International Journal of Instruction, Technology, and Social Sciences
Vol. 5, 39-55, 2026
ISSN: 2716-6546
www.ijitsc.net

Study of research on cyberattack risk mitigation: A bibliometric analysis

TOADER ADRIAN-ȘTEFAN[1]
PhD Student, National University of Science and Technology POLITEHNICA Bucharest, Romania
*adrian.toader0201@stud.faima.upb.ro

GHEORGHE MILITARU[2]
Prof, National University of Science and Technology POLITEHNICA Bucharest, Romania
*gheorghe.militaru@upb.ro

VALENTIN-IONUT-COSMIN DUMITRESCU[3]
PhD Student, National University of Science and Technology POLITEHNICA Bucharest, Romania
*vdumitrescu3007@stud.acs.upb.ro

Abstrat. *Risk management and system security have now become key pillars of organizations' strategic priorities, as a result of the evolution and intensification of cyberattacks. Cyberattacks have moved beyond the stage where they were merely an issue for IT departments, they now have a significant impact on organizational continuity, the security of critical infrastructure, and governance decisions. As a result of this reality, the academic community's interest in reducing cyber risks has intensified, making it one of the most dynamic research areas in cybersecurity. This study provides a bibliometric analysis of the literature on cyber risk reduction, covering 563 Scopus-indexed papers from 2015 to 2025. VOSviewer and the Bibliometrix package in RStudio were used to correlate publication trends, leading authors, contributing countries, and dominant research areas, with a focus on keyword co-occurrence networks, author impact and productivity according to Lotka's Law, most published journals, and thematic clustering. Results show consistent growth in scientific production, with the United States, India, the United Kingdom, and Saudi Arabia leading worldwide production. Author productivity follows Lotka's Law, with a small percentage of researchers concentrating the majority of their contributions in high-impact journals related to risk management and cybersecurity. Several theme clusters that represented the field's evolution from fundamental risk governance to artificial intelligence, machine learning, operational threat detection, and emerging security technologies were identified through keyword co-occurrence analysis. This study provides researchers and practitioners with a clear picture of how cyberattack risk mitigation research has advanced and where future efforts should focus.*
Keywords: cyberattack risk mitigation; bibliometric analysis; risk management; cyber resilience

1. Introduction

Cybersecurity has experienced one of the fastest growths and evolutions in the global economy. In the current context of accelerated digitalization, increasing complexity and diversity of threats, as well as increasingly stringent institutional compliance requirements, mitigating cyber risks has become a priority for organizations across all sectors (Eling & Wirfs, 2019; Agrafiotis et al., 2018). To keep pace with these changes, organizations have been required to adopt various emerging technologies, such as artificial intelligence, machine learning, blockchain, and zero-trust architecture, which have redefined how cyber threats are detected, evaluated, and mitigated (Lallie et al., 2021; Sarker et al., 2021).

Cyber risk can no longer be viewed solely from a technical perspective, it must be integrated into organizational risk management (Cremer et al., 2022). Cyberattacks have a significant impact on operational continuity, data integrity, and the security of critical infrastructure, therefore, mitigating cyber risks serves as a link between cybersecurity, risk management, and the security of information systems (Agrafiotis et al., 2018). Consequently, this reality has necessitated the development of dedicated regulatory frameworks such as the NIST Cybersecurity Framework, the European Union's NIS2 Directive, and the Digital Operational Resilience Act (DORA), which mandates that organizations follow a set of explicit rules for identifying, assessing, and mitigating cyber risks, thereby integrating cybersecurity into the broader realm of risk management (Uchendu et al., 2021).

In order to systematically organize a field of research, bibliometric analysis allows us to observe the conceptual evolution of the specialized literature (Öztürk et al., 2024). Using this tool, we can examine publication patterns, co-citation networks, and the frequency of keyword co-occurrence, which allows us to identify researchers who have made significant contributions, thematic clusters, gaps in the analyzed literature, and future research directions (Donthu et al., 2021).

Upon reviewing the literature, we observe that various bibliometric analyses have been conducted in fields related to cybersecurity. Existing studies present data from fields involving the application of artificial intelligence in cybersecurity, the use of machine learning techniques for intrusion detection, IoT network security, and cyber risk management at the organizational level(O. S. Albahri & A. H. AlAmoodi, 2023; Purnama et al., 2024; Goranin et al., 2024; Cremer et al., 2022). Although these studies provide a valuable framework for the various segments of the field, no study has offered a perspective on cyber risk mitigation as a distinct area of research that serves as the link between cybersecurity and risk management. Therefore, the proposed study has a major impact on researchers and practitioners as it captures the current state of knowledge in this area, contributing a systematic analysis of 563 Scopus-indexed publications from 2015 to 2025.

2. Theoretical background

Cybersecurity is one of the key processes designed to protect information systems, networks, and data against unauthorized access, modification, or destruction (Benaichouba et al., 2024). This industry is required to take all necessary steps to provide the best defense against cyberattacks, which are intentional acts intended to jeopardize the confidentiality, integrity, or availability of digital data (Benaichouba et al., 2024; Yeboah-Ofori & Opoku-Boateng, 2023).

Due to technological advancements, attackers' methods for accessing critical and hard-to-reach data are evolving just as rapidly (Achuthan et al., 2024). Some of the most important

categories of cyberattacks and their vectors are: *ransomware* that works by blocking access to data until a ransom is paid (Fotis, 2024); *malware*, which includes unauthorized viruses, worms, and trojans designed to disrupt a system or collect information from it, *phishing* is the practice of hackers using email links to infect computers and mobile devices with malware in order to steal vital data (Behiry & Aly, 2024); *DDoS* attacks that overwhelm a system's resources with heavy, unauthorized traffic, causing the entire service to go down and making it inaccessible (Hnamte et al., 2024); *man-in-the-middle*, in which a hacker intercepts information on conversations between two people who are not aware of his presence in order to steal or intercept data (Michelena et al., 2024).

The basis of every security posture is risk assessment, which uses multiple variables to measure possible operational or financial losses and assess residual risk, or the threat that persists after all measures are implemented (Bentley et al., 2020; Sánchez-García et al., 2023).

The goal of risk mitigation is to utilize evidence-based strategies to lessen the likelihood or severity of these risks (Woods & Seymour, 2023). Important theoretical frameworks consist of:

- *NIST Framework for Cybersecurity* (National Institute of Standards and Technology, 2024): structured around six key functions: governance, identification, protection, detection, response, and recovery - with an objective of assisting businesses in comprehending, evaluating, prioritizing, and communicating cybersecurity threats;
- *MITRE ATT&CK (Branescu et al., 2024):* provides organizations with an overview of known attack patterns and methods used by attackers, with the aim of enabling them to implement appropriate security measures;
- *Zero Trust Architecture (Lokare et al., 2025):* a strategy to reduce attacks that involves continuously monitoring any entity, regardless of whether it is friendly or hostile.

Detection technologies are one of the main pillars of cybersecurity, as they mark the transition from static defensive mechanisms to active and continuous monitoring of network traffic. Modern systems use artificial intelligence, machine learning, and deep learning to continuously analyze network behavior and identify threats early on with far greater precision and efficiency than traditional methods (Salem et al., 2024).

Cyber resilience provides organizations with the ability to respond to attacks, continue operations, and recover from incidents (Kanthimathinathan et al., 2023). Several major attacks, such as the one at Colonial Pieline (2021), where $4.4 million was lost (Mittal, 2024) , the Kaseya attack (2021), where over 1,000 businesses were affected and had to shut down, suffering both financial and reputational losses (Ghanbari et al., 2024), the MOVEit data breach (2023), in which confidential data was stolen from over 1,000 institutions (Dosumu, 2025), have underscored the importance of adopting a preventive security approach to organizational resilience (Safitra et al., 2023). Thus, the adoption of cyber resilience marks the transition from a defense built solely to prevent incidents to an organization’s ability to restore operational functionality as quickly as possible (Verma et al., 2025).

Modern cyberattacks can no longer be mitigated by a single technology or strategy. By understanding the types of attacks and their vectors, integrating AI-based detection systems, and adopting a cybersecurity approach that enables risk management and organizational recovery following incidents, institutions are building a framework capable of significantly reducing cyberattacks (Kristian et al., 2024).

3. Research methodology

The quantitative bibliometric approach employed in this study is one of the most rigorous methods for mapping the intellectual and collaborative structure of a research topic. Bibliometrics provides an unbiased and comprehensive perspective that enables the quantification of scientific production, the identification of prominent authors, and the depiction of emergent topic clusters. The choice of this method demonstrates a commitment to offering an evidence-based study that can record the advancement of research on cyberattack risk reduction during the preceding ten years.

Scopus was chosen as the primary data source for bibliometric studies of engineering and computer science research because of its rich structured metadata, which includes author affiliations, citation counts, author keyword and index keyword fields, and subject area classifications, as well as its broad coverage of peer-reviewed science and technology literature. The following three-pillar structured query was used to do the search:

TITLE-ABS-KEY (("cyberattack" OR "cyber attack" OR "cyber-attack" OR "cybersecurity" OR "cyber security" OR "cyber threat" OR "cyber threats") AND ("risk management" OR "risk mitigation" OR "risk assessment" OR "risk reduction" OR "threat mitigation" OR "attack mitigation" OR "mitigation strategy" OR "mitigation strategies") AND ("cyber safety" OR "cyber resilience" OR "incident response" OR "cyber defense" OR "cyber defence" OR "intrusion detection" OR "intrusion prevention" OR "threat detection" OR "anomaly detection"))

The query has three thematic pillars. By examining cyberattack incidents, cybersecurity issues, and cyber threat concepts as they emerge in the literature, the first pillar establishes the study's scope and captures research that confronts digital threats and their effects at both organizational and systemic levels. The second addresses risk management and mitigation, ranging from specific risk reduction and response strategies to planning and governance ideas. The third focuses on the technological aspects of risk management implementation, specifically on detection and response capabilities.

The temporal scope was limited to the years 2015–2025, which were characterized by increased regulatory activity and research focus on cyber risk due to the implementation of significant cybersecurity and data protection frameworks as well as the wider digitalization of organizational procedures that increased the attack surface and the policy response. Only English-language journal papers and review articles were accepted as document types.

The bibliometric analysis was conducted using three complementary software tools. VOSviewer (version 1.6.20) was used to construct and visualize the co-occurrence network of keywords. RStudio (version 4.5.3), together with the Bibliometrix package and its web interface Biblioshiny, were used to analyze bibliometric indicators of scientific productivity—the distribution of publications by subject area, the annual evolution of scientific output, the geographical distribution of research, the journals with the highest number of articles and their associated H-index, the most prolific authors, the authors' productivity rate according to Lotka's Law, as well as the authors' local impact. Microsoft Excel was used to organize and verify the data exported from Scopus prior to processing, as well as to supplement the RStudio software in preparing and structuring the datasets.

These methodological limitations, reliance on a single database and the quantitative nature of bibliometric analysis, do not undermine the validity of the results. Scopus offers consistent, repeatable metadata, and the analytical approach makes it possible to find patterns throughout a substantial corpus that would be hidden in qualitative research, supporting a methodical analysis of the evolution of cyberattack risk mitigation research worldwide.

By using bibliometric network analysis to examine publications indexed in the Scopus database, the primary goal of this study is to map the intellectual and thematic structure of research on cyberattack risk mitigation published between 2015 and 2025. The following questions are the focus of the bibliometric analysis that was done:

1. *What is the distribution of studies across subject areas in the cyberattack risk mitigation literature?*
2. *How does the distribution of publications on cyberattack risk mitigation change over the years?*
3. *What is the geographic distribution of scientific production in this field, and which countries contribute most to the literature?*
4. *Which journals concentrate the highest volume of publications on cyberattack risk mitigation?*
5. *Who are the most prolific authors contributing to research on cyberattack risk mitigation?*
6. *What are the dominant thematic clusters and semantic relationships emerging from the co-occurrence network of author keywords?*

4. Results and further discussions

Mitigating the risk of cyberattacks is one of the main goals in the field of cybersecurity. In order to analyze research trends, VOSviewer (Van Eck & Waltman, 2017) and Bibliometrix (Aria & Cuccurullo, 2017) were used to process bibliographic data that was exported from the Scopus database in CSV and BibTeX formats. Data collection used relevant phrases such "cyberattack," "cyber threat," "risk mitigation," "risk assessment," and "anomaly detection" in combination with Boolean operators (AND, OR) to capture conceptual variants. Only English-language journal and review articles published between 2015 and 2025 were included.

185,404 results were returned by the search for "cybersecurity," demonstrating the topic's interdisciplinary nature (Figure 1). Most articles come from the domains of computer science (131,492), engineering (81,537), social sciences (33,088), mathematics (31,807), decision sciences (24,975), business, management and accounting (16,769). Additional contributions from the fields of energy, physics, astronomy, medicine, economics, econometrics, finance, materials science, and environmental science attest to the wide relevance and applicability of cybersecurity in scientific literature.

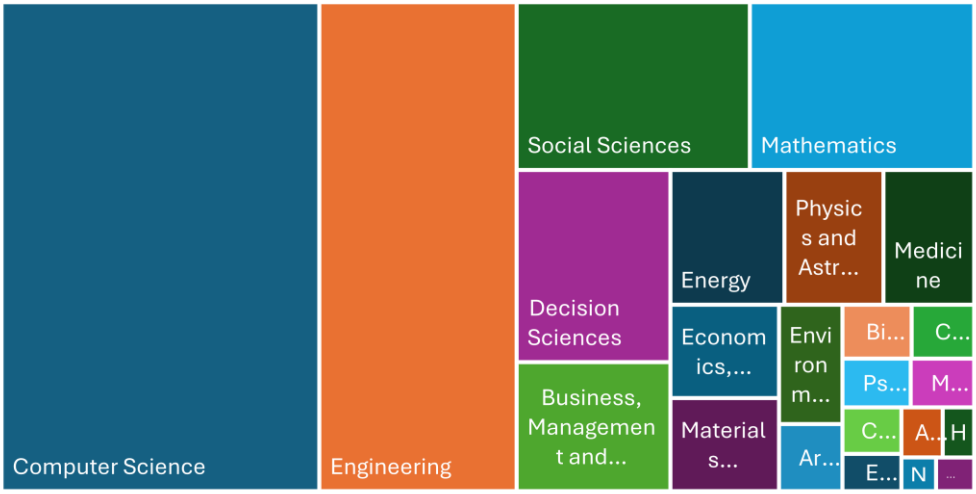

Figure 1. Thematic results for "cybersecurity"

International Journal of Instruction, Technology, and Social Sciences
Vol. 5, 39-55, 2026
ISSN: 2716-6546
www.ijitsc.net

563 documents were found for the analysis after the filters were applied. These documents were mainly from technical and applied fields, with a notable concentration in computer science (390), engineering (290), mathematics (77), social sciences (76), materials science (62), and business, management, and accounting (50). The database reflects the wide range of organizational, technological, and social perspectives applied to cyberattack risk mitigation research. It also includes complementary disciplines such as physics and astronomy, decision sciences, chemistry, biochemistry, genetics and molecular biology, energy, environmental science, medicine, and chemical engineering, among many others. The key characteristics of the dataset are presented in Table 1.

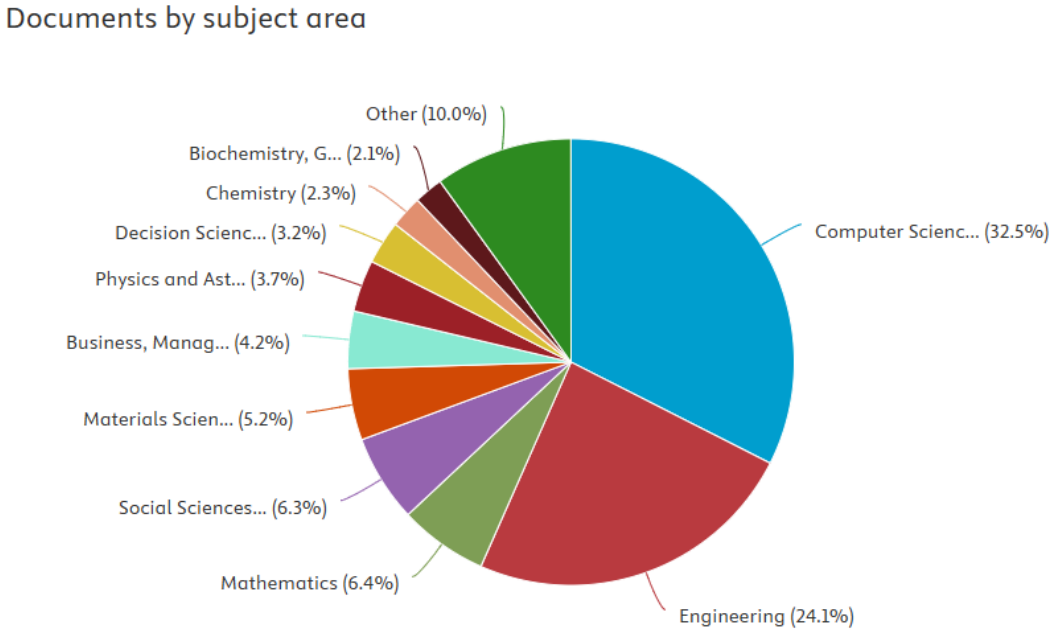

Figure 2. Distribution of publications across subject areas

Timespan	2015:2025
Sources	307
Documents	563
Annual Growth Rate	51.69%
Authors	2099
Authors of single-authored docs	60
International Co-Authorship	34.64%
Co-Authors per Doc	3.92
Author's Keywords (DE)	1992
References	29755

Document Average Age	2.58
Average citations per doc	19.67

Table 1. Dataset key characteristics

A growing trend in interest in the topic under study can be seen in the distribution of scientific articles by year (Figure 3). There were no notable variations in the quantity of publications till 2022. There has been a sharp rise in scientific production since 2023, which is indicative of a quick expansion of research and heightened interest in the subject. This increasing tendency indicates that the sector is going through a period of significant change, propelled by advancements in technology, global partnerships, and rising needs for applied development. The peak between 2023 and 2025 shows a period of increased academic activity during which the number of articles doubles year over year. Due to increased risks and more rigorous international regulations, the academic community is becoming more interested in cybersecurity risk mitigation, as evidenced by this trend.

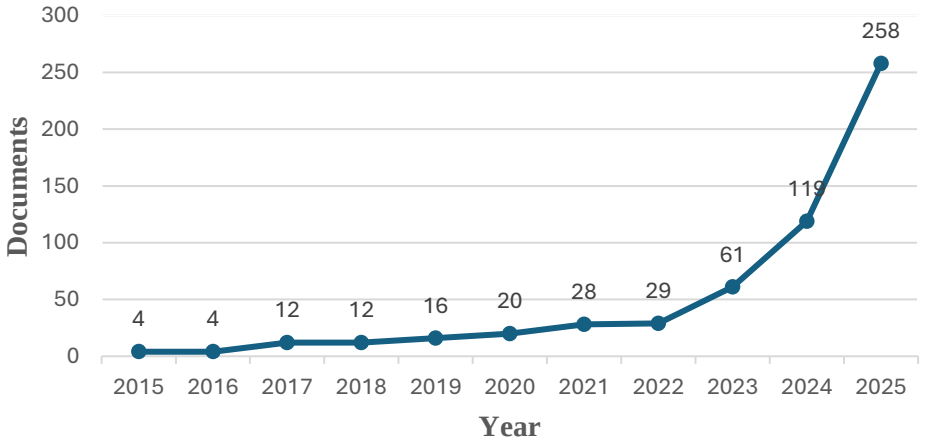

Figure 3. Distribution of the documents by years

The geographic distribution of scientific publications in the field of cybersecurity spans 90 countries, a finding that underscores the importance of this topic as well as the global interest in it (Figure 4). The countries with the most publications are those with developed digital infrastructures, such as the United States (100 papers), India (80 papers), the UK (60 papers), and Saudi Arabia (59 papers). However, the presence of countries such as Iraq (19 papers), Pakistan (19 papers), or Ukraine (14 papers) suggests that the growing interest in reducing cyber risk extends beyond the traditional boundaries of research. The diversity and increased global volume of these contributions reflect the scientific community's growing concern for identifying different solutions to reduce cyberattacks, implementing risk management strategies, and adopting appropriate technologies and methods to protect digital infrastructure.

International Journal of Instruction, Technology, and Social Sciences
Vol. 5, 39-55, 2026
ISSN: 2716-6546
www.ijitsc.net

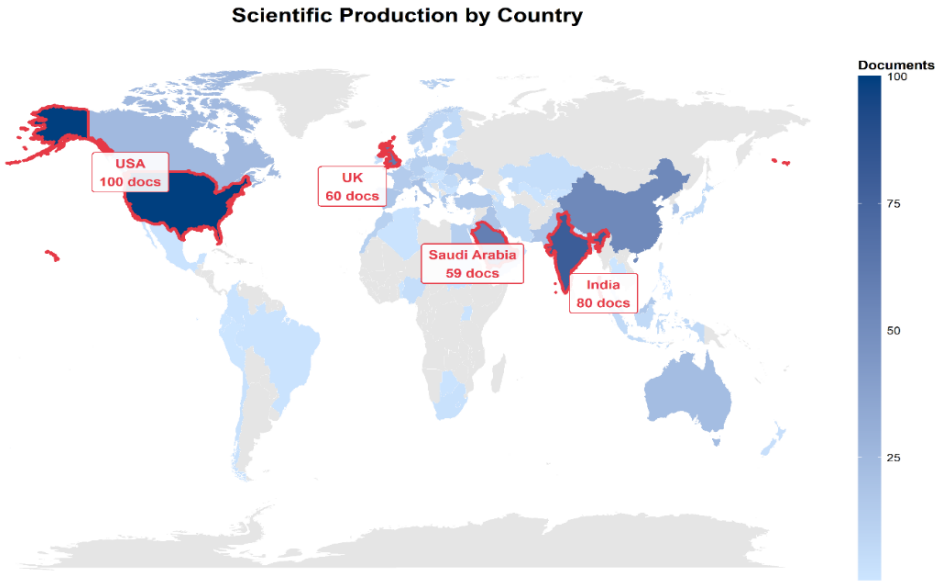

Figure 4. Country scientific production

To identify the most widely published journals, the study was restricted to journals with at least four articles on the subject and they were categorized by quartile based on the SCImago Journal Rank (SJR) classification. After analyzing the publication sources of the 563 articles, only 200 met this criterion (Table 2). It can be observed that a large proportion of them were published in high-impact journals known for their scientific rigor and international recognition, such as IEEE (with 33 articles), followed by Computer and Security and Sensors each with 22 articles. Excellent academic potential is demonstrated by strong bibliometric indicators like the H-index (Figure 5) and the categorization of sources in the top quartiles (Q1–Q2), which confirm the growing interest of the global academic community in the topic.

Sources	Articles	Quartile
IEEE Access	38	Q1
Computers And Security	22	Q1
Sensors	22	Q1
Electronics (Switzerland)	11	Q2
Applied Sciences (Switzerland)	10	Q1
International Journal Of Information Security	9	Q1
Scientific Reports	9	Q1
International Journal Of Critical Infrastructure Protection	8	Q1
Energies	6	Q1
Alexandria Engineering Journal	5	Q1
Computer Networks	5	Q1
Computers And Electrical Engineering	5	Q1
Computers, Materials And Continua	5	Q2

IEE Transactions On Information Forensics And Security	5	Q1
International Journal Of Safety And Security Engineering	5	Q3
Applied Soft Computing	4	Q1
Computers	4	Q1
Ieee Transactions On Smart Grid	4	Q1
Information (Switzerland)	4	Q2
International Journal Of Advanced Computer Science And Applications	4	Q3
Journal Of Cybersecurity And Information Management	4	Q4
Journal Of Network And Computer Applications	4	Q1
Journal Of Supercomputing	4	Q2
Peerj Computer Science	4	Q2
Risk Analysis	4	Q1

Table 2. Top-rated journals in the article

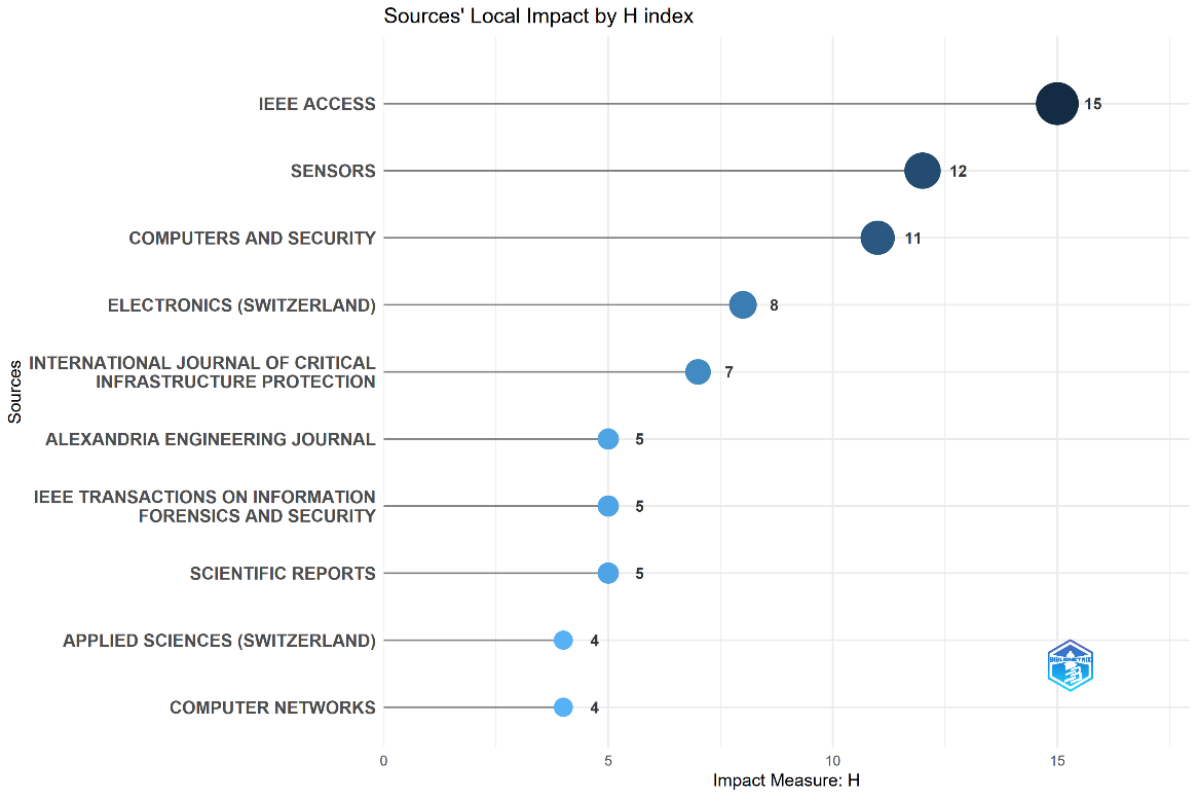

Figure 5. Top-rated journals' H-index

International Journal of Instruction, Technology, and Social Sciences
Vol. 5, 39-55, 2026
ISSN: 2716-6546
www.ijitsc.net

Authors that submitted at least three articles were chosen in order to provide a better examination of the link between the authors. 12 of the 2099 authors satisfy the necessary criteria (Table 3).

Authors	Documents	Strength
TAM K	5	5
CHOO K.K.R	3	3
DUPONT B	3	3
HOPCRAFT R	3	3
JANICKE H	3	3
KATSIKAS S	3	3
MOUSTAFA N	3	3
SANTOS-OLMO A	3	3
TURNBULL B	3	3
HONG J	3	2
SARIGIANNIDIS P	3	2
SHABTAI A	3	2

Table 3. Article's most prolific authors

To learn about a scientific field's intellectual landscape, it is very important to identify the most prolific authors. Tam K. stands out as the most prolific author with 5 publications (Table 3). The other authors each have three publications and significant number of citations, highlighting the fact that there is a well-defined core of active researchers in the field of cyber risk mitigation.

To understand how productivity is distributed among authors in this field, we used Lotka's law, which is widely used in bibliometric analyses. According to this law, generally about 60% of researchers publish only one paper in a given field (Lotka, 1926). In our case, this proportion reaches 96.2% (Figure 6), well above the average, which means that most authors have written a single article on this topic, while the continuation of scientific production is maintained by a small number of researchers. Additionally, the bibliometrix tool provides the impact rate of the most productive authors on this subject (Table 4). Table 4 displays the authors' total number of citations (TC), their number of publications (NP), and the date of their first publication (PY). These statistics show that, despite only starting to publish in 2019, CHOO K.K.R. has the most significant academic impact (407 citations) (Table 4) on this subject.

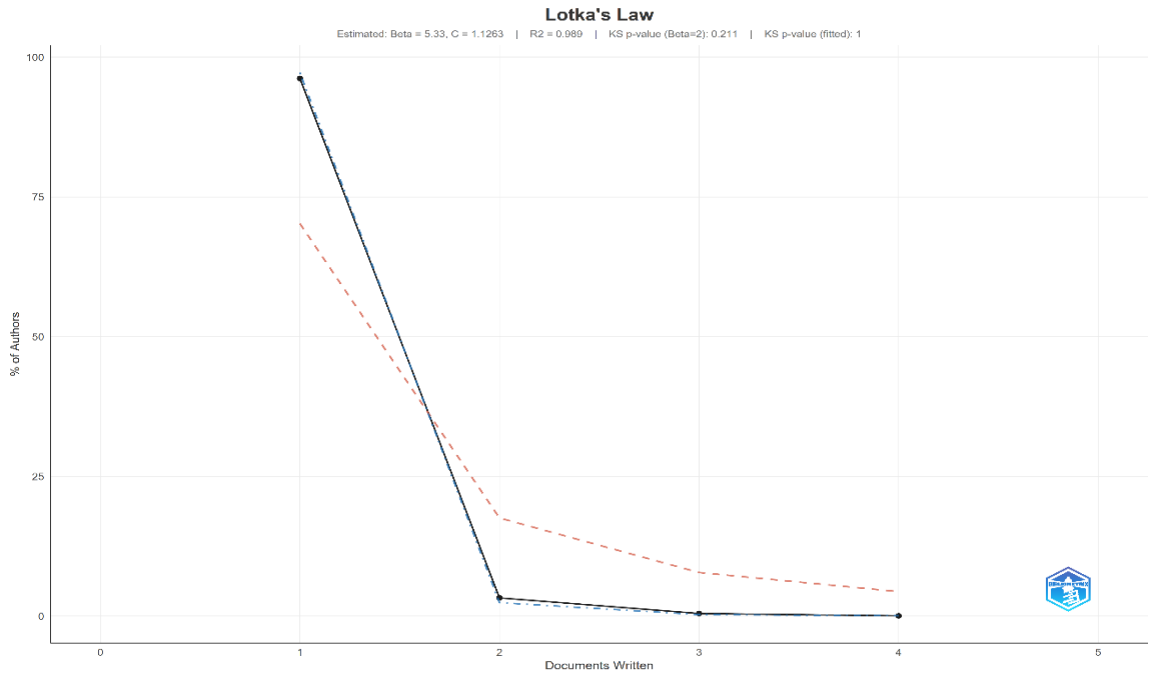

Figure 6. Author rate and Lotka's Law

Authors	h_index	g_index	m_index	TC	NP	PY_start
CHOO K.K.R	3	3	0.375	407	3	2019
DUPONT B	3	3	0.375	127	3	2019
HONG J	2	3	0.25	106	3	2019
HOPCRAFT R	3	3	0.75	43	3	2023
JANICKE H	3	3	0.3	86	3	2017
KATSIKAS S	3	3	0.3	157	3	2017
MOUSTAFA N	3	3	0.428	32	3	2020
SANTOS-OLMO A	3	3	0.75	48	3	2023
SARIGIANNIDIS P	2	3	0.333	46	3	2021
SHABTAI A	2	3	0.4	30	3	2022
TAM K	5	5	1	89	5	2022
TURNBULL B	3	3	0.428	32	3	2020

Tabel 4. Author impact analysis

An analysis of the co-occurrence of the authors' keywords was conducted using the VOSviewer application (version 1.6.20) in order to determine the thematic structure of the literature under study as well as the semantic relationships between the dominant concepts. A total of 1,992 unique terms were identified, but by setting a minimum threshold of 5 co-occurrences, only 62 of these met the criterion. Before generating the map, we used a thesaurus file to standardize spelling variations of the same word, for example, "cyber security," "cyber-security," and "cybersecurity" were treated as a single term.

Created using VOSViewer, the overlay visualization shows the average year of publication for articles containing the terms, with blue representing words that have been in

International Journal of Instruction, Technology, and Social Sciences
Vol. 5, 39-55, 2026
ISSN: 2716-6546
www.ijitsc.net

the literature for a longer time and yellow representing more recent terms (Figure 7). Terms such as cybersecurity, risk management, intrusion detection, and anomaly detection are shaded in blue and blue-green, highlighting that they have significant and consistent importance throughout the analyzed period, underscoring the field's core concerns regarding security, risk management, and threat detection. In contrast, terms such as zero-trust architecture, generative AI, digital twin, cyber threat mitigation, and real-time threat detection appear in shades of yellow, indicating an extension of these concerns toward the integration of advanced technologies and artificial intelligence into cybersecurity systems and supporting the scientific community's new vision.

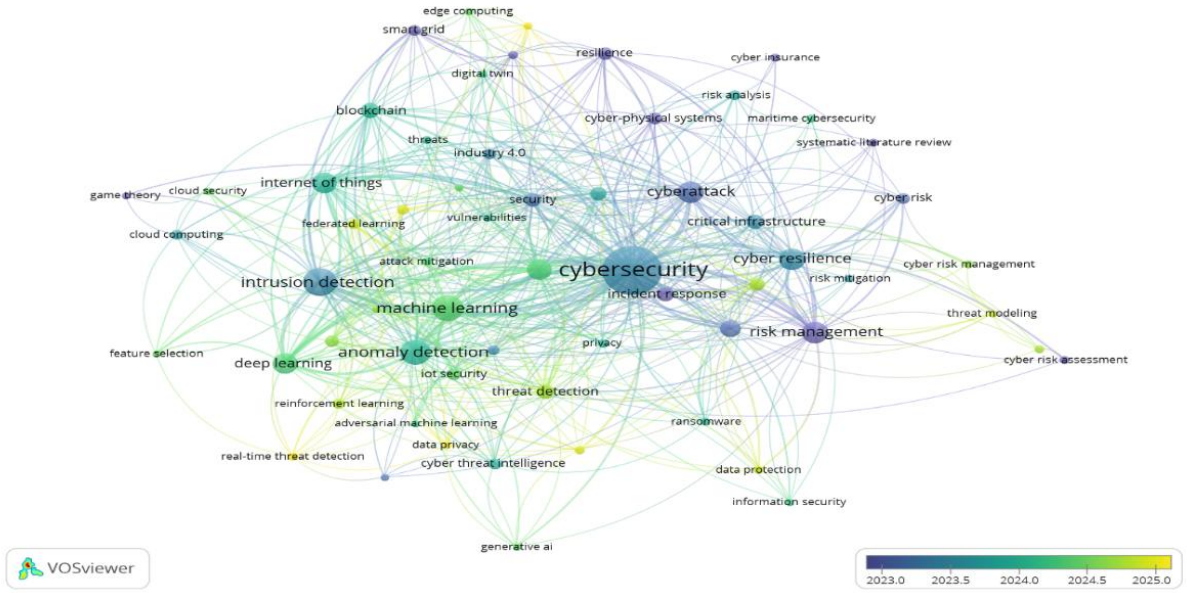

Figure 7. Overlay visualization of the keyword co-occurrence network

Based on an analysis of the co-occurrence network of keywords, a conceptual framework of the literature on cyber risk mitigation is identified (Figure 8). The term "cybersecurity" serves as the central hub, connecting to all other terms—such as risk management, cyber resilience, machine learning, intrusion detection, and anomaly detection—thereby reinforcing its role as the unifying concept of the field Four thematic clusters emerge around this central node: cyber risk management and governance, detection and mitigation based on machine learning, threat detection and cyber intelligence and emerging technologies and security architectures.

The red cluster unites studies on risk management and governance. With "cybersecurity" as its central term, appearing 228 times, and "cyber resilience" (46) and "risk management" (43) in close proximity, the cluster highlights how institutions assess, manage, and mitigate cyber risks—key elements for organizational security strategies. "Cyberattack" (45) frequently appears alongside "critical infrastructure" (20), and the presence of terms such as "ransomware," " mitre att&ck" and "threat modeling" reinforces the fact that interest extends beyond the theoretical realm and focuses on concrete attack vectors.

The green cluster brings together research focused on automated threat detection, with intrusion detection (74), machine learning (62), and deep learning (42) as the main keywords.

International Journal of Instruction, Technology, and Social Sciences
Vol. 5, 39-55, 2026
ISSN: 2716-6546
www.ijitsc.net

Studies in this cluster aim to develop and test algorithms capable of detecting attacks in real time, with a direct focus on securing networks and Internet of Things (IoT) infrastructures.

The blue cluster focuses on operational threat detection and cyber intelligence. The most frequently occurring terms—anomaly detection (60), threat detection (21), and incident response (19)—indicate that the goal of this cluster is to apply artificial intelligence to identify and mitigate threats before they cause any damage. An interesting aspect is the presence of the concepts of adversarial machine learning and generative AI, which indicates that researchers are seeking to discover what happens when an attacker is aware of the detection system and attempts to deceive it.

The yellow cluster includes papers focused on the application of emerging technologies in cybersecurity. Studies in this cluster explore the incorporation of artificial intelligence (41), blockchain (22), and industry 4.0 (12) into security architecture, with the aim of minimizing the attack surface, increasing supply chain security, and developing systems resilient to cyber threats that are constantly evolving. The concepts of zero-trust architecture, digital twins, and edge computing complement the clear focus on proactive security and design-integrated security.

This network highlights the variety and complexity of the thematic connections in the literature on cyber risk mitigation, as well as the maturity of the field and emerging areas of study.

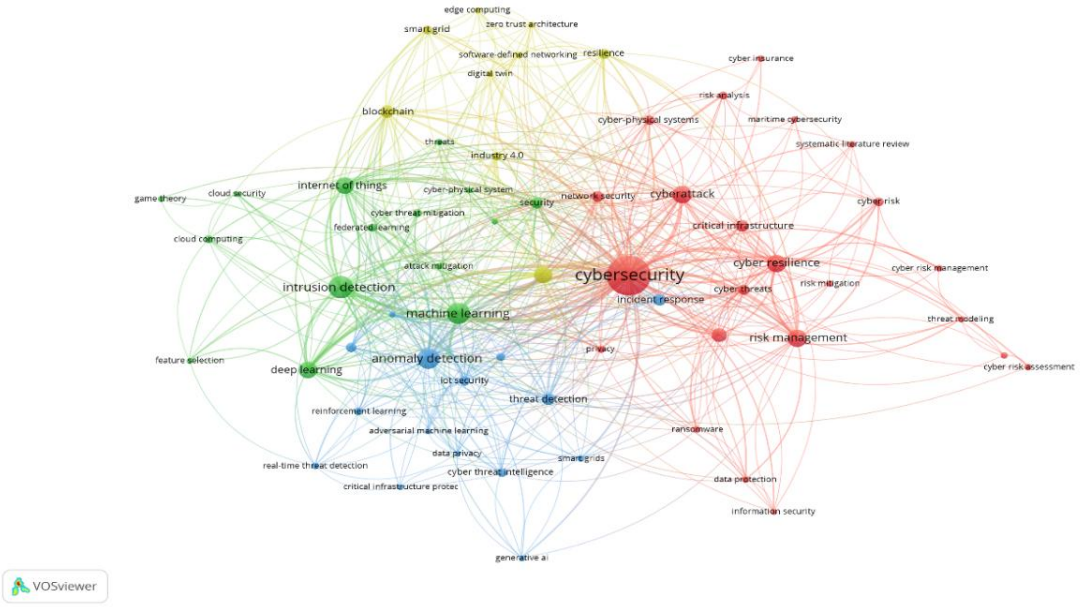

Figure 8. Analysis of the co-occurrence network of keywords

5. Conclusions

The study analyzed 563 publications indexed in Scopus over the past ten years (2015–2025) with the aim of providing new insights into the field of cyber risk mitigation. To conduct this study, VOSviewer was used to analyze keyword co-occurrence networks, along with Bibliometrix and RStudio for productivity indicators, revealing the current state of existing and emerging research directions.

Throughout the review period, scientific publications has continuously increased, with a focus on the areas of cyber risk governance and the integration of artificial intelligence into

the security and protection of critical infrastructure. This growth is closely linked to the evolution of cyberattacks globally, as well as the emergence of various regulations that have imposed a set of concrete cyber risk management rules on organizations, such as the NIST Cybersecurity Framework, the NIS2 Directive, and DORA.

Although most of the research is conducted by countries such as the United States, India, the United Kingdom, and Saudi Arabia, reflecting their advanced technological capabilities, the involvement of countries such as Iraq, Pakistan, and Ukraine suggests that even countries with developing digital infrastructures are aware of the urgency of this issue.

The superior quality of the research and the expanding interest of the global academic community in this field are highlighted by the publications' indexing in high-impact international journals like IEEE Access and Computers and Security, which are categorized in the Q1–Q2 categories.

According to the authors' productivity analysis, the dynamics of knowledge production in this field are highlighted. Tam K. stands out as the most prolific contributor, with five publications, while CHOO K.K.R. demonstrates the greatest academic impact, with 407 citations. These results are in line with Lotka's Law, which this study confirms, highlighting the idea that a small core of researchers drives scientific production and forms the intellectual foundation of research on reducing the danger of cyberattacks.

The most important discovery is the identification of four theme clusters that represent the field's current situation as well as its evolution. The first cluster, which focuses on cyber risk governance and resilience, demonstrates how companies now incorporate cybersecurity into formal risk management structures rather than approaching it separately; this reflects a change in perspective and the way organizations are building their security strategies. The second cluster, dominated by machine learning and deep learning applied to intrusion detection, highlights the advanced stage of development of automated threat detection; in other words, the scientific community is no longer debating the usefulness of AI in cybersecurity but rather the methods by which it can be optimized. A concern for detecting and controlling attacks in real time is reflected in the third cluster, which focuses on operational threat detection through anomaly detection and incident response. There is a growing emphasis on the resilience of detection systems against increasingly complex and sophisticated attacks and techniques, as well as models based on generative artificial intelligence. The final cluster, which is also the most recent, unites research on blockchain, zero trust, and digital twins, indicating a change in viewpoint from reactive security, which reacts to attacks after they happen, to proactive security, which is incorporated into system architecture before threats occur. Organizations that disregard this trend expose themselves to the danger of using traditional security solutions given the current state of threats.

There are a small number bibliometric studies that concentrate on cyber risk reduction as a separate subject in the literature. The present research fills a major vacuum and provides a useful resource for academics who need a clear and current perspective on a rapidly evolving topic as well as for researchers thinking about future studies.

The study also has several limitations, such as the 2015–2025 time range, which may eliminate relevant articles in this subject, and the exclusive use of the Scopus database, which may exclude important contributions from Web of Science or IEEE Xplore. Considerable study published in other languages or in formats like conference proceedings, books, or technical reports was excluded because the study was limited to peer-reviewed articles written in English. Additionally, because bibliometric approaches are quantitative in nature, they are unable to evaluate the incorporated research' empirical quality or theoretical complexity.

Future studies should examine the relationship between risk management frameworks and technical security solutions. At the same time, it is crucial to verify Zero Trust and Digital Twin architectures' functionality in real-world organizational settings.

Author contributions:

- Conceptualization: A.S.T.
- Methodology: A.S.T.
- Investigation: A.S.T.
- Writing original draft: A.S.T
- Writing review and editing: G.M and V.I.C.D.
- Supervision: G.M and V.I.C.D.

Conflict of interest: The Author's declare no Conflict of interest. The funders had no role in the design of the study, in the collection, analyses, or interpretation of data in the writing of the manuscript or in the decision to publish the results.

References

[1] Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions. Frontiers in Big Data, 7, 1497535. https://doi.org/10.3389/fdata.2024.1497535

[2] Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy006

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

[4] Behiry, M. H., & Aly, M. (2024). Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. Journal of Big Data, 11(1), 16. https://doi.org/10.1186/s40537-023-00870-w

[5] Benaichouba, R., Brahmi, M., & Adala, L. (2024). ECONOMIC OF CYBER-SECURITY AND SOCIETY DATABASES: PROTECTING THE DIGITAL ECOSYSTEM FROM CYBER-ATTACKS. International Journal of Professional Business Review, 9(7), e04803. https://doi.org/10.26668/businessreview/2024.v9i7.4803

[6] Bentley, M., Stephenson, A., Toscas, P., & Zhu, Z. (2020). A Multivariate Model to Quantify and Mitigate Cybersecurity Risk. Risks, 8(2), 61. https://doi.org/10.3390/risks8020061

[7] Branescu, I., Grigorescu, O., & Dascalu, M. (2024). Automated Mapping of Common Vulnerabilities and Exposures to MITRE ATT&CK Tactics. Information, 15(4), 214. https://doi.org/10.3390/info15040214

[8] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

[9] 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, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

[10] Dosumu, R. (2025). MOVEit Data Breach: A Case Study in Zero-Day Exploits and Organizational Cybersecurity Preparedness. https://doi.org/10.13140/RG.2.2.17029.26081

[11] Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

[12] Fotis, F. (2024). Cyberattacks: Economic Impacts and Risk Management Strategies. Procedia Computer Science, 251, 672–677. https://doi.org/10.1016/j.procs.2024.11.167

[13] Ghanbari, H., Koskinen, K., & Wei, Y. (2024). From SolarWinds to Kaseya: The rise of supply chain attacks in a digital world. Journal of Information Technology Teaching Cases, 20438869241299823. https://doi.org/10.1177/20438869241299823

[14] Goranin, N., Hora, S. K., & Čenys, H. A. (2024). A Bibliometric Review of Intrusion Detection Research in IoT: Evolution, Collaboration, and Emerging Trends. Electronics, 13(16), 3210. https://doi.org/10.3390/electronics13163210

[15] Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., & Sugali, M. N. (2024). DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 138, 103661. https://doi.org/10.1016/j.cose.2023.103661

[16] Kanthimathinathan, A., Saravanan, S., & Anbalagan, P. (2023). A Novel Cyber Resilience Framework – Strategies and Best Practices for Today's Organizations. International Journal on Recent and Innovation Trends in Computing and Communication, 11(8s), 86–96. https://doi.org/10.17762/ijritcc.v11i8s.7178

[17] Kristian, A., Az-Zahra, A. R., Hidayat, F., Yadi Fauzi, A., & Kallas, E. (2024). Enhancing Cybersecurity Risk Management Strategies in Financial Institutions: A Comprehensive Analysis of Threats and Mitigation Approaches. Journal of Computer Science and Technology Application, 1(2), 96–103. https://doi.org/10.33050/corisinta.v1i2.31

[18] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

[19] Lokare, A., Bankar, S., & Mhaske, P. (2025). Integrating Cybersecurity Frameworks into IT Security: A Comprehensive Analysis of Threat Mitigation Strategies and Adaptive Technologies (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2502.00651

[20] Lotka, A. J. (1926). The frequency distribution of scientific productivity. Journal of the Washington Academy of Sciences, 16(12), 317–323.

[21] Michelena, Á., Aveleira-Mata, J., Jove, E., Bayón-Gutiérrez, M., Novais, P., Romero, O. F., Calvo-Rolle, J. L., & Aláiz-Moretón, H. (2024). A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport. Expert Systems, 41(2), e13263. https://doi.org/10.1111/exsy.13263

[22] Mittal, M. (2024). Colonial Pipeline Cyberattack Drives Urgent Reforms in Cybersecurity and Critical Infrastructure Resilience. International Journal of Oil, Gas and Coal Engineering, 12(5), 106–119. https://doi.org/10.11648/j.ogce.20241205.11

[23] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

[24] O. S. Albahri & A. H. AlAmoodi. (2023). Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. Mesopotamian Journal of CyberSecurity, 2023, 158–169. https://doi.org/10.58496/MJCSC/2023/018

[25] Öztürk, O., Kocaman, R., & Kanbach, D. K. (2024). How to design bibliometric research: An overview and a framework proposal. Review of Managerial Science, 18(11), 3333–3361. https://doi.org/10.1007/s11846-024-00738-0

[26] Purnama, Y., Asdlori, A., Ciptaningsih, E. M. S. S., Kraugusteeliana, K., Triayudi, A., & Rahim, R. (2024). Machine Learning for Cybersecurity: A Bibliometric Analysis from 2019 to 2023. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15(4), 243–258. https://doi.org/10.58346/JOWUA.2024.I4.016

[27] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.3390/su151813369

[28] Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. Journal of Big Data, 11(1), 105. https://doi.org/10.1186/s40537-024-00957-y

[29] Sánchez-García, I. D., Feliu Gilabert, T. S., & Calvo-Manzano, J. A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. Computers & Security, 128, 103170. https://doi.org/10.1016/j.cose.2023.103170

[30] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science, 2(3), 173. https://doi.org/10.1007/s42979-021-00557-0

[31] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

[32] Van Eck, N. J., & Waltman, L. (2017). Citation-based clustering of publications using CitNetExplorer and VOSviewer. Scientometrics, 111(2), 1053–1070. https://doi.org/10.1007/s11192-017-2300-7

[33] Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Toward a Unified Understanding of Cyber Resilience: Concepts, Strategies, and Future Directions. IEEE Access, 13, 49945–49965. https://doi.org/10.1109/ACCESS.2025.3551887

[34] Woods, D. W., & Seymour, S. (2023). Evidence-based cybersecurity policy? A meta-review of security control effectiveness. Journal of Cyber Policy, 8(3), 365–383. https://doi.org/10.1080/23738871.2024.2335461

[35] Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. Continuity & Resilience Review, 5(1), 53–78. https://doi.org/10.1108/CRR-09-2022-0017