A BIBLIOMETRIC ANALYSIS OF CYBER RESILIENCE FROM 2000 TO 2024

[1] **Lilik Muslikhatin**
PhD Candidate
Defence University, Indonesia
muslikhatin.lilik@gmail.com
[2] **Rodon Pedrason**
Lecturer
Defence University, Indonesia
yoedhiswastanto83@gmail.com
[3] **Yoedhi Swastanto**
Defence University, Indonesia
yoedhi.swastanto@idu.ac.id
[4] **Rudi Laksmono**
Defence University, Indonesia
rlwidayatno@gmail.com

Keywords:
Bibliometric, Cyber Resilience, OpenAlec, VOSviewer;
Bibliometric, Ketahanan Siber, OpenAlec, VOSviewer

Abstract
The issue of cyber resilience is a growing global concern, as it reflects a country's ability to prepare for, absorb, recover from, and adapt to cyber threats and attacks. Weak cyber resilience can intensify the rise of digital crimes, making nations more vulnerable to disruption. This study aims to explore and analyse the development of cyber resilience research from 2000 to 2024 through a bibliometric approach. Data was collected from three major academic databases, Scopus, OpenAlex, and Google Scholar which are using relevant keywords such as cyber resilience, cyber security, cybercrime, and cyber defence. VOSviewer software was utilized to create network visualizations that map the connections between authors, research topics, institutions, countries, and keywords. The findings reveal a significant increase in scholarly publications over the years, indicating a growing global interest in this domain. Key research areas such as Cyber-Physical Systems (CPS), cyber resilience strategies, and social technologies have shown notable development. Furthermore, the focus of research has gradually shifted from purely technical aspects to more interdisciplinary themes involving public policy, international relations, risk governance, and the social sciences. The COVID-19 pandemic served as a turning point, amplifying research on societal impacts, remote work vulnerabilities, and risk communication. This evolution emphasizes the need for a holistic and integrated research agenda. The study concludes that international cooperation among scholars and institutions is crucial to strengthen cyber resilience. Future research directions should emphasize multidisciplinary and multimodal approaches to navigate the increasingly complex and

interconnected landscape of cyber resilience, particularly in emerging domains such as social media governance, digital democracy, and AI-driven security.

Abstrak

Isu ketahanan siber (cyber resilience) semakin menjadi perhatian global karena mencerminkan kemampuan suatu negara dalam mempersiapkan diri, menyerap, pulih dari, dan beradaptasi terhadap ancaman serta serangan siber. Ketahanan siber yang lemah dapat memperparah peningkatan kejahatan digital dan membuat suatu negara rentan terhadap gangguan. Studi ini bertujuan untuk mengeksplorasi dan menganalisis perkembangan penelitian tentang ketahanan siber dari tahun 2000 hingga 2024 melalui pendekatan bibliometrik. Data dikumpulkan dari tiga basis data akademik utama yaitu Scopus, OpenAlex, dan Google Scholar dengan menggunakan kata kunci seperti cyber resilience, cyber security, cybercrime, dan cyber defense. Perangkat lunak VOSviewer digunakan untuk memvisualisasikan jaringan yang mencakup hubungan antar-penulis, topik penelitian, institusi, negara, dan kata kunci. Hasil penelitian menunjukkan peningkatan signifikan dalam jumlah publikasi ilmiah sepanjang periode tersebut, menandakan meningkatnya minat global dalam bidang ini. Area penelitian utama seperti Cyber-Physical Systems (CPS), strategi ketahanan siber, dan teknologi sosial mengalami perkembangan yang signifikan. Selain itu, fokus penelitian telah bergeser dari aspek teknis semata menuju kajian-kajian interdisipliner yang melibatkan kebijakan publik, hubungan internasional, tata kelola risiko, dan ilmu sosial. Pandemi COVID-19 menjadi pemicu penting yang mendorong penelitian terkait dampak sosial, kerentanan kerja jarak jauh, dan komunikasi risiko. Perkembangan ini menekankan perlunya agenda riset yang lebih holistik dan terintegrasi. Studi ini menyimpulkan bahwa kolaborasi global antarpeneliti dan lembaga sangat penting untuk memperkuat ketahanan siber. Arah penelitian di masa depan sebaiknya menekankan pendekatan multidisipliner dan multimodal guna menjawab tantangan kompleks dalam lanskap ketahanan siber, khususnya di ranah yang tengah berkembang seperti tata kelola media sosial, demokrasi digital, dan keamanan berbasis kecerdasan buatan (AI).

BRAWIJAYA JOURNAL of SOCIAL SCIENCE

Vol. 5, No. 1, 2025

DOI: https://doi.org.10.21776/ub.bjss.2025.005.01.1

Submitted: 2025-06-02
Accepted: 2025-12-08

1. Introduction

A The issue of cyber resilience demands serious attention from all groups and is a pressing issue for countries around the world. The threat of cybercrime continues to grow, becoming more sophisticated, more massive and more destructive (Hagen, 2018). Virus attacks in ransomware (Humayun et al., 2021), data theft (Deepthi et al., 2023), and cyber sabotage (Tsaruk & Korniiets, 2020), force all elements of the state to increase their capabilities in responding to and mitigating these risks (Dickson & Goodwin, 2019). One of the European Union action is to create a Cyber Resilience Act 2022 to complement the cybersecurity framework (Shaffique, 2024). Indonesia has also issued Law No. 1 2024 as the second revision of the Law on Electronic Information and Transactions (UU ITE) of 2008 (bpk, 2024), which regulates the procedures for the use and utilization of technology including cybersecurity governance and resilience.

The concept of cyber resilience refers to the ability to prepare, absorb, recover, and adapt to cyber attacks and threats (Ding et al., 2025). In agreement with Ding et al. Cyber researchers from Ukraine, Poland, the US and Czech Republic stated that the level of cyber resilience of a country is influenced by factors such as internet penetration, the number of mobile device subscriptions, and the density of security breaches (Lyeonov et al., 2024a). The strength or weakness of a country's cyber resilience affects the prevalence of digital crimes (Samia et al., 2024). Based on the report of Cybersecurity Ventures, global losses due to cybercrime are estimated to reach 6 trillion US dollars in 2021 and are predicted to increase to 10.5 trillion US dollars in 2025 (Cybersecurity Ventures, 2021), by 2025, the cost of cybercrime would increase by 15% yearly worldwide (Matić Bošković, 2023).

Cyber resilience is a crucial aspect in maintaining the economic (Teoh & Mahmood, 2017), social sector (Saniuk et al., 2022), and political stability of a country (Adelmann et al., 2020; Nguyen et al., 2022). The increasingly complex cyber threats affect not only state entities but also non-governmental organizations (Y. Li & Liu, 2021), the military (Bogdanoski, 2022), companies and individuals (Al-Kateb et al., 2024; Dupont et al., 2023; Yıldız & Simsekler, 2023). Cyberattacks can have devastating impacts in financial losses (Lagazio et al., 2014), reputational damage, and even death in industries with vital infrastructure (Dupont, 2019), such as healthcare and energy (de Peralta et al., 2020). Cybersecurity is used in various crucial aspects of life to ensure the confidentiality and integrity of sensitive information (Admass et al., 2024).

Therefore, this study aims to explore information and conduct a comprehensive analysis of the research status and describe the development trends of research in the field of cyber resilience from 2000 to 2024. With a systematic bibliometric analysis approach (Aria & Cuccurullo, 2017), this study identifies trends, research gaps, and opportunities in academic literature related to this topic (Serafin et al., 2019; Singh et al., 2024). The results of this study are expected to provide new insights for policy makers, academics, and practitioners in designing more inclusive and effective strategies in dealing with global cyber threats. We used VOS viewer software to conduct data analysis and visualization (Lyeonov et al., 2024b). We also used the openalex.org website to identify research trends in the field based on keywords (Aria et al., 2023).

2. Research Methods

2.1 Bibliometric Analysis

The methodology used in this study includes quantitative analysis using a systematic bibliometric approach. Bibliometrics is an effective tool for evaluating developments and trends in a particular field, Singh et al. (2024) also stated that this method is used to identify authors, journals, and institutions that contribute significantly to the literature (Singh et al., 2024). Bibliometric analysis in this study was used to analyze existing literature on research in the context of cyber resilience. Several bibliometric researchers such as Ho and Luong (2022) stated that the bibliometric approach allows researchers to explore research trends, find gaps in the literature, and provide insight into future research prospects (Ho & Luong, 2022). According to Aria and Cuccurullo (2017), the data collection process begins with the identification of relevant keywords, including "cyber resilience". In addition, academic databases such as Scopus (Valencia-Arias et al., 2024), OpenAlex (Aria et al., 2023) and Google Scholar (Ho & Luong, 2022) were used to collect relevant articles. This study includes articles published between 2000 and 2024, to ensure that the analyzed data covers the latest developments in this field.

2.2 Search Strategy

The search strategy used in this study used various combinations of keywords to ensure a broad coverage. In addition to the main keywords, the researcher also used related terms such as "cybersecurity", "cybercrime", and "cyber defence". In addition, keywords such as digital, Internet of Things, cybercrime, information system, smart grid and technology were also used to filter publications to suit the research objectives. As part of the search strategy, the researcher also considered using filters available in the database to filter the results based on publication type, year of publication, and language. This helped in identifying articles that best suited the focus of the study.

Article search was conducted on the openalec.org website application. The collected articles were stored in RIS or CSV format as needed in data processing. To obtain a bibliometric diagram, researchers processed the data using VOSviewer software. By using bibliometric analysis software such as VOSviewer (Eck & Waltman, 2010), the researcher was able to visualize the relationships between these concepts and identify patterns that may not be apparent in manual analysis. However, previously researchers filtered the publications to be processed using the PRISMA diagram (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Cantelmi et al., 2021)

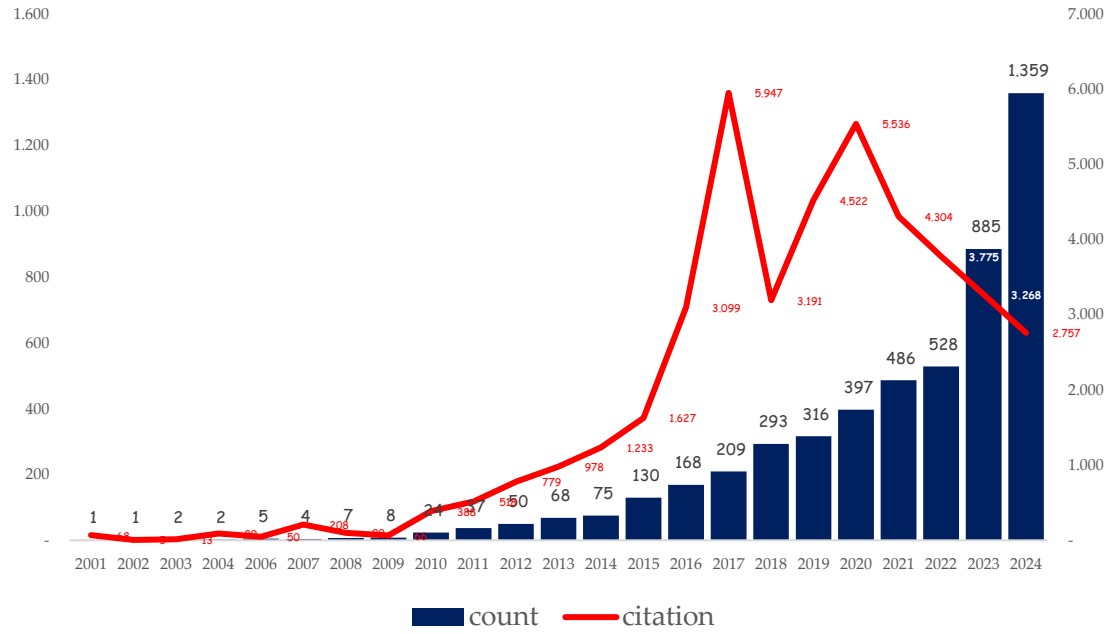
3. Results and Analysis

In this section, the results of data processing that are in accordance with the research questions identified at the beginning will be illustrated in the following figures and tables:

3.1 Publications Trend

Figure 1 shows the development of the number of publications related to cyber resilience from 2000 to 2024 along with the number of citations in the respective years.

Fig.1. Publications trend by count of publications and citations



Source: Data processed by researchers from OpenAlec.org (keywords: cyber resilience)

Over the past 25 years, research on cyber resilience has grown rapidly as more and more cybersecurity issues have hit various sectors. In 2001, only 1 article was published, but since 2015, research has been recorded at over 100 articles, while research in 2024 is almost 3 times than that of 2022.

Over the past 2 and a half decades, cyber resilience researchers have continued to create articles. However, the number of citations to the issue of cyber resilience has fluctuated. The highest citations occurred in 2017, which then experienced a sharp decline in 2018 and then climbed back up until 2020. However, after 2020 to 2024, the number of citations continued to experience a sharp decline.

3.2 Authors Productivity

3.2.1 The Most Productive Authors

Table 1 displays the ten most productive authors based on the number of articles and total citations by each author during the period 2000 to 2024.

Table 1. The Ten Most Productive Authors

No	Author	Number of publications	Number of Citations	Citation average per publication
1	Alexander Kott	28	623	22
2	Igor Linkov	26	1038	40
3	Quanyan Zhu	26	399	15
4	Katherine Davis	25	163	6
5	Xenofon Koutsoukos	21	228	10

6	Craig Rieger	19	221	11
7	Sachin Shetty	18	168	9
8	Anurag K. Srivastava	17	347	20
9	Deepa Kundur	16	428	26
10	Mohammad Shahidehpour	15	879	58

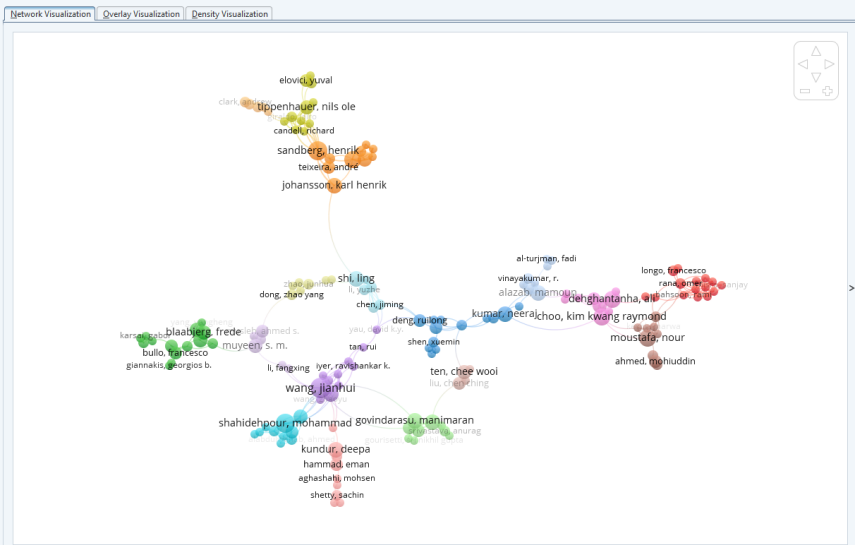
Source: Data processed by researchers from OpenAlec.org (keywords: cyber resilience)

Although Alexander Kott has written more articles than other researchers, the most cited article is Igor Linkov's work with over 1000 citations. Meanwhile, Mohammad Shahidehpour, who only wrote 15 articles, has more citations and average citations per publication than other researchers who have published more. In terms of citations, the 3 articles on cyber resilience with the most citations are Resilience metrics for cyber systems by Igor Linkov got 264 citations (Linkov et al., 2013). Front Lines Against the Darkness: Enhancing the Resilience of the Electricity Grid Through Microgrid Facilities by Mohammad Shahidehpour has been cited 196 times since 2016 (Gholami et al., 2016). Operational resilience: concepts, design and analysis by Alexander Kott, 2016 has been cited 171 times (Ganin et al., 2016). However, if we look more closely, the article entitled A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications by Wei Yu in the IoT journal has been cited 2442 times since 2017 (Lin et al., 2017).

3.2.2 Co-Authorship Authors

Figure 3 shows collaboration between authors through network visualization (threshold 2 articles for an author, 490 authors are shown). This figure shows the collaboration network between academic authors based on connectivity through co-authorship. Each node represents an author, and the lines (edges) indicate that they have co-authored one or more publications. Different colours indicate groups (clusters/communities) of authors who collaborate more frequently with each other. The size of the node reflects the degree of connectivity (degree centrality), the larger it is, the more collaborations with other authors.

Fig.2. Network Visualization of Co-Authorship Author (threshold: 3 articles each author)



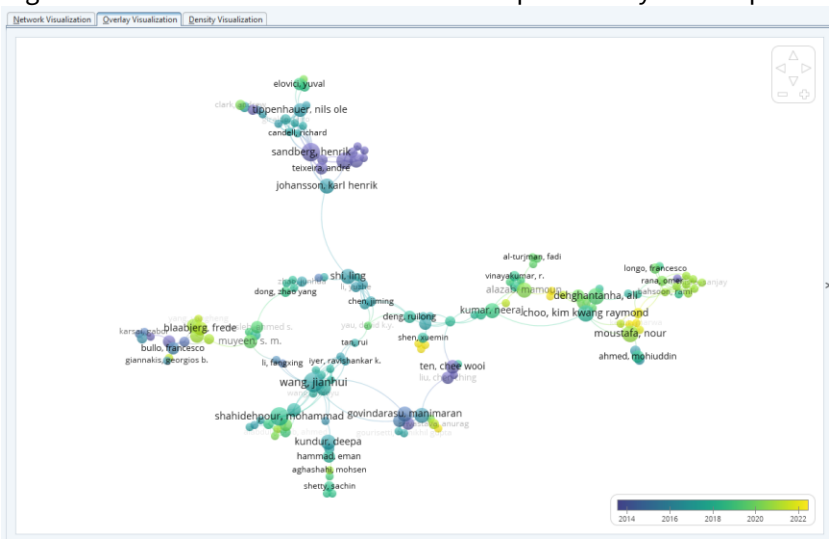
Source: Visualization by VOSviewer

Several groups of authors were identified based on colour and geographic/thematic proximity. The orange cluster is centred on authors such as Sandberg, Henrik, Johansson, Karl Henrik, And Teixeira, Andre. This cluster focuses on the technology and control system aspects of cyber defence such as Cyber-Attack on Remote State Estimation and Supervisory Control and Data Acquisition (SCADA) systems operating in power grids (Guo et al., 2017; Teixeira et al., 2010). The Blue Cluster is led by Ruiqing, Ruoyun, Chen, Jiming, And Shi, Ling, acts as a liaison between several other clusters, marked by the presence of nodes that bridge to the purple and red clusters. Focuses on data and network security topics, as well as developing technical solutions to cyber attacks.

The pink and red clusters are quite dense, with authors such as Kim-Kwang Raymond Choo, Nour Moustafa, And Francis Longo. These authors conduct research on IoT, cybercrime, digital forensics, and cyber threat intelligence, given that many of these names are active in publications on digital crime and policy responses (Al-Hawawreh et al., 2021; Choo, 2021). The Green and Toska clusters with authors such as Shahidehpour, Mohammad And Govindarasu, Manimaran dominates this cluster, this cluster focuses on cyber resilience of critical infrastructure, such as energy or utility systems, which are prime targets of large-scale cyberattacks (Z. Li et al., 2018). The Yellow Cluster consists of authors such as Zhao Yang Dong and Shi Ling, focusing on strategic policies and integration of cybersecurity into organizational and national risk management systems (Liang, 2019).

Meanwhile the visualization in Figure 4 not only shows the relationships between authors, but also shows the time development of their involvement in publications, which is marked by a colour gradient from purple (earlier years, around 2014) to bright yellow (more recent years, around 2022). Most of the nodes are bluish green to light yellow, indicating that active collaboration in this field took place intensively in the 2018 – 2022 time span. There are fewer dark purple nodes, indicating that early authors (pre-2016) were more limited and have now joined a broader collaboration ecosystem.

Fig.3. Network Visualization of Co-Authorship Author by articles period



Source: Visualization by VOSviewer

Labels and circles represent each author's item; the size of the labels and circles depends on the item's weight, which is calculated from the total publications. The thickness of the lines depends on the authors' ability to collaborate (van Eck & Waltman, 2014). Cluster led by Sandberg, Henrik And Johansson, Karl Henrikshowing a dominance of purple and blue, indicating that their contributions have been made since the beginning and are pioneers in a particular field, perhaps related to control systems or technical security. The cluster on the right side (such as that which includes Kim-Kwang Raymond Choo, Nour Moustafa, Francis Longo) shows many bright yellows to green dots. This indicates that the group is relatively new to publishing and is likely involved in current topics, such as digital forensics, cyber threat intelligence, and AI-based cybercrime.

Some writers, such as Shi Ling, Ruoyun Ruiqing, And Wang Jianhui, appear to be a connecting point between clusters with varying colors, from purple to yellow. This indicates that they are active in the long term and play a significant role in bridging collaboration across generations and topics. The widespread yellow color across clusters indicates that interest in cyber issues has increased rapidly in recent years, and collaboration has expanded. This is in line with the increasing global urgency of cyber threats and the importance of digital defense in both the public and private sectors.

3.3 Author's Institutions

3.3.1 The Most Productive Institutions

Table 2 shows the ten most productive author's institutions based on the number of articles and total citations of each institution.

Table 2. The ten most productive author's institutions

No	Authors Institutions	Number of articles	Total Citations
1	United States Department of Energy	166	2770
2	United States Department of Defense	81	1464
3	Office of Science	81	1957
4	Battelle	75	1132
5	Pacific Northwest National Laboratory	50	948
6	United States Department of the Army	48	1290
7	National Nuclear Security Administration	46	529
8	Centre National de la Recherche Scientifique	40	484
9	United States Army Combat Capabilities Development Command	36	1020
10	United States Army Futures Command	36	1020

Source: Data processed by researchers from OpenAlec.org (keywords: cyber resilience)

Based on the author's institution, the United States Department of Energy has produced the most publications in the last 2 and a half decades, as well as the publication with the most citations among other institutions. The article Sequential Service Restoration for Unbalanced Distribution Systems and Microgrids by Bo Chen et al. has been cited 292 times since 2017 (Chen et al., 2018). Meanwhile, the United States Army Combat Capabilities Development Command and the United States Army Futures Command have each published 36 articles, the fewest of the other

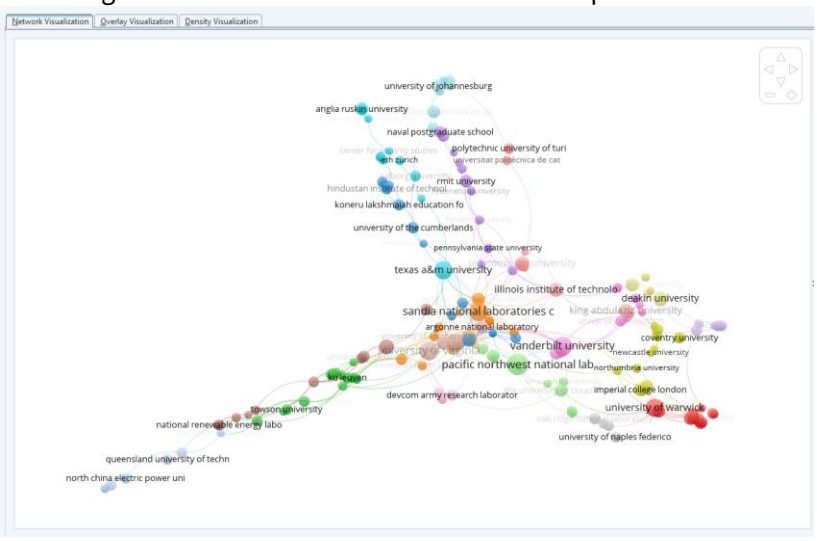
8 institutions, but the number of citations obtained is greater than the institutions that have published more publications. The article entitled Resilience metrics for cyber systems, which is a collaboration between authors from the United States Department of Defense, United States Army Combat Capabilities Development Command, United States Army Futures Command and United States Department of the Army, has been cited 264 times since 2013 (Linkov et al., 2013).

3.3.2 Co-Authorship Institutions

Figure 4 shows the network of co-authorship by institutions involved in research on cyber topics such as cybersecurity, cyber-physical systems, and cyber resilience. Nodes in the visualization represent academic, research, or military institutions, while colours indicate clusters of collaboration based on thematic and collaborative links between institutions.

Sandia National Laboratories and Pacific Northwest National Laboratory are important institutions hubs in the network, indicating that they are key collaborators in many publications. Their central location and high connectivity indicate their high influence and extensive network of research partners. Europe and Australia Cluster: Universities such as Deakin University, University of Warwick, and Imperial College London are closely networked with Coventry University and Northumbria University. United States and Military Cluster: Includes Texas A&M University, Naval Postgraduate School, and Devcom Army Research Laboratory. Asia–Europe Cluster: There is a presence of institutions such as ETH Zurich, Hindustan Institute of Technology, and Koneru Lakshmaiah Education Foundation, strengthening the research network across continents.

Fig.4. Network visualization of Co-authorship institution



Source: Visualization by VOSviewer

Several institutions such as the Devcom Army Research Laboratory, the National Renewable Energy Laboratory, and the Argonne National Laboratory stand out. This indicates the strong involvement of the military and energy sectors in the development of cyber technology and its security. It is apparent that the contribution from Asian institutions such as those from China or Southeast Asia is relatively small and is on the periphery of the network, for example the North China Electric Power University and several others. This shows the potential for strengthening international cooperation that can still be developed further.

3.4 Author's Countries

3.4.1 The most productive countries

Table 3 shows the top ten countries that most frequently produce articles based on the number of publications and total citations from each author's country. According to the author's country, the USA is still the country with the highest number of publications and citations compared to other countries. However, if we look further, even though China publishes articles slightly below the United Kingdom of Great Britain and Northern Ireland, the number of citations of articles from China is almost twice as much as the citations of publications from Prince Charles' country.

The three most cited articles by other researchers are the article entitled A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications written collaboratively by researchers from China and the USA has been cited 2,442 times since 2017 (Lin et al., 2017), then Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison has been cited 966 times since 2019 which is the work of Fei Tao et al. authors from China, Stockholm and Singapore (Tao et al., 2019). Next is Ten Years of Industrie 4.0 by Henning Kagermann and Wolfgang Wahlster both from Germany has been cited 779 times since 2022 (Kagermann & Wahlster, 2022).

Table 3. The ten most productive author's counties

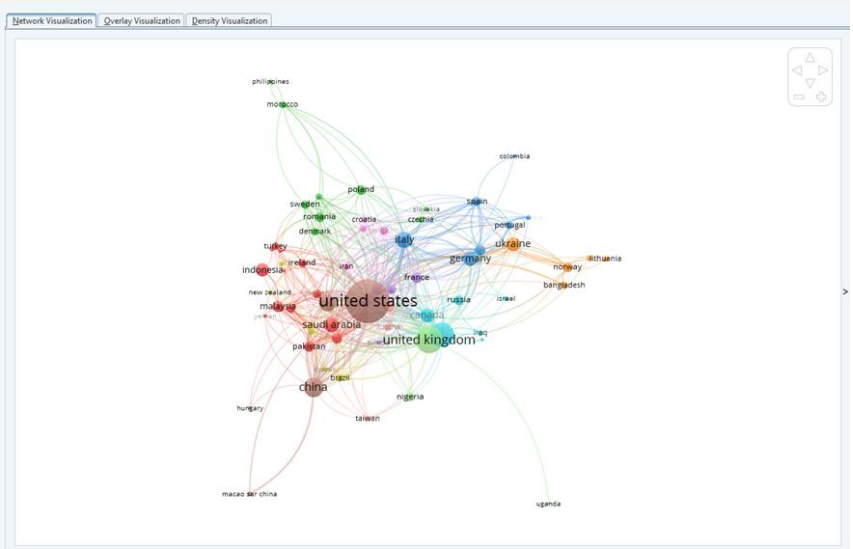
No	Authors' country	Number of publications	Number of Citations
1	United States of America	1158	18320
2	United Kingdom of Great Britain and Northern Ireland	372	3856
3	China	278	7056
4	India	277	1090
5	Italy	162	1393
6	Germany	134	1895
7	Australia	133	1678
8	Canada	130	2172
9	France	113	850
10	Saudi Arabia	91	1372

Source: Data processed by researchers from OpenAlec.org (keywords: cyber resilience)

3.4.2 Co-authorship countries

Figure 10 shows network collaboration among countries in scientific publications relevant to a research topic (related to cybersecurity, IoT, AI, or other technology fields). Each node represents a country, while the connecting lines (edges) show collaborative relationships in the form of joint publications. The size of the node indicates the number of publications, and the thickness and number of connections reflect the intensity of collaboration with other countries.

Fig.5. Network visualization of Co-authorship countries



Source: Visualization by VOSviewer

United States being the largest and most connected network hub, demonstrating great dominance and influence in global research collaboration. The country is closely connected to many countries, including United Kingdom, Germany, China, India, And Canada. Several groups of countries form their own clusters based on geographical proximity or similar research interests, including the Western and Central European Cluster in blue & purple, namely Germany, Italy, Spain, France, Portugal, Poland, and Scandinavian countries, showing close regional collaboration. The red cluster, namely East Asia and the Middle East, consists of China, Saudi Arabia, Pakistan, Iran, and Indonesia, which are interconnected, some are also connected to the US and UK. The green Southeast Asia and Africa cluster includes Indonesia, Malaysia, Nigeria, and Uganda, which are also connected to several large countries such as the UK and US, but are more peripheral. The orange Nordic & Baltic Cluster consists of Norway, Lithuania, and Bangladesh, forming limited regional collaboration but emerging as a separate network.

The UK is the second largest node after the US, demonstrating its important role as a link between European, Asian and African countries. The UK is seen to be connected to countries such as India, Nigeria, Malaysia and Pakistan. It is apparent that collaboration between countries in the Global South (e.g. Africa, Southeast Asia, Latin America) is still highly dependent on connectivity with central countries such as the US, UK and China. Direct connections between Southern countries are not widely visible and are still very limited. Countries such as Philippines, Colombia, Morocco, And Uganda appear in peripheral positions, with a small number of connections and node sizes. This indicates lower or limited participation in global research collaborations in the field being studied.

3.5 Co-Occurrence Keywords

3.5.1 The highest frequency appearing keywords

Table 4 shows keywords that frequently appear together within a given context such as in the same document, paragraph or dataset in cyber resilience research. In text analysis, natural

language processing (NLP), and information retrieval, co-occurrence analysis is used to identify relationships or associations between terms.

Table 4. The top 10 high-frequency appearing keywords as below

Rank	Keywords	Counts	Rank	Keywords	Counts
1	Resilience	3.383	6	Robustness	121
2	Cyber-physical system	977	7	SCADA	107
3	Cyber threats	359	8	Cyberwarfare	97
4	Vulnerability	277	9	Microgrid	96
5	Cyber-attack	202	10	Critical infrastructure protection	93

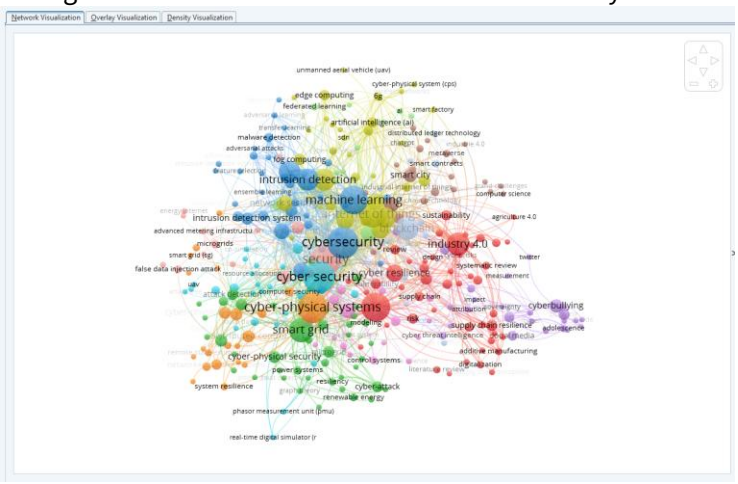
Source: Data processed by researchers from OpenAlec.org (keywords: cyber resilience)

Keywords are words that are considered important by the author which aim to make it easier for readers to find words according to the research. From table 6 it can be concluded that the most frequently appearing keywords in various studies on cyber resilience are Resilience which appears as many as 3,383 followed by Cyber-physical system, Cyber threats, Vulnerability and Cyber-attack. While critical Robustness, SCADA, Cyberwarfare, Microgrid Critical infrastructure protection appear below 125 times.

3.5.2 The most frequently appeared keywords collaboration

Fig. 6 is a network visualization of the cyber resilience research topic. This visualization displays the relationships and associations between keywords or research topics that frequently appear together in the scientific literature.

Fig.6. Network Visualization of Co-Occurrence keywords



Source: Visualization by VOSviewer

Each node (dot) represents a keyword/topic, and the colour indicates a cluster or community of closely related topics. The size of the node reflects the frequency or importance of the topic in the network. Edges between nodes indicate the relationship or co-existence of topics in a document or publication. Some important clusters that are visible include the blue colour that focuses on the topic machine learning, intrusion detection, And cybersecurity. The green colour

represents the relationship between cyber-physical systems, smart grid, And power systems. The red colour contains related topics, industry 4.0, blockchain, smart city, And digitalization. Purple colour shows topics around cyberbullying, social media, And adolescence. This visualization helps in understanding the research landscape, identifying key emerging topics, and seeing potential cross-disciplinary collaborations. For example, the relationship between machine learning and cyber security.

4. Conclusion and Suggestion

This bibliometric analysis offers a comprehensive overview of the evolution of cyber resilience research from 2000 to 2024. The study reveals a significant increase in scholarly attention to the topic, demonstrating its rising importance in the context of global digital transformation. The trajectory of the research shows a clear shift from technical and infrastructure-oriented studies in the early years toward more holistic approaches that consider social, political, and governance-related dimensions. This indicates a growing understanding that cyber resilience is not solely a technological concern but also a socio-political issue that requires multidimensional frameworks. The analysis of authorship and collaboration patterns further highlights a diversification of contributors and the rise of interdisciplinary engagement. These trends suggest a maturing and expanding field that recognizes the complexity of modern cyber threats. By identifying key themes, influential publications, and research gaps, this study contributes to a deeper understanding of how the field has evolved and where it is heading. Ultimately, the findings emphasize the urgent need for integrated, inclusive, and adaptive strategies to build cyber resilience in an increasingly interconnected and vulnerable digital world.

Based on the findings of this bibliometric analysis, several suggestions are proposed to enhance the future development of cyber resilience research. First, researchers are encouraged to adopt more interdisciplinary perspectives that combine insights from technology, social sciences, policy studies, and behavioural sciences. This is essential to fully capture the complexity of cyber resilience, which increasingly intersects with governance, societal trust, and democratic stability. Second, future studies should focus on developing more refined theoretical models and methodological tools to measure cyber resilience across diverse contexts, including governmental, private, and civil society sectors.

In addition, more attention should be given to exploring region-specific challenges and opportunities, especially in developing countries where digital infrastructure and cyber capacity vary widely. Expanding the scope of research to include the Global South will promote more equitable and inclusive cyber resilience frameworks. Researchers are also advised to engage with policymakers and industry practitioners to ensure that academic insights are translated into actionable strategies. Finally, fostering international and institutional collaborations will be crucial in building a resilient global digital ecosystem capable of withstanding complex and evolving cyber threats.

References

Adelmann, F., Ergen, I., Gaidosch, T., Jenkinson, N., Morozova, A., Schwarz, N., & Wilson, C. (2020). Cyber Risk and Financial Stability: It's a Small World After All. In *Staff Discussion Notes* (Vol. 2020, Issue 007). books.google.com. https://www.elibrary.imf.org/view/journals/006/2020/007/article-A001-en.xml

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future

directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/https://doi.org/10.1016/j.csa.2023.100031

Al-Hawawreh, M., Moustafa, N., Garg, S., & Hossain, M. S. (2021). Deep Learning-Enabled Threat Intelligence Scheme in the Internet of Things Networks. In *IEEE Transactions on Network Science and Engineering* (Vol. 8, Issue 4). ieeexplore.ieee.org. https://doi.org/10.1109/TNSE.2020.3032415

Al-Kateb, G. E., Khaleel, I., & Aljanabi, M. (2024). CryptoGenSec: A Hybrid Generative AI Algorithm for Dynamic Cryptographic Cyber Defence. In *Deleted Journal* (Vol. 4, Issue 3). https://doi.org/10.58496/mjcs/2024/013

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959–975. https://doi.org/https://doi.org/10.1016/j.joi.2017.08.007

Aria, M., Le, T., Cuccurullo, C., Belfiore, A., & Choe, J. (2023). openalexR: An R-Tool for Collecting Bibliometric Data from OpenAlex. *R Journal*, *15*(4), 167–180. https://doi.org/10.32614/RJ-2023-089

Bogdanoski, M. (2022). Building cyber Resilience against hybrid treats. In *Building Cyber Resilience against Hybrid Threats*. IOS Press. https://doi.org/10.3233/nicsp61

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. In *Environment Systems and Decisions* (Vol. 41, Issue 3, pp. 341–376). Springer. https://doi.org/10.1007/s10669-020-09795-8

Chen, B., Chen, C., Wang, J., & Butler-Purry, K. L. (2018). Sequential Service Restoration for Unbalanced Distribution Systems and Microgrids. *IEEE Transactions on Power Systems*, *33*(2), 1507–1520. https://doi.org/10.1109/TPWRS.2017.2720122

Choo, K.-K. R. (2021). *Internet of Things (IoT) Security and Forensics*. https://doi.org/10.1145/3462633.3484691

de Peralta, F. A., Gorton, A. M., Watson, M. D., Bays, R. M., Boles, J. R., Gorton, B. T., Castleberry, J. E., & Powers, F. E. (2020). Cybersecurity resiliency of marine renewable energy systems–part 1: Identifying cybersecurity vulnerabilities and determining risk. *Marine Technology Society Journal*, *54*(6), 97–107. https://doi.org/10.4031/MTSJ.54.6.9

Deepthi, M., Harini, M., Geethika, P. S., Kalyan, V., & Kishor, K. (2023). Data Classification of Dark Web using SVM and S3VM. In *International Journal for Research in Applied Science and Engineering Technology* (Vol. 11, Issue 9). International Journal for Research in Applied Science and Engineering Technology (IJRASET). https://doi.org/10.22214/ijraset.2023.55643

Dickson, F., & Goodwin, P. (2019). Five Key Technologies for Enabling a Cyber-Resilience Framework UPDATED REPORT. In *IDC Analyze The Future* (Issue August). kyndryl.com. https://www.kyndryl.com/content/dam/kyndrylprogram/en/services/security-and-resiliency/idc-five-key-technologies_2020-new_final_87017287USEN.pdf

Ding, W., Abdel-Basset, M., Ali, A. M., & Moustafa, N. (2025). Large language models for cyber resilience: A comprehensive review, challenges, and future perspectives. *Applied Soft Computing*, *170*, 112663. https://doi.org/https://doi.org/10.1016/j.asoc.2024.112663

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. In *Journal of Cybersecurity* (Vol. 5, Issue 1). academic.oup.com. https://doi.org/10.1093/cybsec/tyz013

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers and Security*, *132*. https://doi.org/10.1016/j.cose.2023.103372

Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., & ... (2016). Operational resilience: concepts, design and analysis. In *Scientific reports*. nature.com. https://www.nature.com/articles/srep19540.

Gholami, A., Aminifar, F., & Shahidehpour, M. (2016). Front Lines Against the Darkness: Enhancing the Resilience of the Electricity Grid Through Microgrid Facilities. *IEEE Electrification Magazine*, *4*(1), 18–24. https://doi.org/10.1109/MELE.2015.2509879

Guo, Z., Shi, D., Johansson, K. H., & Shi, L. (2017). Optimal Linear Cyber-Attack on Remote State Estimation. *IEEE Transactions on Control of Network Systems*, *4*(1), 4–13. https://doi.org/10.1109/TCNS.2016.2570003

Hagen, J. (2018). Building resilience against cyber threats in the energy sector. In *International Journal of*

Critical Infrastructure Protection (Vol. 20, pp. 26–27). safirdep.com. https://doi.org/10.1016/j.ijcip.2017.11.003

Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. In *SN Social Sciences* (Vol. 2, Issue 1). https://doi.org/10.1007/s43545-021-00305-4

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. In *Egyptian Informatics Journal* (Vol. 22, Issue 1, pp. 105–117). https://doi.org/10.1016/j.eij.2020.05.003

Kagermann, H., & Wahlster, W. (2022). Ten Years of Industrie 4.0. *Sci*, *4*(3). https://doi.org/10.3390/sci4030026

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers and Security*, *45*, 58–74. https://doi.org/10.1016/j.cose.2014.05.006

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

Li, Z., Shahidehpour, M., Galvin, R. W., & Li, Y. (2018). Collaborative Cyber-Physical Restoration for Enhancing the Resilience of Power Distribution Systems. *IEEE Power and Energy Society General Meeting*, *2018-Augus*. https://doi.org/10.1109/PESGM.2018.8585955

Liang, G. (2019). Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks. *IEEE Transactions on Smart Grid*, *10*(3), 3162–3173. https://doi.org/10.1109/TSG.2018.2819663

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, *4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. In *Environment Systems and Decisions* (Vol. 33, Issue 4). Springer. https://doi.org/10.1007/s10669-013-9485-y

Lyeonov, S., Strielkowski, W., Koibichuk, V., & Drozd, S. (2024a). Impact of Internet and mobile communication on cyber resilience: A multivariate adaptive regression spline modeling approach. *International Journal of Critical Infrastructure Protection*, *47*(May). https://doi.org/10.1016/j.ijcip.2024.100722

Lyeonov, S., Strielkowski, W., Koibichuk, V., & Drozd, S. (2024b). Impact of Internet and mobile communication on cyber resilience: A multivariate adaptive regression spline modeling approach. *International Journal of Critical Infrastructure Protection*, *47*, 100722. https://doi.org/10.1016/j.ijcip.2024.100722

Matić Bošković, M. M. (2023). Cybercrime Money Laundering Cases and Digital Evidence. *Strani Pravni Život*, *66*(4), 451–167. https://doi.org/10.56461/spz_22406kj

Nguyen, T. A., Koblandin, K., Suleymanova, S., & Volokh, V. (2022). Effects of "digital" country's information security on political stability. In *Journal of Cyber Security and Mobility* (Vol. 11, Issue 1). https://doi.org/10.13052/jcsm2245-1439.1112

Samia, N., Saha, S., & Haque, A. (2024). Predicting and mitigating cyber threats through data mining and machine learning. *Computer Communications*, *228*, 107949. https://doi.org/10.1016/j.comcom.2024.107949

Saniuk, S., Grabowska, S., & Straka, M. (2022). Identification of Social and Economic Expectations: Contextual Reasons for the Transformation Process of Industry 4.0 into the Industry 5.0 Concept. *Sustainability (Switzerland)*, *14*(3), 1391. https://doi.org/10.3390/su14031391

Serafin, M. J., Garc, G. R., Garc, P., Caicedo, M. I., & Correa, J. C. (2019). *Cyberbehavior : A Bibliometric Analysis*. 1–12.

Shaffique, M. R. (2024). Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? *Computer Law and Security Review*, *54*(July). https://doi.org/10.1016/j.clsr.2024.106009

Singh, A., Rejeb, A., Nangru, H., & Pathak, S. (2024). Global research trends on cyberbullying: A bibliometric study. *Computers in Human Behavior Reports*, *16*(October). https://doi.org/10.1016/j.chbr.2024.100499

Tao, F., Qi, Q., Wang, L., & Nee, A. Y. C. (2019). Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison. *Engineering*, *5*(4), 653–661. https://doi.org/10.1016/j.eng.2019.01.014

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., & Sastry, S. (2010). Cyber security analysis of state estimators in electric power systems. *2021 60th IEEE Conference on Decision and Control (CDC)*, 5991–5998. https://doi.org/10.1109/cdc.2010.5717318

Teoh, C. S., & Mahmood, A. K. (2017). National cyber security strategies for digital economy. *Journal of Theoretical and Applied Information Technology*, *95*(23), 6510–6522. https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85038375248&origin=inward

Tsaruk, O., & Korniiets, M. (2020). Hybrid nature of modern threats for cybersecurity and information security. *Smart Cities and Regional Development (SCRD) Journal*, *4*(1), 57–78. https://doi.org/10.25019/scrd.v4i1.63

Valencia-Arias, A., Palacios-Moya, L., Barandiarán-Gamarra, J. M., Valencia, J., Garces Giraldo, L. F., & Gallegos, A. (2024). Analyzing Research Trends in Cybersecurity Involvement of Women: A Bibliometric Approach. In *Lecture Notes in Networks and Systems* (Vol. 1056, pp. 31–42). https://doi.org/10.1007/978-981-97-4892-1_3

van Eck, N. J., & Waltman, L. (2014). Visualizing Bibliometric Networks. In Y. Ding, R. Rousseau, & D. Wolfram (Eds.), *Measuring Scholarly Impact: Methods and Practice* (pp. 285–320). Springer International Publishing. https://doi.org/10.1007/978-3-319-10377-8_13

Yıldız, E., & Simsekler, O. (2023). Corporate Cyber Security In Turkey Investigation of Legal and Corporate Infrastructure : A Meta-Synthesis Study. *Global Journal of Computer Sciences Theory and Research*, *13*(1), 46–58. https://doi.org/10.18844/gjcs.v13i1.8858

UU ITE 2nd Revision retrieved from http://www.bps.go.id on 15th March 2025

Cybersecurity ventures annual report retrieved from https://www.esentire.com/resources/library/2023-official-cybercrime-report on 15th March 2025

Application Programming Interface (API) OpenAlec.org retrieved from https://api.openalex.org/works?page=1&filter=title_and_abstract.search:cyber+resilience+and+security,language:languages/en&sort=relevance_score:desc&per_page=10&apc_sum=false&cited_by_count_sum=false on 26th March 202