scopus Database

The publication trend presented in Figure 2 indicates a substantial increase in academic attention toward cybersecurity policy studies over the last decade. Although publications remained relatively limited during the 2015–2019 period, research productivity increased significantly after 2020, suggesting that cybersecurity policy has become an increasingly important research agenda within contemporary social science scholarship. This growth coincided with the acceleration of digital transformation, increasing cyber threats, and the expansion of digital governance discussions during and after the COVID-19 period (Andreasson et al., 2020; Carrapico & Farrand, 2020; Wang et al., 2020).

The increasing trend also reflects a shift in how cybersecurity is understood within academic discussions. Earlier studies tended to emphasize technical protection and cyber defense mechanisms, whereas more recent publications increasingly position cybersecurity policy as a governance, institutional, and socio-political issue (Fuster & Jasmontaite, 2020; Verhelst & Wouters, 2020). Discussions regarding regulation, digital sovereignty, institutional resilience, and multi-stakeholder collaboration became more prominent after 2020, indicating the growing integration of cybersecurity issues into broader public policy and governance debates.

Compared to previous bibliometric studies that generally focused on technical cybersecurity themes or information systems research (Barcellos-Paula et al., 2025; Lang, 2025), this study specifically highlights the growing relevance of cybersecurity policy from a social science perspective. The findings therefore suggest that cybersecurity policy research is no longer peripheral, but is increasingly positioned as an interdisciplinary governance issue with long-term relevance for digital society, institutional adaptation, and public policy development. These findings directly address RQ1 by demonstrating the sustained growth and strategic significance of cybersecurity policy research in contemporary academic discourse.

RQ2: How is the current allocation of research investigations related to cybersecurity policy in the study of social sciences?

To examine the global distribution of cybersecurity policy research, Figure 3 presents the number of publications contributed by the top 10 countries or regions identified in the dataset.

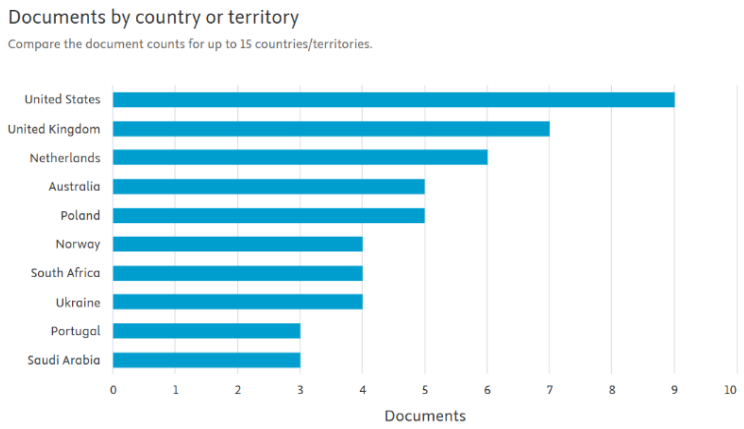

Figure 3. Number of publications by country/region (top 10 countries)
Source: Scopus database

The distribution of publications across countries demonstrates that cybersecurity policy research has developed through highly interconnected and multidisciplinary academic networks. Figure 3 shows that the United States and the United Kingdom remain dominant contributors, followed by several European countries such as the Netherlands and Poland.

The dominance of the United States and the United Kingdom can be interpreted through several structural and institutional factors. Both countries possess strong research infrastructures, advanced digital governance systems, extensive cybersecurity funding mechanisms, and long-standing geopolitical interests in cyber governance and digital security. In addition, their dominance reflects the concentration of influential academic institutions, international research collaborations, and policy-oriented cybersecurity initiatives. Previous studies similarly indicate that countries with stronger digital state capacity and institutional maturity tend to produce more extensive cybersecurity governance research (Farrand et al., 2024; Mishra et al., 2022).

At the same time, the presence of countries such as South Africa, Saudi Arabia, and Ukraine indicates that cybersecurity policy concerns are increasingly expanding beyond traditionally dominant Western countries. However, the unequal distribution of publications also reveals continuing disparities in research capacity between developed and developing countries. Many developing countries still face institutional limitations, resource constraints, and uneven digital infrastructure, which may affect their contribution to cybersecurity policy scholarship (Imran et al., 2024; Malatji et al., 2021). This finding suggests that future research should provide greater attention to contextual cybersecurity governance challenges in developing regions.

To further analyze international collaboration patterns among countries, Figure 4 visualizes the country network relationships generated through VOSviewer analysis.

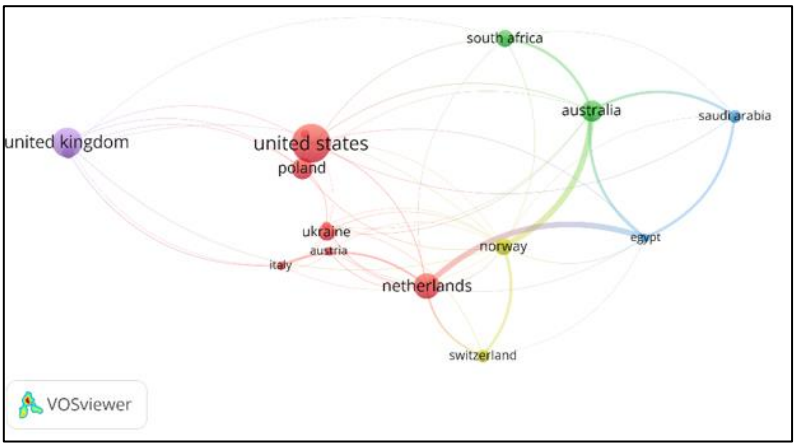

Figure 4. Country Network Visualization
Source: Output from VOSviewer Software

The visualization indicates that the United States functions as a central collaboration hub connected to multiple countries, reflecting its strategic role in shaping global cybersecurity governance discussions. Meanwhile, European countries demonstrate relatively dense collaborative patterns, suggesting the importance of regional governance frameworks and policy coordination in cybersecurity studies. Rather than merely indicating publication relationships, these findings illustrate how cybersecurity governance increasingly operates through transnational policy networks, institutional partnerships, and collaborative knowledge production.

To identify institutional contributions to cybersecurity policy research, Figure 5 presents the top affiliated institutions based on publication productivity.

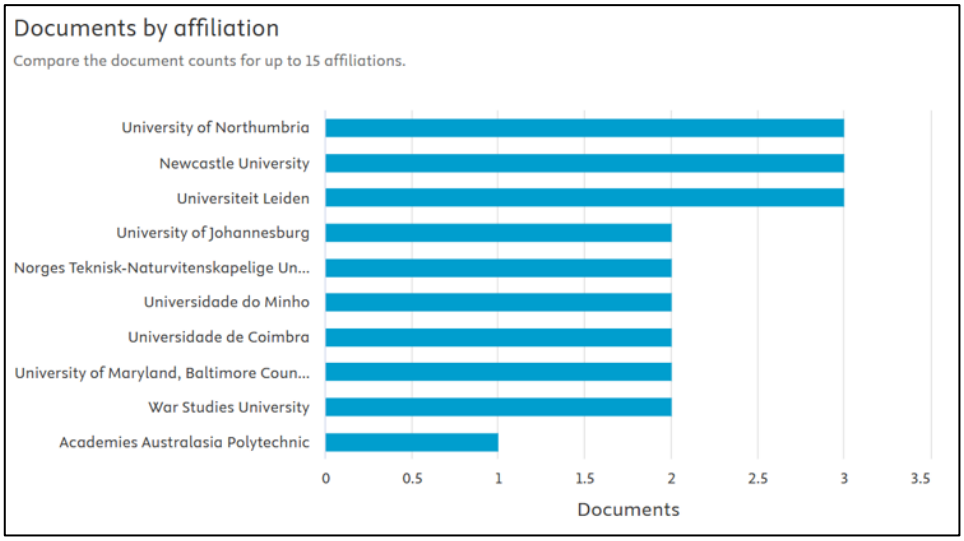

Figure 5. Documents By Affiliate (Top 10 Affiliates)
Source: Scopus Database

Although institutions from the United Kingdom and the Netherlands demonstrate relatively strong productivity, the broader distribution of affiliations across multiple countries indicates that cybersecurity policy studies are not concentrated within a single academic region. This pattern reflects the multidimensional character of cybersecurity governance, which intersects with public policy, international relations, law, digital governance, criminology, and information systems research.

To understand the disciplinary spread and publication concentration of cybersecurity policy studies, Figure 6 presents the distribution of publications across major journal sources.

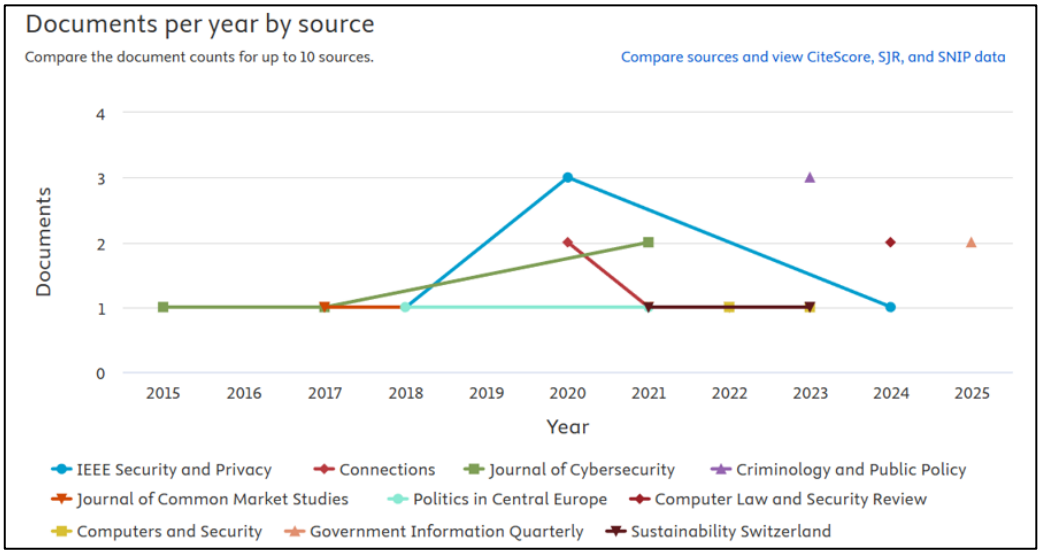

Figure 6. Documents Per Year by Source (Top 10 Sources)
Source: Scopus Database

The dominance of journals such as IEEE Security and Privacy, Journal of Cybersecurity, Government Information Quarterly, and Computers and Security indicates that cybersecurity policy discussions increasingly bridge technical, governance, legal, and socio-political perspectives. This finding strengthens the argument that cybersecurity policy has evolved into an interdisciplinary research domain requiring collaboration across multiple academic traditions.

To identify the dominant forms of scientific publication used in cybersecurity policy research, Figure 7 presents the distribution of publication types within the dataset.

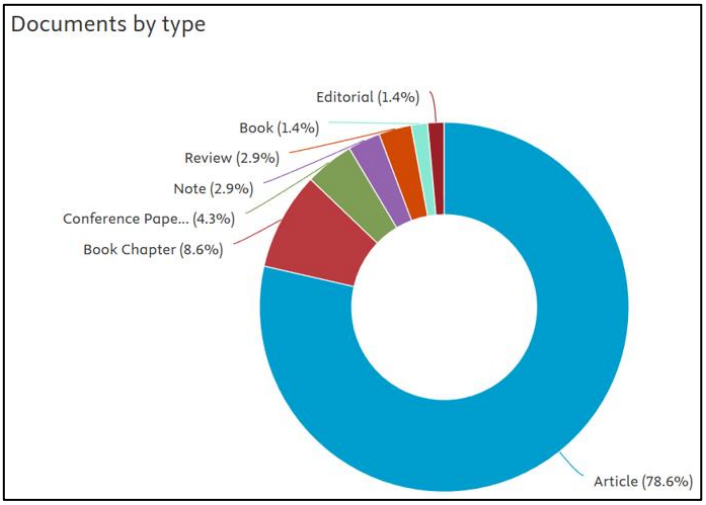

Figure 7. Documents by Type
Source: Scopus Database

The dominance of journal publications indicates that cybersecurity policy research continues to rely heavily on empirical investigation, theoretical discussion, and evidence-based policy analysis. This pattern also reflects the increasing academic institutionalization of cybersecurity policy discussions within contemporary scholarly communication.

Overall, the bibliometric findings reveal that cybersecurity policy research is increasingly shaped by interactions among governance structures, institutional capacity, international collaboration, and socio-political dynamics. These findings contribute theoretically by positioning cybersecurity policy not merely as a technical security issue, but as a multidimensional governance construct closely related to institutional adaptation, digital state capacity, and transnational policy coordination. In addition, this study offers novelty by integrating bibliometric mapping with social governance perspectives to identify the relationship between cybersecurity policy determinants and broader social variables, including institutional resilience, organizational capacity, collaboration networks, and governance legitimacy.

However, this study also has several limitations. The exclusive use of the Scopus database and open-access publications may limit the overall coverage of relevant literature, particularly studies indexed in alternative databases or non-open-access sources. Therefore, future studies are encouraged to expand database coverage, include multilingual publications, and incorporate comparative regional perspectives to strengthen the comprehensiveness of cybersecurity policy research.

RQ3: What are the theoretical and practical implications from the perspective of cybersecurity policy research in the field of social sciences in the future?

To explore the theoretical and practical implications of cybersecurity policy research, this study conducted a bibliometric co-occurrence analysis using VOSviewer based on metadata extracted from 70 selected publications indexed in the Scopus database. This analysis was intended to identify dominant themes, conceptual relationships, and emerging patterns within cybersecurity policy studies. In addition to mapping research trends, the bibliometric findings also provide insights into the conceptual development of cybersecurity policy as a governance and socio-political issue. These findings are expected to contribute both theoretically and practically by supporting the development of adaptive, collaborative, and evidence-based cybersecurity governance frameworks.

To identify the conceptual relationships among keywords frequently appearing together in the literature, Figure 8 presents the co-occurrence network visualization generated through VOSviewer analysis.

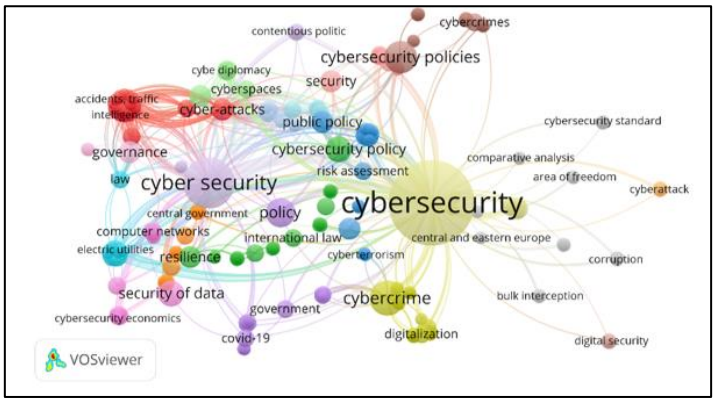

Figure 8. Co-occurrence Framework and Key Terms Representation
Source: VOSviewer software output

The co-occurrence analysis shows that "cybersecurity" acts as the central node connecting multiple thematic clusters, including governance, public policy, cyber-attacks, law, resilience, and data security. The visualization indicates that cybersecurity policy research has increasingly developed beyond technical protection issues and expanded into governance, institutional, and socio-political dimensions. The co-occurrence analysis revealed several thematic clusters representing different areas of cybersecurity policy research. The dominant clusters were associated with regulatory governance and public policy, cyber threats and cybercrime, organizational resilience and institutional capacity, digital transformation, and collaborative governance. Each cluster reflects a distinct yet interconnected dimension of cybersecurity policy, illustrating how the field has evolved beyond technical security concerns toward broader governance, institutional, and socio-political discussions. A more detailed examination of the cluster composition indicates that governance- and policy-related themes occupy central positions within the network, while resilience, collaboration, and digital transformation emerge as complementary areas that shape the broader cybersecurity policy landscape.

The analysis also demonstrates that discussions regarding cybersecurity are closely associated with public policy, institutional coordination, and legal adaptation. This finding supports previous studies emphasizing that cybersecurity policy is not merely a technological issue, but also a governance challenge shaped by institutional structures, political priorities, and social adaptation processes (Fuster & Jasmontaite, 2020; Veale & Brown, 2020). Compared with previous bibliometric studies that mainly focused on technical cybersecurity domains (Barcellos-Paula et al., 2025; Lang, 2025), this study highlights the stronger integration of governance, law, and social resilience dimensions within cybersecurity policy discussions. To complement the visualization results, Table 2 presents the keywords with the highest total link strength identified through the co-occurrence analysis.

Table 2. Keyword by Authors

Rank	Keyword	Total link strength
1	Cybersecurity	268
2	Cyber security	191
3	Network security	67
4	Cyber-attacks	65
5	Cybersecurity policies	60
6	Law	56
7	Policy	54
8	Crime	52
9	Public policy	51
10	Governance	49

Source: VOSviewer software output

The keyword analysis confirms that cybersecurity research remains strongly connected to governance and regulatory discussions. Keywords such as "law," "policy," "public policy," and

"governance" indicate that the field increasingly emphasizes institutional arrangements and policy responses rather than purely technical mitigation strategies. At the same time, the coexistence of terms such as "crime," "cyber-attacks," and "network security" reflects the continuing influence of security threat narratives in shaping cybersecurity policymaking.

Although research productivity has increased significantly since 2020, the findings reveal that scholarly contributions remain concentrated in developed countries, particularly the United States and the United Kingdom. This dominance is closely related to their stronger institutional capacity, advanced digital infrastructure, larger research funding allocation, and strategic geopolitical interests in cybersecurity governance. These countries also possess more mature digital governance systems and stronger collaboration between governments, universities, and private technology sectors. Consequently, they are better positioned to produce influential cybersecurity policy research and shape international cybersecurity discourse.

In contrast, developing countries remain underrepresented despite experiencing growing cybersecurity threats and digital vulnerabilities. Limited institutional capacity, insufficient cybersecurity infrastructure, unequal access to digital resources, and weak regulatory implementation contribute to this imbalance. This finding suggests that future research should place greater emphasis on comparative and contextual studies from developing regions to ensure more inclusive and globally representative cybersecurity policy frameworks.

The bibliometric findings also reveal several important research gaps. Existing studies are still largely dominated by discussions on regulation, governance, and national security. This tendency is evident from the bibliometric findings, where governance-related keywords such as "cybersecurity," "law," "policy," "public policy," and "governance" exhibit relatively high total link strength and occupy central positions within the co-occurrence network. By contrast, themes related to public trust, digital inequality, organizational behavior, policy implementation effectiveness, and community resilience were either absent from the most influential keywords or appeared only marginally within the thematic clusters. These findings indicate that the current literature places greater emphasis on governance and regulatory dimensions, while socio-empirical aspects of cybersecurity policy remain comparatively underexplored and warrant further scholarly attention. This indicates that future cybersecurity policy research should increasingly integrate social science perspectives to better understand the human and institutional dimensions of cybersecurity governance.

The conceptual model presented in Figures 9 and 10 was developed through thematic synthesis derived from co-occurrence analysis, keyword clustering, and critical interpretation of the reviewed literature. The grouping process identified recurring relationships among governance, regulation, institutional capacity, collaboration, resilience, and social adaptation variables, which were then synthesized into broader conceptual dimensions. Therefore, the model does not merely represent a descriptive visualization, but reflects an integrated theoretical interpretation of dominant patterns found across the reviewed studies.

To summarize the conceptual relationships identified from the literature synthesis, Figure 9 presents the five main factors that determine cybersecurity policy development.

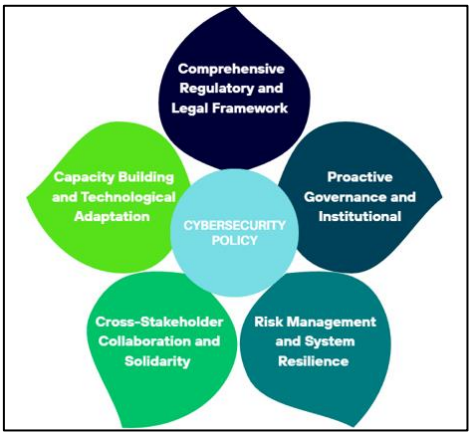

Figure 9. Key Factors That Determine Cybersecurity Policy
Source: Processed by Researcher 2026

Figure 9 presents a conceptual model derived from the thematic synthesis of findings obtained through bibliometric analysis and literature review. Specifically, the model was developed by examining keyword co-occurrence patterns, thematic clusters, and recurring concepts identified across the reviewed studies. Concepts that frequently appeared together and reflected similar governance-related concerns were grouped into broader categories through an interpretative synthesis process. This procedure resulted in five interrelated dimensions: (1) comprehensive regulatory and legal frameworks, (2) proactive governance and institutional capacity, (3) risk management and system resilience, (4) cross-stakeholder collaboration, and (5) capacity building and technological adaptation. Therefore, the model should be interpreted as a conceptual representation of dominant themes within the literature rather than as an empirically validated framework. These dimensions collectively illustrate that cybersecurity policy effectiveness depends not only on formal regulation, but also on institutional readiness, public participation, and adaptive governance mechanisms.

First, comprehensive legal and regulatory frameworks function as the primary foundation for cybersecurity governance. Studies emphasize the importance of national cybersecurity strategies, sectoral regulations, accountability mechanisms, and legal harmonization with international standards to maintain digital stability and governance certainty (Fuster & Jasmontaite, 2020; Napetvaridze & Chochia, 2019). In many countries, cybersecurity policies are increasingly integrated into broader national security and digital sovereignty agendas (Farrand et al., 2024). Second, governance and institutional capacity determine the ability of governments and organizations to coordinate cybersecurity responses effectively. Institutional fragmentation, unclear authority distribution, and weak policy enforcement frequently reduce policy effectiveness, particularly in developing countries (Farooqui et al., 2025; Wadesango & Maveneka, 2025). Conversely, adaptive governance structures and strong institutional coordination improve crisis response capacity and policy implementation (Kianpour & Frantz, 2024; Malatji et al., 2021). Third, risk management and resilience are central dimensions in cybersecurity policymaking. The literature highlights the importance of vulnerability assessments, incident response mechanisms, critical infrastructure protection, and adaptive resilience strategies against evolving cyber threats (Kelemen, 2023; Shkolnyk et al., 2025). Cybersecurity policies increasingly focus on anticipating systemic disruptions that may affect economic and political stability. Fourth, cross-stakeholder collaboration reflects the transnational nature of cybersecurity challenges. Public-private partnerships, regional cooperation, academic involvement, and international coordination are widely recognized as essential components for strengthening cyber resilience (Baezner, 2020; Kaponig, 2020). This finding reinforces governance theory perspectives emphasizing collaborative governance and network-based policymaking. Fifth, capacity building and technological adaptation highlight the importance of cybersecurity awareness, digital literacy, workforce development, and continuous technological adjustment. Several studies indicate that cybersecurity policies are less effective when human resource capacity and organizational awareness remain low (Norris et al., 2018; Saeed, 2023). Therefore, cybersecurity governance requires long-term investments in education, institutional learning, and digital competency development.

The five determinants identified in this study contribute theoretically to the development of cybersecurity policy studies by demonstrating that cybersecurity governance operates as a multidimensional socio-political system rather than solely a technical regulatory framework. These findings strengthen governance and institutionalism perspectives by emphasizing the interaction between regulation, institutional coordination, social participation, and adaptive state capacity in responding to digital threats.

The literature synthesis further indicates that cybersecurity policy significantly influences broader social, political, and economic variables. To illustrate these relationships, Figure 10 presents the main social variables affected by cybersecurity policy.

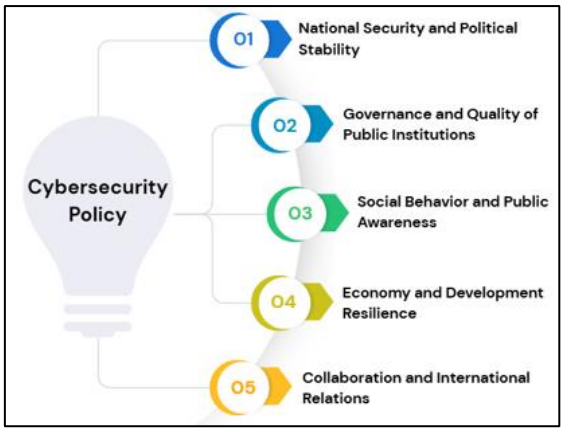

Figure 10. Social Variables Influenced by Cybersecurity Policy
Source: Processed by Researcher 2026

Figure 10 presents a conceptual representation of the major social dimensions that are frequently associated with cybersecurity policy in the reviewed literature. Based on the thematic synthesis and bibliometric findings, the literature consistently highlights five interconnected dimensions: (1) national security and political stability, (2) governance and institutional quality, (3) social behavior and public awareness, (4) economic resilience and development, and (5) collaboration and international relations. The relationships illustrated in the figure are conceptual in nature and reflect patterns identified across the reviewed studies rather than empirically tested causal relationships.

First, cybersecurity policy directly influences national security and political stability. Strong cybersecurity governance enhances national resilience against cyber warfare, disinformation campaigns, and geopolitical threats (Antonio, 2024; Górka, 2022). Conversely, weak cybersecurity systems increase vulnerabilities that may disrupt democratic institutions and policymaking processes (Carrapico & Farrand, 2020). Second, cybersecurity policy affects governance quality and institutional effectiveness. Effective cybersecurity governance improves institutional coordination, accountability, and administrative integration, while weak implementation increases operational and regulatory risks (Farooqui et al., 2025; Malatji et al., 2021). Third, cybersecurity policy shapes public behavior and social awareness. Security policies influence organizational culture, employee compliance, digital literacy, and public perceptions regarding digital risks (Saeed, 2023). Public support for cybersecurity regulation is also strongly influenced by perceived threat severity and trust in government institutions (Snider et al., 2021). Fourth, cybersecurity policy contributes to economic resilience and sustainable development. Cybercrime and digital attacks create substantial economic losses and threaten critical infrastructure stability (He, 2024; Ruvin et al., 2020). Effective cybersecurity policies therefore function as instruments for protecting digital economies, strengthening market confidence, and supporting sustainable digital transformation. Fifth, cybersecurity policy influences patterns of international cooperation and global governance. Cybersecurity challenges increasingly require regional coordination, diplomatic engagement, and collaborative governance mechanisms among states and institutions (Baezner, 2020; Gao, 2024). This demonstrates that cybersecurity governance has evolved into an important component of international political relations and digital sovereignty strategies.

Overall, the findings confirm that cybersecurity policy represents a multidimensional socio-political phenomenon that shapes governance structures, institutional behavior, public trust, economic resilience, and international cooperation within the digital era. The bibliometric patterns demonstrate that cybersecurity governance cannot be adequately understood solely through technical or technological approaches, but instead requires broader integration with governance theory, institutionalism, public policy analysis, and socio-political perspectives. The dominance of themes related to governance, regulation, institutional coordination, and public policy further indicates that cybersecurity has evolved into a strategic governance issue rather than merely a technical security concern.

LIMITATION

This study has several limitations that should be acknowledged. First, the analysis relied solely on the Scopus database, which may have excluded relevant studies indexed in other databases such as Web of Science, Dimensions, or Google Scholar. Second, the study only included open-access publications written in English, potentially limiting the representation of non-English and subscription-based research. Third, the focus on the Social Sciences subject area may not fully capture the interdisciplinary nature of cybersecurity policy research, particularly contributions originating from computer science, law, and engineering disciplines.

In addition, the bibliometric analysis was primarily based on publication metadata and VOSviewer mapping. Although this approach is effective for identifying publication trends, thematic structures, and collaboration patterns, it does not provide an in-depth qualitative evaluation of the theoretical and methodological rigor of each study. Furthermore, the dataset only included publications available until March 17, 2026, meaning that more recent developments and emerging issues in cybersecurity policy were not captured in this analysis. Future studies are therefore encouraged to integrate multiple databases, apply comparative cross-regional approaches, and develop empirical or mixed-method models to better examine the determinants, implementation, and impacts of cybersecurity policies within evolving digital governance environments.

CONCLUSION

This study demonstrates, based on a systematic literature review and bibliometric analysis, that cybersecurity policy has increasingly been discussed as a multidimensional governance issue extending beyond technical protection and digital security mechanisms. The reviewed literature indicates that contemporary cybersecurity policy research increasingly emphasizes governance structures, institutional coordination, legal frameworks, public policy, social resilience, and international collaboration. The observed growth in publications after 2020 further suggests that cybersecurity policy has become an increasingly important research agenda within contemporary social science scholarship.

The literature synthesis and bibliometric findings identified five interrelated determinants frequently highlighted in cybersecurity policy studies, namely: (1) regulatory and legal frameworks, (2) governance and institutional capacity, (3) risk management and resilience, (4) cross-stakeholder collaboration, and (5) capacity building and technological adaptation. These determinants were synthesized into a conceptual governance model that illustrates how the reviewed literature conceptualizes cybersecurity policy as a socio-political and institutional system. In addition, the reviewed studies consistently associate cybersecurity policy with broader social dimensions, including institutional quality, public trust, political stability, economic resilience, social awareness, and international cooperation.

Theoretically, this study contributes to the development of cybersecurity policy research by strengthening governance theory, institutionalism, and digital governance perspectives within cybersecurity studies. The literature consistently highlights institutional readiness, collaborative governance mechanisms, and socio-political adaptation as important elements of cybersecurity governance alongside technological capacity. Furthermore, the integration of bibliometric mapping with governance-oriented literature synthesis provides a broader conceptual understanding of cybersecurity policy within contemporary digital society.

From a practical perspective, the findings suggest that policymakers, public institutions, and digital governance actors should consider not only technological infrastructure but also institutional strengthening, regulatory coordination, cybersecurity literacy, and long-term governance capacity development. The reviewed literature also highlights the importance of inclusive and collaborative cybersecurity governance, particularly in contexts where institutional capacity, digital infrastructure, and resource availability remain uneven. These observations are derived from recurring patterns identified across the reviewed studies rather than from a direct evaluation of specific countries. Strengthening adaptive governance frameworks and international collaboration is therefore frequently emphasized in the literature as an important consideration for supporting sustainable digital transformation and enhancing resilience to evolving cyber threats.

AUTHOR CONTRIBUTIONS

RATP developed the main idea of the study, prepared the research design, collected the data, conducted the systematic literature review, carried out the bibliometric analysis, interpreted the results, and drafted the manuscript. IDAN provided academic supervision, strengthened the theoretical foundation, reviewed the methodological approach, and contributed to the critical revision and editing of the manuscript. FA assisted in the literature screening process, organized the research data, supported the analysis, and contributed to the review and editing of the manuscript.

REFERENCES

Afshari-Mofrad, M., Amrollahi, A., & Abedin, B. (2024). Adopt agile cybersecurity policymaking to counter emerging digital risks. *MIS Quarterly Executive*, *23*(4), 371–386. https://doi.org/10.17705/2msqe.00102

Alhumud, T. A. A., Omar, A., & Altohami, W. M. A. (2023). An assessment of cybersecurity performance in the Saudi universities: A total quality management approach. *Cogent Education*, *10*(2),1-16. https://doi.org/10.1080/2331186X.2023.2265227

Al Husaeni, D. F., & Nandiyanto, A. B. D. (2022). Bibliometric using VOSviewer with Publish or Perish (using Google Scholar data): From step-by-step processing for users to the practical examples in the analysis of digital learning articles in pre and post COVID-19 pandemic. *ASEAN Journal of Science and Engineering*, *2*(1), 19–46. https://doi.org/10.17509/ajse.v2i1.37368

Andreasson, A., Artman, H., Brynielsson, J., & Franke, U. (2020). A census of Swedish government administrative authority employee communications on cybersecurity during the COVID-19 pandemic. *Proceedings of the 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 727–733. https://doi.org/10.1109/ASONAM49781.2020.9381324

Antonio, J. M. A. (2024). Disparities and backlogs in Mexico's national and international cybersecurity policies vis-à-vis the United States and Canada: Challenges of cooperation for North America. *Norteamérica*, *19*(1), 35-68. https://doi.org/10.22201/cisan.24487228e.2024.1.663

Baezner, M. (2020). Cybersecurity in Switzerland: Challenges and the way forward for the swiss armed forces. *Connections*, *19*(1), 63–72. https://doi.org/10.11610/Connections.19.1.06

Barcellos-Paula, L., Gil-Lafuente, A. M., & Merigó, J. M. (2025). Research on cybersecurity and business: A bibliometric review (2004-2023). *Management Notebooks*, *25*(1), 19–36. https://doi.org/10.5295/cdg.242288lb

Barrington, M. J., D'Souza, R. S., Mascha, E. J., Narouze, S., & Kelley, G. A. (2024). Systematic reviews and meta-analyses in regional anesthesia and pain medicine (Part I): Guidelines for preparing the review protocol. *Regional Anesthesia and Pain Medicine*, *49*(6), 391–402. https://doi.org/10.1136/rapm-2023-104801

Ben Mamia, S., Schunck, C. H., Arunkumar, M., & Roßnagel, H. (2025). Security awareness versus secure behaviour: A bibliometric study of the state of research on human factors in IT Security. In H. Rossnagel, C. H. Schunck, & D. Pohn (Eds.), *Lecture Notes in Informatics (LNI), Proceedings—Series of the Gesellschaft für Informatik (GI): P-364* (pp. 167–173). Gesellschaft für Informatik (GI). https://doi.org/10.18420/OID2025_13

Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of COVID-19: The case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111–1126. https://doi.org/10.1080/07036337.2020.1853122

Charlet, K., & King, H. (2020). The future of cybersecurity policy. *IEEE Security & Privacy*, *18*(1), 8–10. https://doi.org/10.1109/MSEC.2019.2953368

Farooqui, M. O., Sarhan, A., & Mustafa, F. (2025). Aviation cyber security in India: Legal gaps, international frameworks, and policy reforms. *Yustisia Jurnal Hukum*, *14*(2), 186–224. https://doi.org/10.20961/yustisia.v14i2.101653

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs*, *100*(6), 2379–2397. https://doi.org/10.1093/ia/iiae231

Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European Union: The digital, the critical and fundamental rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The ethics of cybersecurity* (Vol, 21, pp. 97–115). Springer. https://doi.org/10.1007/978-3-030-29053-5_5

Gan, Y.-N., Li, D.-D., Robinson, N., & Liu, J.-P. (2022). Practical guidance on bibliometric analysis and mapping knowledge domains methodology – A summary. *European Journal of Integrative Medicine*, *56,* 102203. https://doi.org/10.1016/j.eujim.2022.102203

Gao, X. (2024). Challenges and opportunities: Estonia's role in shaping EU cybersecurity policy. In A.-L. Högenauer & M. Mišík (Eds.), *Small states in EU policy-making: Strategies, challenges, opportunities* (pp. 159–173). Routledge. https://doi.org/10.4324/9781003380641-12

Górka, M. (2022). Catalysts of cyber threats on the example of Visegrad Group countries. *Politics in Central Europe*, *18*(3), 317–342. https://doi.org/10.2478/pce-2022-0014

He, Y. (2024). China's digital shadows: Unveiling the economic toll of cybercrime. *Humanities and Social Sciences Communications*, *11*(1), 1416. https://doi.org/10.1057/s41599-024-03952-z

Holt, T. J., Griffith, M., Turner, N., Greene-Colozzi, E., Chermak, S., & Freilich, J. D. (2023). Assessing nation-state-sponsored cyberattacks using aspects of situational crime prevention. *Criminology & Public Policy*, *22*(4), 825–848. https://doi.org/10.1111/1745-9133.12646

Imran, M. F., Gunawan, H., & Asmoro, D. (2024). Addressing the hurdles: Enhancing better policies in Indonesia cyber security management amidst uncertainty. *Journal of Public Service Management*, *8*(2), 275–290. https://doi.org/10.24198/jmpp.v8i2.52212

Kaponig, M. G. H. (2020). Austria's national cyber security and defense policy: Challenges and the way forward. *Connections: The Quarterly Journal*, *19*(1), 21–37. https://doi.org/10.11610/Connections.19.1.03

Kelemen, R. (2023). The impact of the Russian-Ukrainian hybrid war on the European Union's cybersecurity policies and regulations. *Connections: The Quarterly Journal*, *22*(2), 75–90. https://doi.org/10.11610/Connections.22.2.55

Kianpour, M., & Frantz, C. (2024). Analysis of institutional design of European Union cyber incident and crisis management as a complex public good. *Regulation & Governance, 19*(4), 1037-1062. https://doi.org/10.1111/rego.12640

Kosasih, A., Aditya, T., & Ramadhan, S. A. (2025). Evaluation of infrastructure and cybersecurity in supporting the digital transformation of public services in Tangerang City. *Jurnal Manajemen Pelayanan Publik*, *9*(3), 802–826. https://doi.org/10.24198/jmpp.v9i3.65900

Lang, M. (2025). The fragmented research space of cybersecurity: A map of the territory. In I. Praça, S. Bernardi, & P. R. M. Inácio (Eds.), *Communications in Computer and Information Science* (Vol. 2500, pp. 116–132). Springer. https://doi.org/10.1007/978-3-031-94855-8_8

Malatji, M., Marnewick, A. L., & von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability*, *13*(1), 1–33. https://doi.org/10.3390/su13010291

Malmqvist, J., Machado, T., Meikleham, A., & Hugo, R. (2019). *Bibliographic data analysis of CDIO conference papers from 2005–2018*. In J. Bennedsen, A. B. Lauritsen, K. Edström, N. Kuptasthien, J. Roslöf, & R. Songer (Eds.), *Proceedings of the 15th International CDIO Conference* (pp. 816–833). Aarhus University.

Mering, M. (2017). Bibliometrics: Understanding author-, article-, and journal-level metrics. *Serials Review*, *43*(1), 41–45. https://doi.org/10.1080/00987913.2017.1282288

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers and Security*, *120*, 102820. https://doi.org/10.1016/j.cose.2022.102820

Napetvaridze, V., & Chochia, A. (2019). Cybersecurity in the making-policy and law: A case study of Georgia. *International and Comparative Law Review*, *19*(2), 155–180. https://doi.org/10.2478/iclr-2019-0019

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of internet security. *Journal of Homeland Security and Emergency Management*, *15*(3), 20170048. https://doi.org/10.1515/jhsem-2017-0048

Okigui, H. H., Cronjé, J. C., & Francke, E. R. (2024). An analysis of cybersecurity policy compliance in organizations. *Applied Cybersecurity and Internet Governance*, *3*(2), 303–321. https://doi.org/10.60097/ACIG/191942

Oliveira, E., & Baldi, V. (2022). Systematic review on cybersecurity risks and behaviours: Methodological approaches. In *Proceedings of the 7th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2022)* (Vol. 1, pp. 49–56). SciTePress. https://doi.org/10.5220/0010762600003197

Ribeiro, D., Fonte, V., Ramos, L. F., & Silva, J. M. (2025). Assessing the information security posture of online public services worldwide: Technical insights, trends, and policy implications. *Government Information Quarterly*, *42*(2), 102031. https://doi.org/10.1016/j.giq.2025.102031

Ruvin, O., Isaieva, N., Sukhomlyn, L., Kalachenkova, K., & Bilianska, N. (2020). Cybersecurity as an element of financial security in the conditions of globalization. *Journal of Security and Sustainability Issues*, *10*(1), 175–188. https://doi.org/10.9770/jssi.2020.10.1(13)

Saeed, S. (2023). Digital workplaces and information security behavior of business employees: An empirical study of Saudi Arabia. *Sustainability*, *15*(7), 6019. https://doi.org/10.3390/su15076019

Shkolnyk, I., Tiutiunyk, I., Semenog, A., Kovalenko, Y., & Pavlenko, L. (2025). Institutional, technological, and financial drivers of national cyber resilience under armed conflict and post-conflict recovery. *Problems and Perspectives in Management*, *23*(4), 665–683. https://doi.org/10.21511/ppm.23(4).2025.45

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1), 1-11. https://doi.org/10.1093/cybsec/tyab019

Soni, K. D. (2025). Critical appraisal of systematic reviews and meta-analyses. *Indian Journal of Anaesthesia*, *69*(1), 161–164. https://doi.org/10.4103/ija.ija_1223_24

Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T., & Van Eeten, M. (2020). Governance challenges for European cybersecurity policies: Stakeholder views. *IEEE Security & Privacy*, *18*(1), 46–54. https://doi.org/10.1109/MSEC.2019.2945309

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4), 1–22. https://doi.org/10.14763/2020.4.1533

Verhelst, A., & Wouters, J. (2020). Filling global governance gaps in cybersecurity: International and European legal perspectives. *International Organisations Research Journal*, *15*(2), 105–124. https://doi.org/10.17323/1996-7845-2020-02-07

Wadesango, N., & Maveneka, E. (2025). Cyberthreats and their impact on financial integrity: Evaluating the effectiveness of local authorities' cybersecurity policies in preventing and detecting fraud. *Corporate Law and Governance Review*, *7*(2), 32–40. https://doi.org/10.22495/clgrv7i2p3

Wang, Q. H., Miller, S. M., & Deng, R. H. (2020). Driving cybersecurity policy insights from information on the internet. *IEEE Security & Privacy*, *18*(6), 42–50. https://doi.org/10.1109/MSEC.2020.3000765