Informatio: Journal of Library and Information Science Vol. 4, No. 1 (January 2024) 65-78
ISSN 2775-0043 (Online)

A bibliometric analysis of the of cybersecurity policy research

Opik Qorahman[1*], Nova Nauval Akbar[2]
[1,2]Informatics, Faculty of Engineering Fakulty, Universitas Majalengka
Jl. Raya K H Abdul Halim No.146, Majalengka Kulon, Kec. Majalengka, Majalengka 45418
)* Corresponding Author, Email: opikqorahman332@gmail.com

Received: December 2023; Accepted: February 2024; Published: January 2024

Abstract

The cybersecurity policy is a fundamental framework for developing a robust defense strategy for an organization's digital landscape. It involves various critical steps, including classifying information based on sensitivity, implementing strict access control, encrypting data in transit and at rest, continuous security awareness training, an incident response plan for addressing security breaches, deploying network security measures such as firewalls and intrusion detection systems, and physical security protocols to protect data centers and infrastructure. The purpose of this study is to answer the following questions: How are articles on Cybersecurity Policy classified? What are the latest study trends in Cybersecurity Policy analysis? What are the most frequently published research topics? What are the potential areas for future research in Cybersecurity Policy analysis? This research used a quantitative-descriptive technique. This bibliometric analysis explores the extensive and dynamic domain of cybersecurity policy, examining academic outputs from various dimensions. Utilizing standardized methodologies, including Mendeley software, VOSviewer, and PoP, this study navigates the complex terrain of academic literature. The findings reveal major topics such as 'Cybersecurity policy,' 'Network security policy,' and 'Cybersecurity' emerge, illuminating both well-explored areas and less developed fields such as 'National cybersecurity' and 'Cyberspace.' These unexplored aspects present intriguing avenues for future research.

Keywords: cs (cyber scurity); cybersecurity policy; cyber threats; bibliometric; policy

Abstrak

Kebijakan keamanan siber merupakan kerangka dasar yang fundamental untuk mengembangkan strategi pertahanan yang kuat pada lanskap digital suatu organisasi. Ini melibatkan berbagai langkah kritis, termasuk klasifikasi informasi berdasarkan sensitivitasnya, kontrol akses yang ketat, enkripsi untuk data yang sedang ditransfer dan yang disimpan, pelatihan kesadaran keamanan yang berkelanjutan, rencana tanggap insiden untuk mengatasi pelanggaran keamanan, penerapan langkah-langkah keamanan jaringan seperti firewall dan sistem deteksi intrusi, serta protokol keamanan fisik untuk melindungi pusat data dan infrastruktur. Tujuan dari studi ini adalah untuk menjawab pertanyaan-pertanyaan berikut. Bagaimana artikel-artikel tentang Kebijakan Keamanan Siber diklasifikasikan? Apa tren studi terbaru dalam analisis Kebijakan Keamanan Siber? Apa topik penelitian yang paling sering dipublikasikan? Apa area potensial untuk penelitian masa depan dalam analisis Kebijakan Keamanan Siber? Penelitian ini menggunakan teknik deskriptif kuantitatif. Analisis bibliometrik ini mengeksplorasi domain luas dan dinamis dari kebijakan keamanan siber, memeriksa output akademis dari berbagai dimensi. Dengan memanfaatkan metodologi standar, termasuk perangkat lunak Mendeley, VOSviewer, dan PoP, studi ini menavigasi medan kompleks literatur akademik. Hasil yang ditemukan dalam penelitian ini adalah topik-topik utama seperti 'Kebijakan keamanan siber', 'Kebijakan keamanan jaringan', dan 'Keamanan siber' muncul, memberikan penerangan pada area yang telah banyak dieksplorasi dan wilayah yang kurang berkembang seperti 'Keamanan siber nasional' dan 'Cyberspace'. Aspek-aspek tidak dikenal ini menawarkan jalur menarik untuk penelitian masa depan.

Kata kunci: *cs (cyber scurity);* kebijakan keamanan siber; ancaman siber; bibliometrik; kebijakan

DOI: https://doi.org/10.24198/inf.v4i1.52033
Copyright © 2024 Author(s). This is an open access article under the CC BY-SA license
Website: http://jurnal.unpad.ac.id/informatio

INTRODUCTION

Each numbered entry in the multifaceted terrain of global cybersecurity reveals a separate dimension of the complex difficulties and imperatives that define the digital age. Cybersecurity is more than just a technical issue; it is a complex combination of individual behaviors, corporate initiatives, and government policies. The link between macro-level state security and micro-level user actions magnifies the unique national security issue provided by cybersecurity (Kostyuk & Wayne, 2021). Meanwhile, the pervasive threat of cyber-attacks and the risks connected with wireless communication technologies threaten private companies and government organizations all over the world, emphasizing the critical importance of safeguarding electronic data in our technologically reliant world (Li.Y & Liu, 2021). Cybersecurity as a notion goes beyond the protection of Internet-connected systems; it needs legal frameworks requiring firms to strengthen their systems against a wide range of cyber threats (Srinivas, Das, & Kumar, 2019). However, the recent cyberwars highlight the need for greater readiness, exposing the failure to develop integrated cybersecurity policy (Bruijn & Janssen, 2017). A nation's authority in the twenty-first century is inextricably tied to its technological supremacy, as practically all actions, from personal to official, rely on information technology (Rizal & Yani, 2016).

Increased worries about cybersecurity risks induce large investments within enterprises, fueled by the assumption of beneficial returns on these preemptive measures (Li.L et al., 2019). The individual security requirements of companies, as well as the type of information protected, influence the nuanced selection and deployment of cybersecurity policies (Mishra, Alzoubi, Gill, & Anwar, 2022). Recognizing cybersecurity as more than a technological issue, its complexities include psychological, business operations, economic, and human behavioral factors that operate in cyberspace according to different norms (Charlet & King, 2020). In the ever-changing world of cybersecurity, practitioners must constantly change their procedures and policies to handle the ever-changing threat landscape (Shively, 2021). Globally, the revolutionary impact of information and communications technology is driving more countries to establish comprehensive national cybersecurity strategies (Lilli, 2020). However, as the reliance on digital communications grows, there is a worrying increase in chances for malevolent actors to exploit technology for political and economic benefit (Carrapico & Farrand, 2020).

While terrorist acts frequently dominate headlines, daily cyberattacks and cybercrimes sometimes go unreported by the public and media, underscoring the widespread and underreported nature of digital dangers (Brandão & Camisão, 2021). Debates about digital surveillance revolve around finding a fine balance between accessing encrypted materials and maintaining civil rights in the context of security (Snider, Shandler, Zandani, & Canetti, 2021). Meanwhile, public officials face substantial obstacles in IoT public policy, ranging from a lack of policy direction to the need for clarity and comprehension of user values connected to cybersecurity (Smith, Dhillon, & Carter, 2021). Effective cybersecurity planning arises as a

vital need in this ever-changing landscape, requiring not just strategic insight but also enough resources. Officials are being asked to submit their thoughts on measures that will safeguard communities from the prevalent and rising threats posed by cybersecurity breaches (Hatcher, Meares, & Heslen, 2020). As we go through these interconnected using bibliometrics, a thorough grasp of the complex nature of cybersecurity emerges, paving the way for a deeper investigation of the issues and solutions that define this crucial sector. We navigate the terrain of cyber dangers, legislation, and technological developments in this bibliometric setting, using a scholarly framework to evaluate the evolving cybersecurity discourse. The bibliometric analysis-based contribution to the field of cybersecurity and cyber forensics in general. In terms of the benefits of this effort, first and foremost, the acknowledgment of the most influential scholars, institutions, nations, journals, and their mutual partnerships in this sector is extremely beneficial to the entire scientific research community. Second, the temporal evolution of study subjects, topics, and keywords during the last decade enables researchers to focus their investigations on niche and underexplored regions. This study identifies some key future/emerging themes that will help upcoming researchers in this sector (Sharma, Mittal, Sekhar, Shah, & Renz, 2023).

Bibliometric analysis is a commonly used and comprehensive method for analyzing and interpreting large amounts of scientific data. This strategy allows for the unraveling of evolutionary complexities within a single discipline while also providing useful insights into new areas of the field (Donthu, Kumar, Mukherjee, Pandey, & Lim, 2021).The analysis of bibliometrics in academic publishing can provide information on the growth of academic publishing over time and the significance of key words (Sulardja, 2021).

Google is a popular information retrieval system that is widely used by users today, owing to its ease of use, comprehensiveness, and reliability in providing results. Google has been operating for 23 years. On September 4, 1998, Google launched an innovative service to meet the growing demand for information in the fields of economics, education, management, social science, research, and finance. Google Scholar, also known as Google Cendekia in Indonesian, is one of the Google services that caters to information needs in the fields of education and research. Google scholar is an educational service that assists users in meeting their information needs through the publication of academic journals and online publications from various disciplines throughout the world (Zakiyyah, Winoto, & Rohanda, 2022). Google Scholar, Google's freely accessible academic bibliographic database, has been offered as a potential alternative or supplement to commercial citation databases such as Web of Knowledge (ISI/Thomson) and Scopus (Elsevier). This study presents a novel methodology for evaluating the database's efficacy for bibliometric analysis, with a specific focus on research evaluation. Instead of employing author or institution names, a webometric study of academic web domains is performed. Google Scholar was used to collect bibliographic entries for 225 top-level web domains (TLDs), 19,240 university domains, and 6,380 research center domains. Notably, over 63.8% of the entries are related with generic names such as.com or.org, indicating that a considerable percentage of Scholar's data is sourced from large commercial or

non-profit organizations. When looking at institutions having at least one record, 10,442 universities account for one-third of the other items (10.6% of the total), whereas 3,901 research centers add 7.9% to the entire dataset (Aguillo, 2012).

The Vosviewer software for bibliometric analysis has three visualization displays: Network, Overlay, and Density Visualization. The Network view depicts the connections between the visualized concepts, with the thickness of trajectories representing the strength and abundance of interconnections between one term and others. Bold trajectories imply strong and numerous connections, whereas sparsely written ones with little circles suggest weaker interactions. The Overlay display is used to demonstrate the historical progression of research. In bibliometric analysis, darker visuals reflect longer-term research, whereas lighter colors indicate more current research initiatives. For example, bibliometric analysis in the period 2018 to 2021, then in the Overlay visualization section in 2018 will be displayed in the form of a dark network, and will get lighter in subsequent years. This shows that 2021 will display the brightest network. The last visualization, Density, is used to demonstrate the concentration or attention on research groups. This feature of bibliometric analysis visualization aids in identifying locations with uncommon or plentiful research activity. Researchers find this tool especially useful when planning new research projects since it provides insights into the current landscape of research emphasis and density, assisting in the identification of underexplored or heavily investigated regions. In Vosviewer software, datasets that can be read for bibliometric analysis are very diverse, including datasets from Dimensions, Lens, Scopus, Web of Science, and Pubmed. In addition, there are also Endnote, RIS (can be used through the Publish or Perish application), and RefWork dataset formats. In addition, Vosviewer can be accessed in Microsoft Academic, Crossreff, Europe PMC, Semantic Scholar, OCC, COCI, and Wikidata formats (Zakiyyah et al., 2022).

Tabel 1. State of the CyberSecurity

Author & Year	Citation	Source	Finding
(Y. Li & Liu, 2021)	261	*google scholar*	In the third millennium, cyberspace and related technologies have emerged as important sources of power. Cyberspace's unique characteristics, such as low-cost accessibility, anonymity, vulnerability, and asymmetry, have resulted in power diffusion. This implies a change away from traditional power dynamics between governments and toward the participation of other actors such as private enterprises, organized criminal and terrorist groups, and individuals. While governments continue to play an important role, the landscape today includes a broader range of stakeholders. Despite this transformation, governments continue to play an important role in preserving national security among the shifting dynamics of power in cyberspace.

(Srinivas et al., 2019)	200	*google scholar*	We began by investigating various cyber threats, as well as the security requirements and remedies for each. Following that, we moved our focus to the Cyber Security Incident Management Framework (CIMF), highlighting its role in supporting thorough and efficient participation of organizations in a national coordinated response to cyber incidents. We investigated the issues of standardization in cyber security, which includes tools, security ideas, policies, protection measures, risk management, and training as vital components. Our conversations included the national cybersecurity plan as well as other government measures. Finally, significant advice were presented that are relevant to both cyber security and cyber defense activities.
(Carrapico & Farrand, 2020)	51	*google scholar*	While major and long-term changes are expected in EU politics for health and migration in reaction to the treatment and movement of individuals during a pandemic, the field of cybersecurity displays a distinct pattern. Rather than substantial policy upheavals, there is a reinforcement of existing ideas and attitudes, albeit with fresh vigour and more activity. The existence of disinformation, as well as the function of social media in its propagation, is neither unique nor surprising. Instead, the Commission's confirmation of its previous position is attributed to the ineffectual efforts adopted by social media sites to combat disinformation. This confirmation has resulted in policy statements that are consistent with previously stated aims, rather than representing a radical break from prior policies.
(Mishra et al., 2022)	32	*google scholar*	In this era of widespread digital transformation, information and communication technology (ICT) has become inextricably linked to numerous economic fields. However, the increased usage of ICT has presented significant issues in the field of cybersecurity (CS). These difficulties highlight the growing need of strengthening organizations' ICT infrastructure. CS arises as an important factor for protecting client information from cyber threats and malicious activity on the Internet. The basic purpose of CS is to ensure that systems are secure, reliable, and available. Security measures include the establishment of security policies to secure an organization's cyberspace. The current study examined and discussed numerous customer service rules designed to efficiently manage client information and meet their expectations.

(Brandão & Camisão, 2021)	18	*google scholar*	This article discusses the Commission's significant activities in countering cyber risks in general, and cybercrime in particular, from 2000 to 2016. The emphasis is on how the Commission effectively broadened its mandate to include the important security issue of cybersecurity. The findings show that the Commission made a conscious strategic relationship between the Single Market (especially its digital aspect) and cybersecurity. The institution emphasized that cybercrime is a significant impediment to the full realization of the Single Market, with significant economic consequences for Europe, and argued for the need for a comprehensive approach due to the cross-border, multilevel, and multisectoral nature of the cyber threat. As a policy entrepreneur, the Commission persistently championed and investigated this complete approach.

Source: PoP, 2023

So far, no bibliometric analysis of Cybersecurity Policy appears to exist. The purpose of this study is to answer the following this questions. How are articles on Cybersecurity Policy classified? What are the most recent study trends in Cybersecurity Policy analysis? What are the most often published research topics? What are the potential areas of future research for Cybersecurity Policy analysis? This article's preparation begins with a survey of the literature on the subject of Cybersecurity Policy based on past research findings. Part 2 includes a discussion of the research objectives in addition to Part 1. Part 2 will go over the definition of Cybersecurity Policy as well as the most recent review of Cybersecurity Policy concepts. Part 3 describes the approach utilized to conduct the bibliometric study phase, which involved the use of databases from three separate journals. Part 4 shows the results obtained with the help of VOS Viewer. Part 5 includes study concepts, conclusions, and limits the of Cybersecurity Policy Research.

RESEARCH METHOD

The inquiry used a quantitative technique. By applying the technique of bibliometric analysis, the investigation obtained data taken from the google scholar database. A mechanism of classifying article titles, abstracts, and keywords was used Publish or Perish to search the google scholar database for the term "cybersecurity policy" in order to obtain data. Bibliometric analysis is a useful method for carefully extracting insights from large amounts of unstructured data, allowing for the interpretation and mapping of cumulative scientific knowledge and nuanced advances within established fields. Thorough bibliometric research can lay solid groundwork for expanding a discipline in novel and significant ways. This technique enables scholars to (1) gain a thorough picture, (2) identify knowledge gaps, (3) develop new ideas for research, and (4) strategically place their planned contributions within the subject. The advent of scientific databases such as Scopus and Web of Science has made it

easier to collect large amounts of bibliometric data, while software tools such as Gephi, Leximancer, and VOSviewer enable practical study (Donthu et al., 2021). Clusters generated by VOSviewer are automatically colored in the map. Figure 1 depicts the study framework based on the description above. The data articles used in this study are research data from journals indexed by Google Scholar. The reference managers program was used to collect the data. Publish or perish is a research reference manager's application. The type of article we accept is one that has been published in a journal. Every article data indexed by Google Scholar and in the form of journal articles that correspond to the search for the themes needed in this study is saved in a file that is used in utilizing VOSviewer (Nandiyanto & Al Husaeni, 2022).

This table explicitly describes the profiles and metrics of the selected journals. Table 3 presents some essential information obtained from the metadata using the Publish or Perish (PoP) method on November 28, 2023.

Tabel 2. Metrics Information of Terms

Metrics Data	Cyber Security Policy
Publication year	2002-2023
Citation year	21
Paper	200
Citations	11832
Citation/ year	563.43
Citation/ paper	59.14
Author/ paper	6775.42
h-index	56
hI,norm	45
hI,annual	2.14
hA-index	21

Source: PoP, 2023

The research sample consists of scholarly papers on scientific learning media published within the last three years (2020-2023) and indexed by Google Scholar. This study's data collecting was finished on November 28, 2023. The research population consists of scientific articles about science learning media that are indexed by Google Scholar in scientific journals, conferences, books, or other forms of publication. Using the Publish or Perish (PoP) program, data is gathered by searching for "Cybersecurity Policy" on the Google Scholar page. The articles are journal articles, the search is limited to the years 2020-2023, and there can be no more than 200 search results. The data was gathered from two distinct journal websites. The next step was to tidy up the references using the Mendeley tool. References are required to ensure that all article metadata, such as author information, keywords, abstracts, and other features, are provided.

RESULTS AND DISCUSSION

To achieve the primary goal of this work, which is to classify Cyberscurity policy articles, VOSviewer software was used to create a map utilizing text data retrieved from the title and abstract fields. The binary counting method identified 1142 terms, which were then reduced

to 65 terms by establishing a minimum occurrence threshold of four times. The relevance score was then calculated for each of the 65 terms. The top 60%, or 39 terms, were selected automatically based on their relevancy scores. However, a human verification step is required to exclude extraneous phrases such as "editorial," "sample," and "abstract" from the final list.

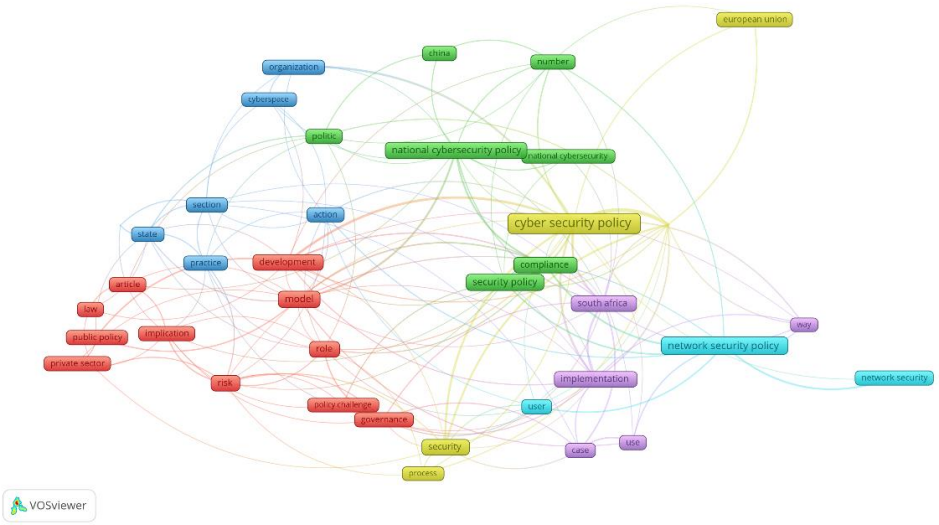

Figure 1. Network Visualization Map of Keyword
Source: VOSviewer, 2023

Figure 1 shows a visual representation of various clusters marked by colors such as blue, purple, yellow, red, light blue, and green. These clusters reveal notable trends, highlighting the prevalence of specific term within each and providing useful information. Table 3 provides access to further information.

Tabel 3. Clusters and keyword therein

Cluster	Total item	Most frequest keywords (occurences)	Keywords
1	12	Model(16), Development(13) ,Risk(10)	Article, development, future, governace, implication, law, model, policy challenge, private sector, public policy, risk, role
2	7	National cybersecurity policy(17), security policy(15), compliance(12)	China, compliance, national cybersecurity, national cybersecurity policy, number, politic, security policy
3	7	Practice(9), Organization(9), State(7)	Action, cyberspace, organization, policy option, practice, section, state
4	5	cyber security policy(44), cyber security(20), security(12)	Cyber security, Cyber security policy, European union, process, security
5	5	Implementation(10), south Africa(10)	Case, implementation, south Africa, user, way

6	3	network security policy(20)	Network security, Network security policy, user.

Source: VOSviewer, 2023

Figure 2 is an exemplary roadmap based on published research for addressing concerns about societal trends in transdisciplinary cooperative studies within information tourism research. Notably, Cluster 3 appears as a focal point, visually depicting the prevalence of terms like 'cyber security policy,' 'cyber security,' and 'security.' These recurring phrases in Cluster 3 give insight on common themes, implying a focus on investigating opportunities and tackling obstacles in the context of transdisciplinary information tourism research.

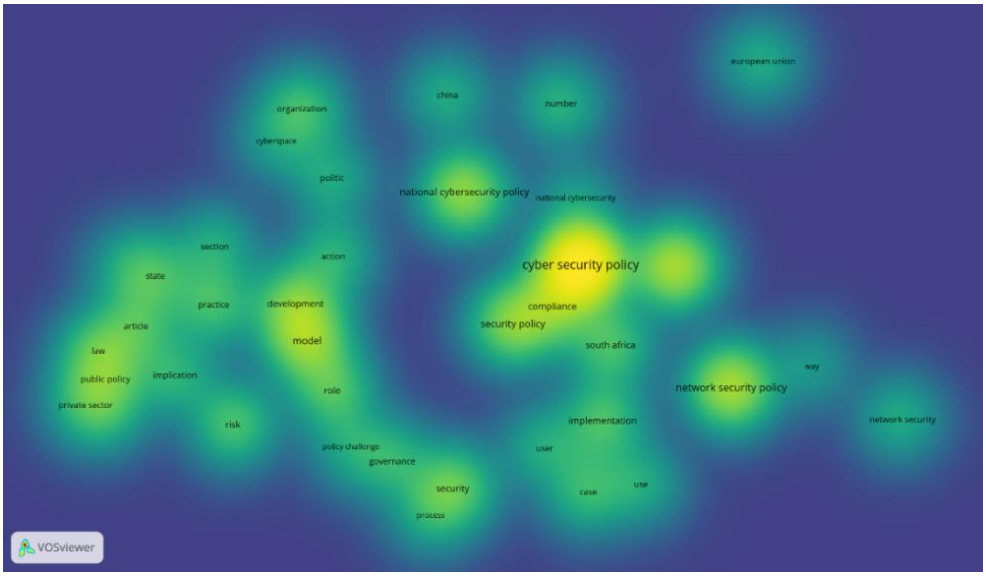

Figure 2. Density Visualization Map of Keywords

Source: VOSviewer, 2023

Keyword density visualizations provide a comprehensive perspective of phrase frequencies within a dataset in the context of Cybersecurity Policy. The terms 'Cyber Security Policy' 'Security Policy,' 'Compliance,' 'Model,' 'Network Security Policy,' and 'National Cybersecurity policy' appear frequently, indicating key emphasis points in the research topic. Notably, phrases such as 'politic,' 'cyberspace,' and 'way' appear less frequently in these keyword clusters, indicating possible research gaps. This insight suggests that more research in these areas is needed, showing the expanding landscape of Cyber Security policy and its potential alignment with global contexts, both present and future.

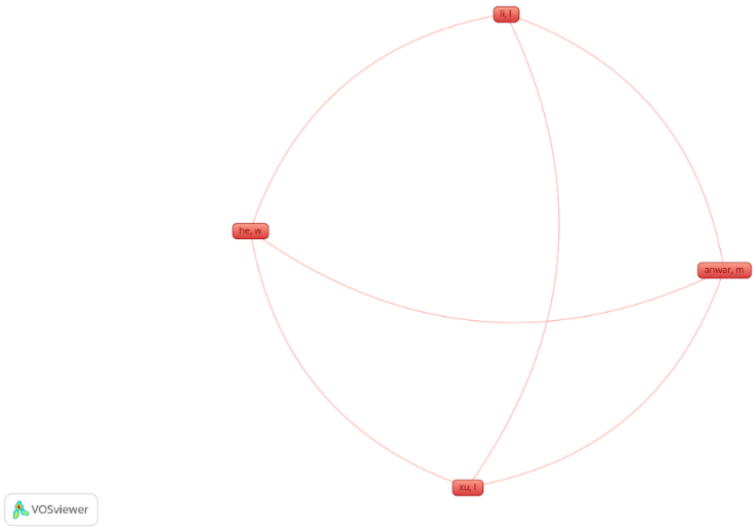

Figure 3. Network Visualization Map of Authors
Source: VOSviewer, 2023

Figure 3 clearly shows the top four contributors inside each different cluster, as indicated by a significant concentration of dots within each cluster boundary. The graphic representation emphasizes the writers' unique relationship with their respective publications, with W. He, L. Li, M, Anwar, and L. Xu each providing four papers in this scenario. When considering the hypothetical scenario of potential undermining, the importance of authorship integrity becomes clear. Table 4 calculations are scheduled to be completed on November 29, 2023, giving additional insights into the distribution and impact of contributions in the dataset

Tabel 4. The Top Five Cited Documents in Cybersecurity Policy

Citations	Authors and Year	Title
261	Y Li, Q Liu (2021)	A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments
85	Ameen, Nisreen, Tarhini, Ali, Shah, Mahmood, Madichie, Nnamdi, Paul, Justin, and Choudrie, Jyoti (2021)	A cross-cultural study of cybersecurity compliance and the Gen-Mobile workforce in international Business
62	Shappie, Alexander T. Dawson, Charlotte A. Debb, Scott M.(2020)	Personality as a predictor of cybersecurity behavior
59	Nadiya Kostyuk, Carly Wayne(2021)	The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public
57	Calderaro. A, JS Craig. A (2020)	Transnational Governance of Cybersecurity: policy challenges and global inequalities in cyber capacity building

Source: PoP, 2023

Direct quotations were common in Cybersecurity Policy documentation from 2020 to 2023, with an abundance of citations indicating extensive background research by the authors in the most recent materials. Turning to Table 5, we want to identify the research fields that have made a substantial contribution to the production of academic publications.

Tabel 5. The 15 Most and Fewer Occurences Terms in Bioinformatics

Occurrences	Term	Occurrences	Term
44	Cyber security policy	4	National cybersecurity
20	Network security policy	4	Cyberspace
20	Cyber security	4	Way
17	National cybersecurity policy	4	Policy option
16	Model	5	Future
15	Security policy	5	Policy challenge
13	Development	5	Process
12	Compliance	5	Network security
10	Security	6	Private sector
10	Risk	6	China
10	Role	6	Use
10	Implementation	6	Politic
10	South Africa	6	Section
9	Law	6	European union
9	Practice	6	User

Source: VOSviewer, 2023

A bibliometric examination of cybersecurity policy topics reveals considerable trends and scientific activity in this domain. The terms "cyber security policy" and "network security policy" stand out as focus topics in academic literature, demonstrating persistent attention. Their frequent appearance indicates continuous research and sustained interest. Similarly, "cyber security" and "national cybersecurity policy" emerge as key themes, indicating a vigorous scholarly conversation.

The phrases that appear less frequently in the context of cybersecurity policy give exciting potential for specialized scholarly research. "National cybersecurity," with its few mentions, inspires scholars to delve into the complexities of securing a country's digital infrastructure. Scholars in international relations, cybersecurity, and political science may look into the particular issues of protecting national cyberspace and the geopolitical ramifications of various approaches. The phrase "Cyberspace" has scholarly potential in the fields of computer science, philosophy, and law. Researchers can delve into cyberspace's conceptual underpinnings, studying the consequences for privacy, governance, and the shifting form of digital conflicts. This interdisciplinary approach could help researchers gain a better grasp of the virtual realm that lies beneath cybersecurity concerns. The term "policy option" provides doors for scholars in public policy, decision sciences, and political science. This research could focus on evaluating and proposing various policy approaches to address cybersecurity concerns. This could include the creation of decision models, comparative policy analysis, and the investigation of the efficacy of various strategic approaches.

Scholars can contribute to both fundamental and practical knowledge in their respective domains by investigating these words. Furthermore, interdisciplinary collaboration between law, political science, computer science, and public policy experts may improve the discourse surrounding these less usually stated terminology in the field of cybersecurity policy. Overall, these concepts give academics with niche areas in which to expand our understanding of crucial cybersecurity policy features and create a holistic approach to resolving new concerns.

CONCLUSION

This study provides an overview of the present state of cybersecurity policy research. It also proposes strategies to improve future research on this area. The findings will be beneficial to scholars and policymakers working in the ever-changing field of cybersecurity policy. Through bibliometric data analysis and cluster identification, major topics such as' Cyber security policy,' ' Network security policy,' and' Cyber security ' emerge, shedding light on both well-explored areas and underdeveloped territory such as ' National cybersecurity ' and ' Cyberspace ' These unknown aspects offer intriguing avenues for future research, harmonizing with current and predicted global situations. The identification of significant writers within clusters emphasizes the importance of author reputation in driving scholarly debates. Notably, the shift in citation patterns from 2020 to 2023 reflects the growth of scholarly methodology, stressing substantial background study over excessive dependence on direct citations.

This study delves into the field of cybersecurity policy research utilizing figures and technologies like Mendeley, VOSviewer, and PoP, with a focus on what's in the Google scholar index. In this study, we discovered that the way we talk about things is primarily focused on statistics. However, it is crucial to note that we also utilized our discretion, which may have resulted in errors. To strengthen future studies, we recommend looking at more papers from diverse sources, not only those in Google Scholar. To further compare and evaluate material, we also recommend using other programs such as BibExcel and HistCite. A complete study of the Cybersecurity Policy Research, utilizing bibliometric analysis and mapping approaches, finds important trends and gaps in this burgeoning field of cybersecurity policy. The Cybersecurity policy study lacks depth, making it a potential topic for future research in this increasing digital age, despite the fact that it is critical and affects the state, company, and society.

ACKNOWLEDGEMENTS

The author expresses gratitude to those who contributed to the realization of this journal, including friends, family, and course instructors Mr. Ade Bastian who have always guided us and encouraged us. And to Informatics, Faculty of Engineering, Universitas Majalengka for providing us with the opportunity to bring this journal to fruition.

REFERENCES

Aguillo, I. F. (2012). Is Google Scholar useful for bibliometrics? A webometric analysis.

Scientometrics, *91*(2), 343–351. https://doi.org/10.1007/s11192-011-0582-8

Brandão, A. P., & Camisão, I. (2021). Playing the market card: The commission's strategy to shape EU cybersecurity policy. *JCMS: Journal of Common Market Studies*, *60*(5), 1335–1355. https://doi.org/10.1111/jcms.13158

Bruijn, H. de, & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

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 and Privacy*, *18*(1), 8–10. https://doi.org/10.1109/MSEC.2019.2953368

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*(April), 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. *Journal of Cyber Policy*, *5*(2), 302–325. https://doi.org/10.1080/23738871.2020.1792956

Kostyuk, N., & Wayne, C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies*, *6*(2). https://doi.org/10.1093/jogss/ogz077

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*(February 2018), 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lilli, E. (2020). President Obama and US cyber security policy. *Journal of Cyber Policy*, *5*(2), 265–284. https://doi.org/10.1080/23738871.2020.1778759

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*, *22*(2), 1–35. https://doi.org/10.3390/s22020538

Nandiyanto, A. B. D., & Al Husaeni, D. F. (2022). Bibliometric analysis of engineering research using vosviewer indexed by Google Scholar. *Journal of Engineering Science and Technology*, *17*(2), 883–894.

Rizal, M., & Yani, Y. (2016). Cybersecurity policy and iIts implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Sharma, D., Mittal, R., Sekhar, R., Shah, P., & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. *Results in Control and Optimization*, *10*(2), 100204. https://doi.org/10.1016/j.rico.2023.100204

Shively, J. (2021). Cybersecurity policy and the Trump administration. *Policy Studies*, *42*(5–6), 738–754. https://doi.org/10.1080/01442872.2021.1947482

Smith, K. J., Dhillon, G., & Carter, L. (2021). User values and the development of a cybersecurity public policy for the IoT. *International Journal of Information Management*, *56*, 102123. https://doi.org/10.1016/j.ijinfomgt.2020.102123

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

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Sulardja, E. C. (2021). Analisis bibliometrik publikasi ilmiah bidang digital asset management berbasis data Scopus 2011-2020. *Informatio: Journal of Library and Information Science*, *1*(3), 259. https://doi.org/10.24198/inf.v1i3.35339

Zakiyyah, F. N., Winoto, Y., & Rohanda, R. (2022). Pemetaan bibliometrik terhadap perkembangan penelitian arsitektur informasi pada Google Scholar menggunakan VOSviewer. *Informatio: Journal of Library and Information Science*, *2*(1), 43. https://doi.org/10.24198/inf.v2i1.37766