Issues in Information Systems
Volume 24, Issue 3, pp. 43-57, 2023

DOI: https://doi.org/10.48009/3_iis_2023_105

Ten years of cybersecurity governance, risk and compliance: a bibliometric examination of research themes, trends, and influencers

Rahul Dwivedi, *Texas A&M University-Central Texas, rahul.dwivedi@tamuct.edu*

Abstract

Cybersecurity is an area of predominant research both for academicians and practitioners. With organizations scrambling to keep up with growing cybersecurity concerns, tremendous growth is observed in the number of articles published in this area. The purpose of this research is to examine the conceptual foundations of cybersecurity governance, risk, and compliance based on a detailed analysis of research articles published within the last 10 years (2013 – 2023). Using a combination of bibliometrics and text analysis techniques, this study aims to (a): identify the research themes, and their relationship, (b): the evolution of research themes over time, and (c): identify the most influential authors, articles, journals, institutions, and countries. As per the results, twelve important research themes were identified, with recent studies focusing on cybersecurity research in relation to artificial intelligence, blockchain, IoT, autonomous vehicles, and supply chains. Based on the corpus, RLUK – a consortium of research libraries in the United Kingdom is the institution and the United States of America is the nation, with the most author affiliations. IEEE Access is the top journal in terms of the number of articles and Computers & Security is the most cited journal.

Keywords: cybersecurity governance, cybersecurity risk, cybersecurity compliance, research themes, co-word analysis, performance analysis.

Introduction

Organizations are facing growing concerns about securing their networking and computer infrastructure against cybersecurity attacks. Numerous industry reports emphasize the importance of cybersecurity within business organizations in terms of expenditure toward protecting the firm's infrastructure and losses due to cybersecurity breaches. In one such report from the International Business Machine (IBM) and the Poneman Institute, the average total cost of a data breach within the United States is 4.5 million USD (https://www.ibm.com/downloads/cas/3R8N1DZJ). Another report found ransomware to be a leading cause of invading organizational networks for financial or personal gain by an external agent (https://www.verizon.com/business/resources/T1d3/reports/dbir/2022-data-breach-investigations-report-dbir.pdf). Cybersecurity is not only a matter of grave concern for business organizations, but governments across the world also have official publications regarding their policies on national cybersecurity and the protection of critical cyber infrastructures against cyber warfare (Hathaway & Klimburg, 2012).

Cybersecurity is defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets." (von Solms & van Niekerk, 2013). This all-inclusive definition of cybersecurity from the International Telecommunications

Union includes references to security policies, guidelines, risk management approaches, and best practices. Hence, this definition is used within the context of this study, which focuses on analyzing recent academic articles published in the field of cybersecurity in general, and cybersecurity governance, risk, and compliance, to be more specific. These subfields (or keywords) of cybersecurity are chosen with a view to being relevant to the theme of the Annual Conference of the International Association for Computer Information Systems for the year 2023.

The research carried out in this study can be considered as one undertaken to understand the intellectual structure of cybersecurity governance, compliance, and risk as addressed within the academic literature. Studying the intellectual structure of different disciplines is an active area of academic research. Some notable examples include entrepreneurship (Ferreira et al., 2019), supply chain management (Charvet et al., 2008), operations management (Pilkington & Meredith, 2009), and health information systems research in IS (Chen et al., 2019). In line with this tradition, this research seeks to explore the scholarly structure and evolution of cybersecurity research with an emphasis on governance, risk, and compliance over a period of ten years (2013 – 2023). This study aims to answer the following research questions:

1) What are the broad underlying research themes for cybersecurity research emphasizing governance, compliance, and risk?

2) Is there a change in these themes over a period? In other words, is there a gradual evolution of research themes over the years?

3) Who are the influential (most cited and most productive) authors, institutions, articles, journals, and countries emphasizing research in this domain?

Articles publishing cybersecurity governance, compliance, and risk research over a ten-year period (2013-2022) from Clarivate's Web of Science's core collection (https://clarivate.com/products/scientific-and-academic-research/research-discovery-and-workflow-solutions/webofscience-platform/) comprised the corpus of research analyzed in this study. The techniques of citation analysis, bibliographic coupling, and co-word analysis are used to address the research questions.

The goal of this research is to elucidate the extant research on cybersecurity governance, risk, and compliance, with the aim of investigating the current state of academic research and identifying the opportunities for extending the boundaries of knowledge in this area. Given the attention lavished on cybersecurity within organizations, this endeavor can provide a foundation for future research and improved practices in the real world.

The organization of the article proceeds as follows. The next section discusses the relevant literature and details of the research methods employed in the study. Subsequently, data collection is explained followed by the findings from our analysis, and the results related to the research questions. The summary of results, discussion of the contribution to theory and implications for practice, and conclusions of the study are discussed in the last few sections.

Methodology

The techniques of citation analysis, bibliographic coupling, and co-word analysis are used in this research to explore cybersecurity research published over the past ten years (2013 – 2023). The subsequent sub-sections provide an overview of these methodologies and their appropriateness for our study.

Citation Analysis

A citation, in general, is a relationship between a cited document and a citing document (Malin, 1968; Smith, 1981). The very first step in carrying out citation analysis involves identifying either articles or authors for a time-period under consideration (McCain, 1990; Zhao & Strotmann, 2015). The units of analysis for this study are the cybersecurity articles from the Web of Science core collection for the years 2013 to 2023, with a focus on governance, risk, and compliance. Details of data collection are described in the next section. In our study, citation counts are used to identify the most cited authors, articles, journals, and institutions within the corpus of articles.

Bibliographic Coupling

Two articles are bibliographically coupled, if they cite the same article (Kessler, 1963). Thus, the number of shared cited articles between any two articles measures the similarity of the citing articles (Zhao & Strotmann, 2015). Articles with strong bibliographic coupling tend to form distinctive groups (Kessler, 1963), and hence can be used not only to explore the underlying research themes of groups of articles, but also to assess the conceptual relatedness of such groups or clusters of articles. Following previous research (Donthu, Kumar, Pandey, et al., 2021), bibliographic coupling was used to understand the underlying knowledge areas or research themes and their relationships for the cybersecurity risk, governance, and compliance research. VOSviewer (N. van Eck & Waltman, 2009) software is used to identify article clusters that represent the underlying research themes based on bibliographic coupling.

Co-word Analysis

Co-word analysis technique "aims at mapping the structure of scientific research" (Callon et al., 1983). The goal of this technique is to analyzes the co-occurrence of keywords related to each other (Mangalaraj et al., 2022). It enables one to visualize the connections between thoughts and ideas (in the form of keywords) that a small group of specialists have recognized (the authors, in our case). Similar to bibliometrics, co-word analysis has been used in the past to identify the underlying research themes and intellectual structure across different disciplines (Ding et al., 2001; Kim, 2017; Mangalaraj et al., 2022; B.-N. Yan et al., 2015). VOSviewer software (N. van Eck & Waltman, 2009) is used to carry out co-word analysis and visualization of co-word networks.

Data Collection

The search terms "cybersecurity governance," "cybersecurity risk," and "cybersecurity compliance" are used to retrieve bibliometric data from the Web of Science core collections database. The articles selection along with various inclusion/exclusion criteria are shown in Figure 1. The search resulted in 1480 articles.

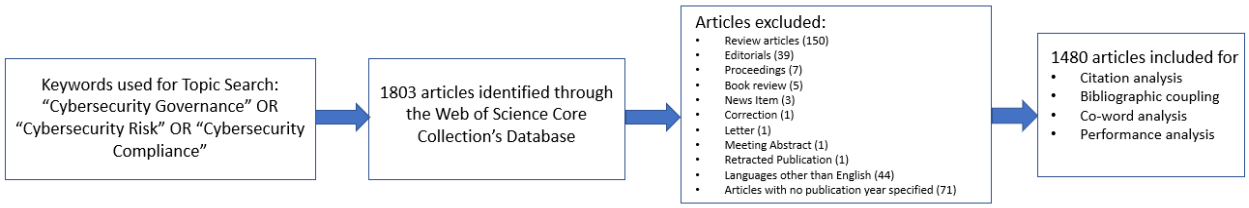

Figure 1: Article Selection Criteria

The number of articles published over the years are shown in Figure 2. The data includes articles indexed in the Web of Science till May 2023, and since all the articles have not been published yet for the ongoing year, there's an apparent drop in the number of articles.

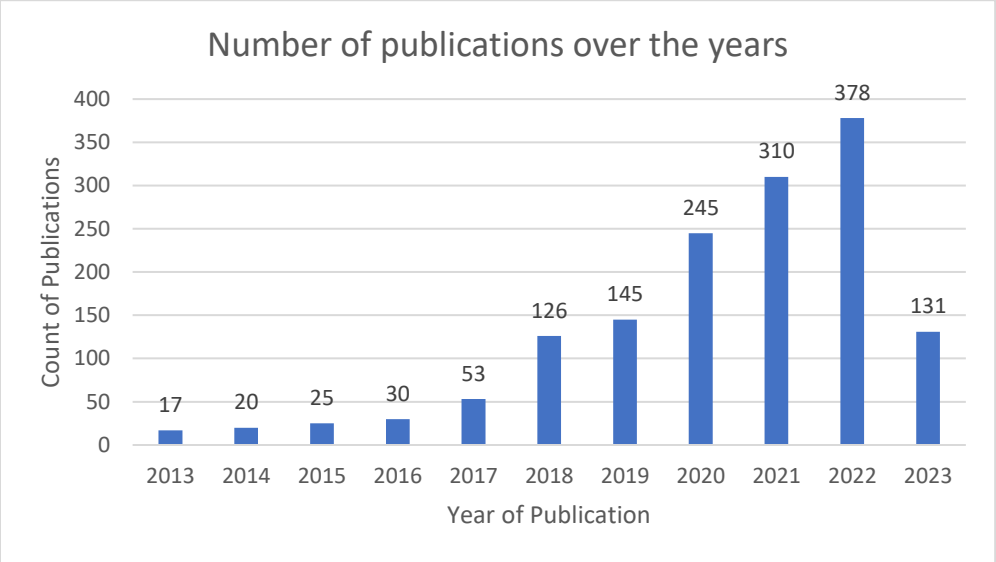

Figure 2: Frequency Distribution of Cybersecurity articles on governance, risk, and compliance

As far as the individual journals are concerned, the corpus includes 646 unique journals with an average of 2.29 articles per journal and median of 1 article per journal. IEEE Access (with 58 publications) is the most prominent journal, followed by Computer & Security (50), and Applied Sciences (36). The frequency distribution for the top ten journals over the years is shown in Figure 3.

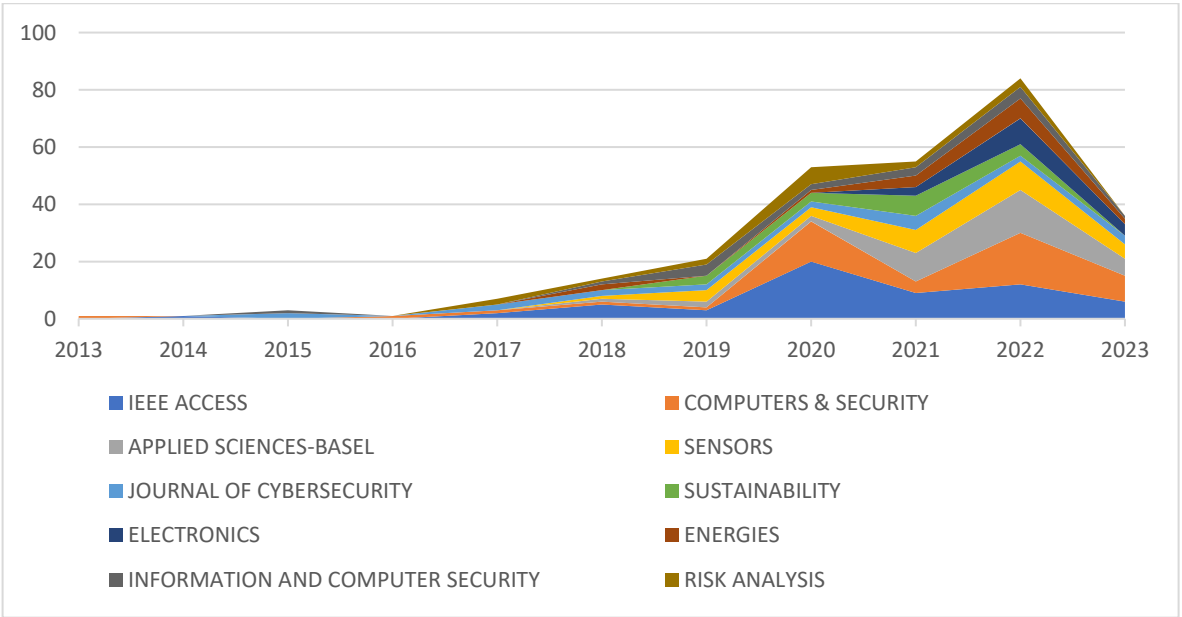

Figure 3: Prominent Journals over the Years

From Figure 2 and 3, one can observe that there's a surge of articles published in this area after the year 2017 both in prominent journals, as well as in general (1335 of 1480 or 90.2% of articles published after

2017). This trend also aligns with the importance received by cybersecurity from business and government organizations in the wake of recent cybersecurity incidents during this time-period. Few notable examples include, data breach in the United States Government's Office of Personal Management in 2015 (Bachura et al., 2022), the adoption of General Data Protection Regulation (GDPR) by the European Union in 2016 (https://gdpr-info.eu/), Equifax data breach affecting approximately 148 million US consumers in 2017 (https://archive.epic.org/privacy/data-breach/equifax/), and Facebook's privacy fiasco involving Cambridge Analytica in the aftermath of US elections in 2018 (Isaak & Hanna, 2018), among others. In addition to being important from the standpoint of cybersecurity risk, policy, and governance research, these events attracted considerable media attention, which may have had an impact on the academic community to publish more pertinent studies.

Analysis and Findings

Underlying Research Themes

The technique of bibliographic coupling is used to group articles based on the shared citations. The semantic overlap in terms of common topics/themes between two articles increases with the number of shared references between them, or with their bibliographic coupling (Boyack & Klavans, 2010; E. Yan & Ding, 2012). VOSviewer software (N. J. van Eck & Waltman, 2013; N. van Eck & Waltman, 2009) is used to cluster articles based on bibliographic coupling, as shown in Figure 4. Each node represents an article and a link between two articles is representative of these articles citing another common article. The distance between articles is representative of their relatedness, with nodes/articles farther from each other being less related than nodes/articles closer to each other. The node color determines the cluster to which an article belongs, and the node size is representative of the importance of the article. Consistent with prior research, the most cited articles (minimum citation count = 10) are used to extract the article clusters representing underlying research themes (Srivastava et al., 2021). Application of bibliographic coupling technique to the corpus resulted in twelve clusters with 347 documents. The underlying research themes were derived from the article abstracts and keywords based on word clouds for each cluster (not shown here).

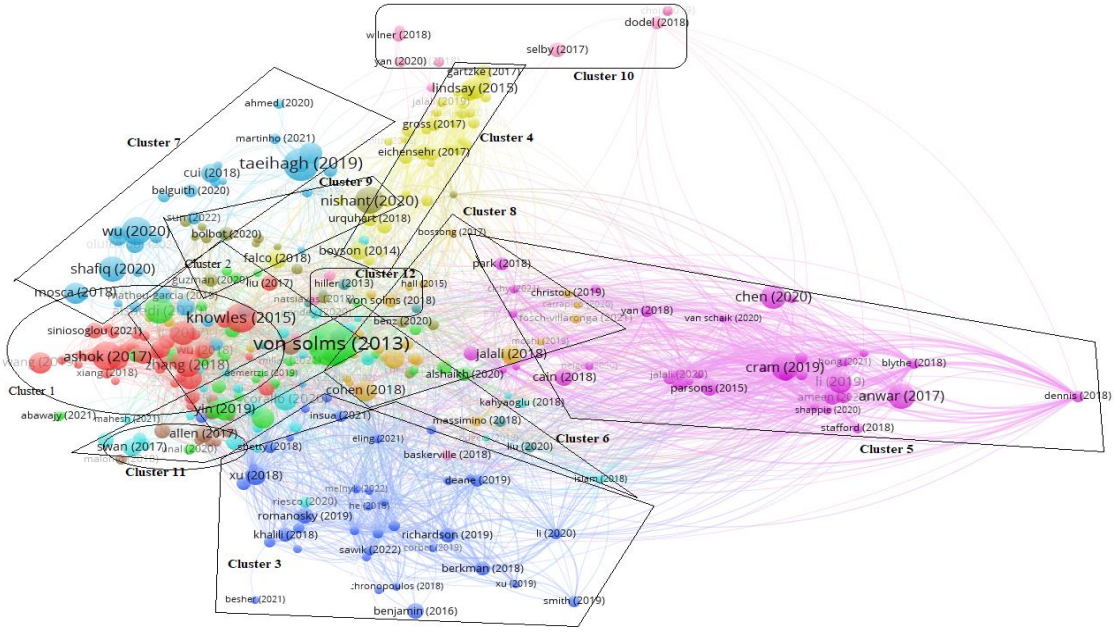

Figure 4: Article Clusters

Table 1: Representative Author Keywords and Underlying Research Themes

Cluster #	Representative Author Keywords	Research Theme
1	Cybersecurity, control systems, risk assessment, industrial, grid, power system, smart network, cyber-physical, attack, intrusion detection, resilience, SCADA, Bayesian, Optimization.	Power, grid, and control systems. Cyber-physical systems and SCADA. Assessment, intrusion detection, and resilience of industrial systems.
2	Cybersecurity, security, malware detection, internet, risk, smart city, learning, IoT, blockchain, networks, assessment, digital information, machine, intelligence, data, anomaly, deep, neural.	Malware detection, Internet, IoT, blockchain networks. Machine intelligence, data anomaly, and deep neural networks.
3	Cybersecurity, Cyber, risk, security, analysis, management, insurance, information, data, breach, supply chain, economics, investments, corporate governance, incident, disclosure, sharing.	Cybersecurity risk and analysis. Data breach disclosure, sharing, and cyber insurance. Economics of cybersecurity. Supply chain investments and corporate governance.
4	Cybersecurity, security, management, internet, protection, critical, governance, risk, infrastructure, resilience, perception, global, control, content, regulatory/regulation, industrial, human, cyber.	Cybersecurity management and internet protection. Infrastructure resilience. Global control and regulations.
5	Cybersecurity, information, security, behavior, compliance, theory, management, system, cyber, motivation, self-efficacy, perception, protection, awareness, social, systems, risk, internet, training, education, judgement, smartphone.	Information security behavior and compliance. Self-efficacy and protection-motivation theory. Training, education, awareness, and judgement.
6	Cybersecurity, supply chain, security, management, manufacturing, blockchain, risk, smart, cyber, intelligence, threat, systems, technology, information, digital, internal, analysis, cyber-attack, cyber-risk, cyber-resilience, Ethereum.	Supply chain security management. IT systems. Internal analysis for cyber-attack, risk, and resilience. Blockchain and Ethereum.
7	Cybersecurity, security, vehicles/vehicle, autonomous, automated, network, risk, detection, intrusion, internet, learning, smart, privacy, technology, IoT, control, connected, systems, simulation, sustainable, entropy, driverless, in-vehicle, controller, assessment.	Cybersecurity, risk, and privacy issues with autonomous/driverless vehicles, and smart IoT control systems.
8	Cybersecurity, security, information, risk, data, cyber, privacy, health, simulation, phishing, vulnerability, resilience, threat, medical, safety, governance, ethics, technology, assessment, healthcare, mobile, policy, hospitals.	Cybersecurity and privacy for healthcare and medical systems. Ethics and governance issues with technology usage within hospitals.
9	Cybersecurity, security, maritime, risk, autonomous, assessment, safety, systems, management, information, artificial intelligence, navigation, resilience, cyberattack, human, inland, agenda.	Cybersecurity, risk, safety, and assessment for (autonomous) maritime systems.
10	Cybersecurity, information, security, digital, artificial intelligence, law, international, data, trade, national, internet, integration, internal, analysis, skills, cyberspace, critical, hit, countermeasures, infrastructure, external.	Artificial intelligence and information security. International cyberspace and law. Countermeasures for infrastructure protection.

Cluster #	Representative Author Keywords	Research Theme
11	Risk, cybersecurity, security, assessment, attack, infrastructure, applications, optimization, networks, theory, models, blockchain, IoT, control, dynamic, critical, federated, cloud, industrial.	Network theory and optimization models. Blockchain, IoT, and cloud infrastructure.
12	Cybersecurity, fuzzy, analysis, security, risk, information, decision, theory, interval-valued, intuitionistic, mining, complex, breach, governance, centralized, heterogeneity.	Cybersecurity-based on complex fuzzy logic and intuitionistic logic.

As one can observe from Figure 4 and Table 1, most research themes are unique with clear boundaries among them, while few others overlap. For instance, cluster 1 includes articles based on securing cyber-physical and industrial systems such as power grids, and SCADA. Similarly, cluster 8 deals with articles focused on security of healthcare systems and related privacy and ethical issues. Cluster 5 is another example, comprising of a group of articles based on behavioral information security and related theories; and cluster 3 is focused on economics of information security. On the other hand, blockchain networks, IoT, and security for networks/Internet are topics of relevance to multiple clusters. To summarize, most research themes with a few exceptions have clear boundaries with respect to the groups of articles and provides us with the current state of cybersecurity research focused on governance, risk, and compliance.

Terms and Co-word Analysis

Before carrying out co-word analysis for author keywords and terms in article abstracts, a preliminary analysis based on frequently occurring author keywords is carried out to further investigate the most prominent research themes. The corpus consists of 8857 author keywords of which 4687 are unique. The top twenty author keywords with a minimum frequency count greater than 25 are shown in Figure 5. The majority of the prominent author keywords, such as Cybersecurity, Security, Risk management, information security, computer security, and risk assessment, are representative of cybersecurity academic research in general. Machine learning, privacy, blockchain, Internet of Things, Artificial Intelligence, cybercrime, data breach, and cyber-physical systems are keywords specific to specific research themes identified above.

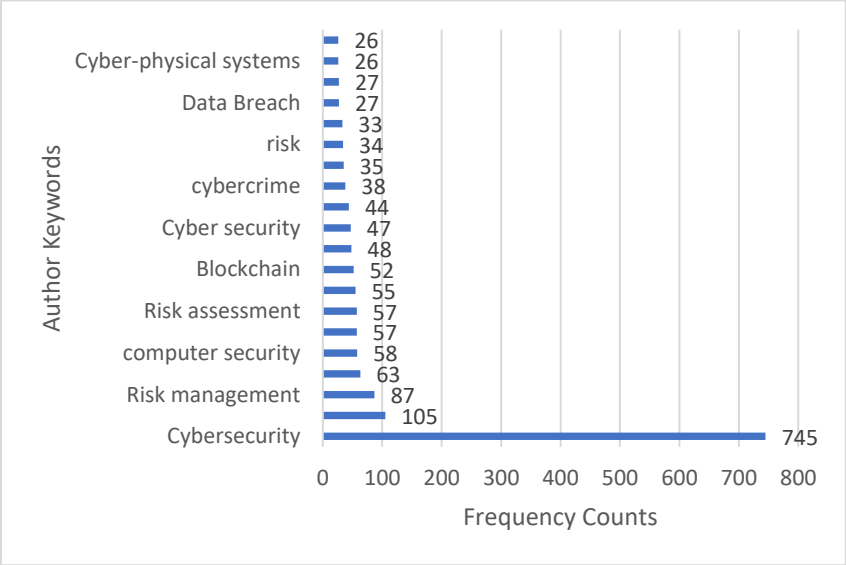

Figure 5: Prominent Author Keywords with Frequency Counts

Figure 6 shows the co-word network of 48 most relevant terms extracted from the article abstracts using the VOSviewer software. Here, each term has a minimum frequency count of 100. Each node corresponds to a unique term from article abstract and the size of node is representative of the frequency of the term. The link between terms/nodes represents their co-occurrence and link thickness signifies frequency of co-occurrence. Based on Figure 6, three clusters emerge. The first cluster includes terms such as country, cyberspace, firm, government, and organization, thematically referring to cybersecurity at both the organizational as well as country level. The second cluster includes terms such as application, attack, blockchain, device, internet, IoT, network, system, technique, thing, and vulnerability. This cluster is representative of research involving securing devices and networks against cybersecurity attacks. The final cluster includes terms such as control, critical infrastructure, and cyberattack, representative of studies focused on securing cyber-physical systems and critical infrastructures. These clusters (along with others) are same as identified above using bibliographic coupling.

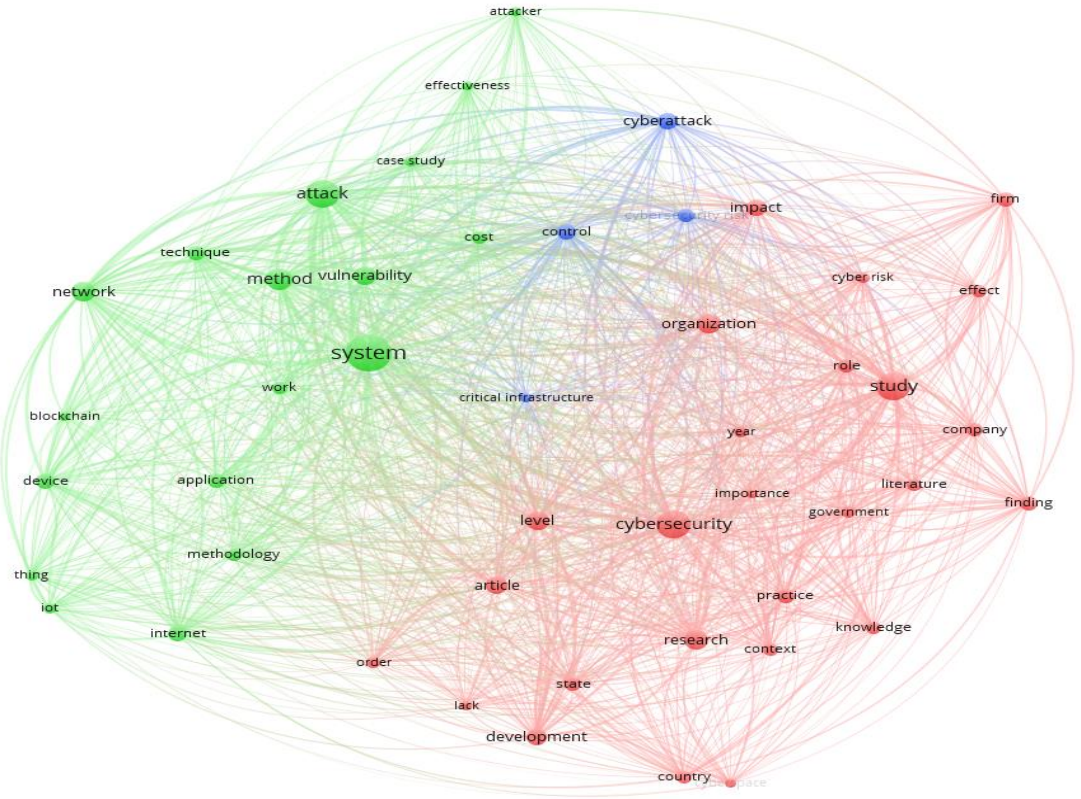

Figure 6: Co-occurrence Network for Terms within Article Abstracts

Although the analyses and findings carried out so far are interesting, these results (and visualizations) does not allow us to investigate the gradual change of interest among cybersecurity researchers over time. Figure 7 shows the choice of words used by cybersecurity researchers for their article titles over the last five to six years. Titles of aticles were often regarded as a means of knowledge transmission informing the reader as to what the article is about (Haggan, 2004). Hence, terms used by researchers in article titles were investigated using co-word network visulizations to extract the underlying themes and their relatinships. The co-occurrence network shoen in Figure 7 consist of 98 terms with mimum frequency count of 6. Since, majority of publications (about 90%) for cybersecurity governance, risk, and compliance within our corpus happened after 2017, the range of years for this overlay visualization is choosen as between 2018 and 2023 (till May 23, 2023).

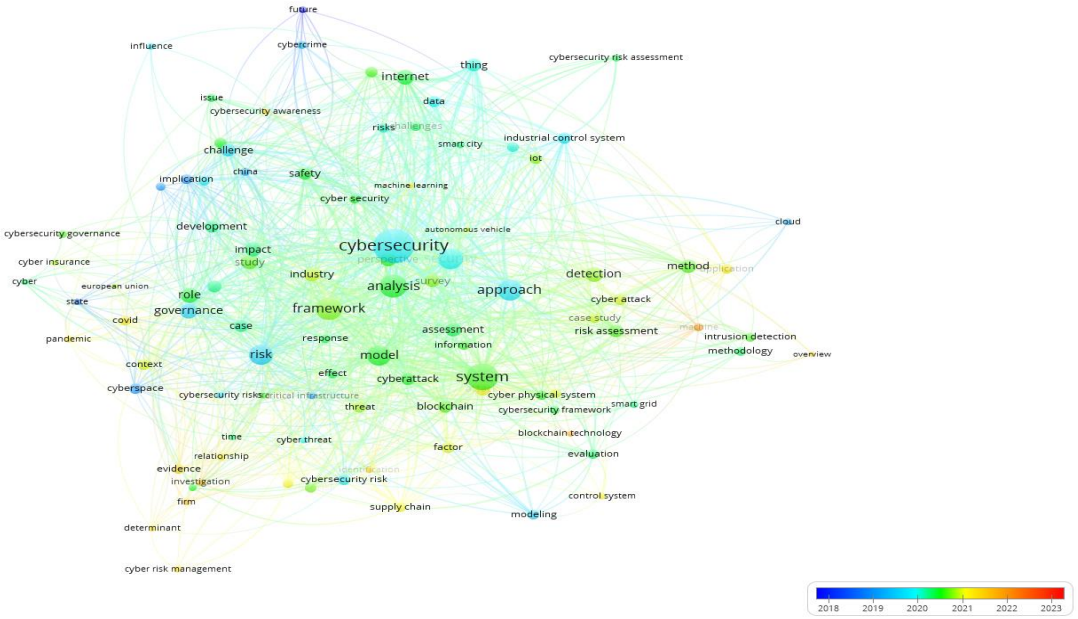

Figure 7: Co-occurrence Network of Terms within Article Titles over Time

The legend in Figure 7 shows the range of colors associated with the timeline of interest (2018 – 2023). The node color for the term represents the average year in which it is most popularly used within the title of articles. For instance, the average publication year for the term "cyberspace" is 2019.14, hence represented as light blue corresponding to the year 2019. Similarly the average publishing year for "artificial intelligence" is 2020.60, and is 2021.71 for "blockchain technology", as used in the article titles.

An interesting insight from this representation of terms used by authors in the article titles over the past few years shows the gradual shift in cybersecurity governance, risk, and compliance research. Terms as used in the titles (and hence articles representative of these terms) such as future, cybercrime, implication, information security, state, critical infrastructure, cloud, and cyberspace were more pupularly used in the 2018 and early 2019. Influence, challenge, governance, risk, cybersecurity risk, approach, industrial control system, cyber threat, security, privacy, trust, cyberphysical system, data, technology, smart city, safety, evaluation, impact, internet, cyberattack, information, intrusion detection, assessment, model, smart grid, and thing were important title terms used in late 2019 and early 2020. Late 2020, followed by 2021 and 2022 saw usage of terms such as control system, pandemic, covid, artificial intelligence, IoT, autonomous vehicle, detection, risk assessment, blockchain, cyber risk, machine learning, machine, application, supply chain, firm, cyber risk management, threat, and case study. Hence, one can conclude a gradual shift in cybersecurity academic research focussing on critical infrasructure, cybercrime, and information security towards blockchain, IoT, and artificial intelligence.

Performance Analysis

Performance analysis pertains to examining the academic contributions of research units or components such as authors, institutions, and nations (Donthu, Kumar, Mukherjee, et al., 2021). Our corpus consists of 5239 authors of which 4526 are unique. Within the corpus, there are 263 single author papers and the maximum number of authors on a single paper is 38. The average number of authors per paper is 3.37 and the median is 3. Most research articles were written by three (6.47%), two (6.36%), or four (5.08%) authors. Chunjie Zhou is the top publishing author (n=10), followed by Scott J. Shackelford (n=9), Yuanqing Qin (n=8), and Lingfeng Wang (n=8).

Authors in our corpus are affiliated with 4127 institutions of which 1385 are unique. Most number of authors (n=118) are affiliated with the RLUK or Research Libraries UK, which is a consortium of significant research libraries in the United Kingdom and Ireland. RLUK is followed by The Indiana University System (n=61), and The State University System of Florida (n=53). The distribution of the top institutions with the number of author affiliations greater than 20 is shown in Figure 8.

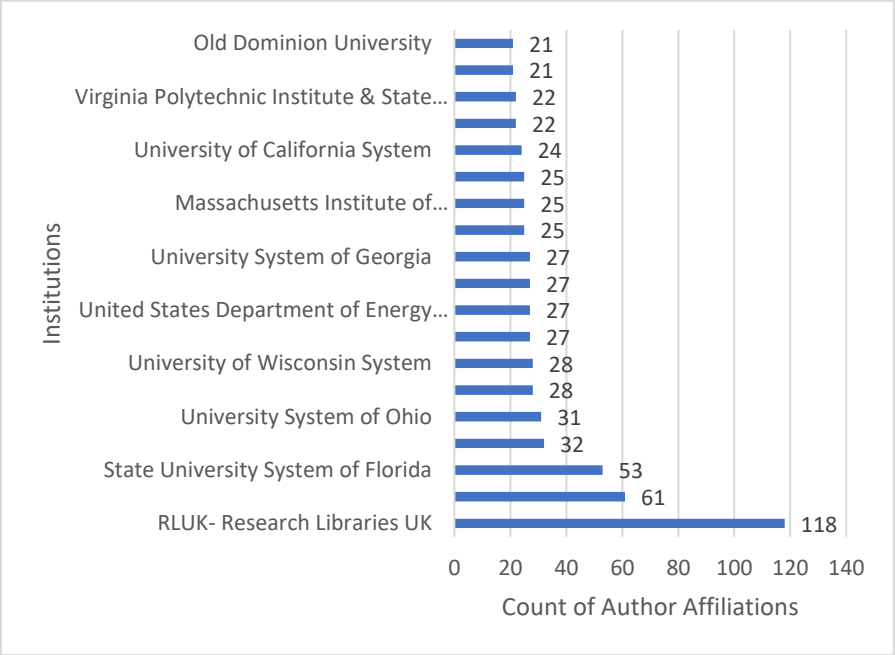

Figure 8: Institutions with Most Author Affiliations

With respect to countries, authors within our corpus are affiliated with institutions in 96 different countries. The greatest number of articles were published from institutions within the United States of America (n=566). This is followed by England (n=144), the Peoples Republic of China (n=129), and Australia (n=99).

As a final performance metric, we investigated the citations received by individual authors, articles, and journals. Table 2 shows the ten most cited authors, their current institutional affiliations, number of documents in the corpus, and number of citations received.

Table 2: Most Cited Authors

Author Name	Current Author Institution Affiliation	Number of Documents	Number of citations received
R Von Soms	Nelson Mandela University	2	343
J Van Niekerk	Nelson Mandela University	1	309
CJ Zhou	Huazhong University of Science and Technology	10	290
HSM Lim	National University of Singapore	3	283
A Taeihagh	National University of Singapore	3	283
YQ Qin	Huazhong University of Science and Technology	8	246
L Xu	Hunan University	5	211
NX Xiong	Colorado Technical University	4	205
W He	Old Dominion University	4	200
M Anwar	North Carolina AT&T State University	3	196

Table 3: Most Cited Articles and Author Keywords

Article	# of citations received	Author Keywords/Title
(von Solms & van Niekerk, 2013)	309	Information security, Cyber security, Cybersecurity, Cyber-Security, Computer security, Risk, Threat, Vulnerability
(Taeihagh & Lim, 2019)	175	Autonomous vehicles; automated driving; policy; governance; risks; safety; liability; privacy; cybersecurity; incumbent industries
(Knowles et al., 2015)	144	"A survey of cyber security management in industrial control systems"
(Ashok et al., 2017)	136	Attack resilience; attack-resilient framework; cyber-physical security; wide-area monitoring protection and control
(Wu et al., 2020)	130	Controller area network (CAN), cybersecurity, in-vehicle network (IVN), intrusion detection system (IDS), information entropy, machine learning.
(Alsaedi et al., 2020)	118	Internet of Things (IoT), Industrial Internet of Things (IIoT), cybersecurity, intrusion detection systems (IDSs), dataset.
(Anwar et al., 2017)	107	Gender differences, Cybersecurity beliefs, Cybersecurity behaviors, Cybersecurity behavior model
(Cram et al., 2019)	105	Information security, cybersecurity, information security policies, compliance, meta-analysis, relative weight analysis
(Li et al., 2017)	92	Cyber-physical systems, cybersecurity, defense in-depth strategy, microgrid-based distributed electric power systems, risk assessment and mitigation, software-defined networking
(Zhang et al., 2018)	89	Bayesian network (BN), cybersecurity, fuzzy probability, industrial control systems (ICSs), risk assessment

The purpose of including the author keywords (or article title) in Table 3 is to further identify the underlying research themes based on the most cited articles within our corpus. Based on the author keywords (and title for one article where author keywords were not available) foremost cited articles, three themes emerge – 1) cybersecurity for autonomous vehicles, 2) behavioral information and cyber security, and 3) cybersecurity for cyber-physical, industrial, and IoT systems. These research areas again overlap with our themes based on bibliographic coupling.

Table 4: Most Cited Journals

Journal	Number of citations received	Number of Articles
Computers & Security	717	51
IEEE Access	633	58
Proceedings of the IEEE	306	6
International Journal of Information Management	262	5
Computers in Human Behavior	247	9
Journal of Cybersecurity	243	20
Sensors	214	31
Risk Analysis	200	18
IEEE Transactions on Smart Grid	197	11
Transport Reviews	195	2

The corpus includes articles published in 674 unique journals of which the most cited ones and the corresponding number of articles are shown in Table 4. The number of citations and impact factor of a journal along with many other criteria are often considered by a researcher while deciding where to publish his/her research (Suiter & Sarli, 2019). Hence, this list of most cited journals allows a researcher working in cybersecurity compliance, risk, and governance to choose a journal.

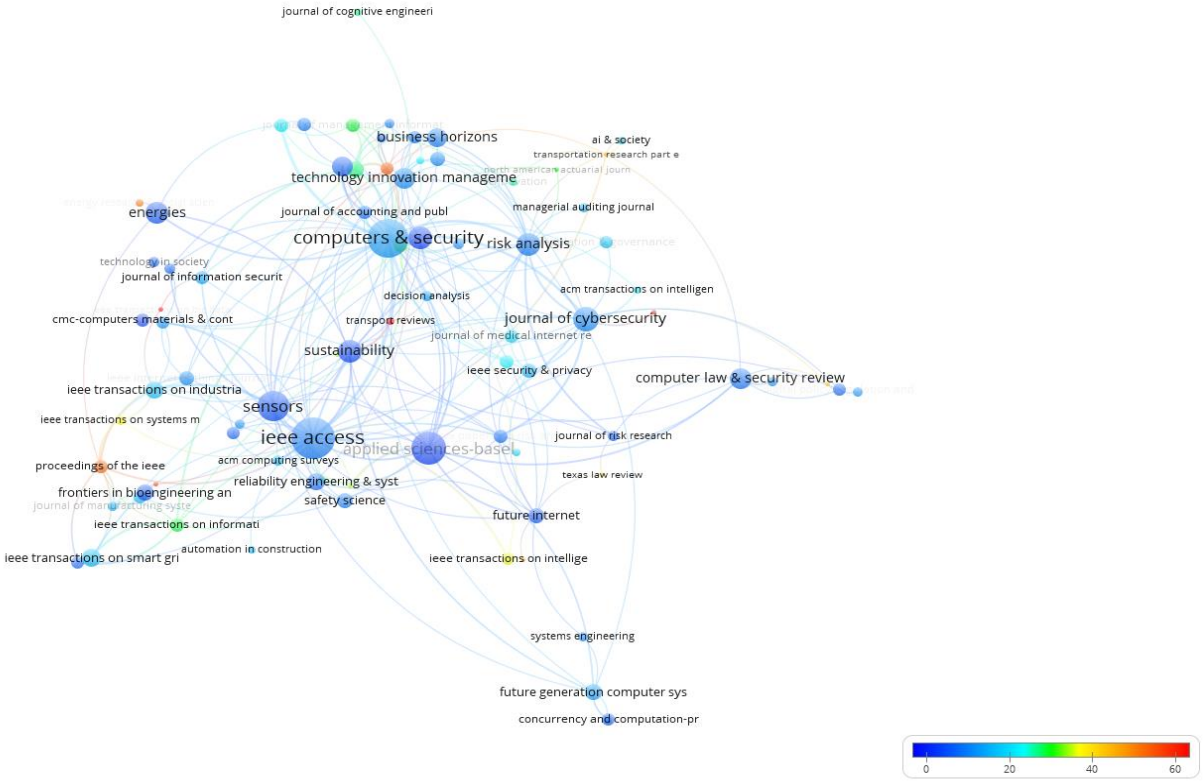

Figure 9: Network of Most Cited Journals

Figure 9 shows an overlay network visualization of 84 most cited journals within our corpus, with each journal having a minimum citation count of 29. The size of the node is representative of the number of articles for the respective journal. The greater number of articles the larger the node size. The node color represents the average citation received by the journal, as per the legend. For instance, the number of articles published in the Computers & Security journal is 51, and the total number of citations received by these articles is 717. Hence, the node size for this journal is large. The average number of citations received per article for this journal is 14.06, hence represented by a blue colored node. On the other hand, the node for the Transport Reviews journal is small since there are only 2 documents in our corpus for this journal. The total number of citations received by these two articles is 195. Since, the average number of citations for this journal is 97.5, the node color is red.

Results

Article clusters and their respective research themes were identified, first using bibliographic coupling analysis, and then using author keyword co-occurrence analysis to answer the first research question. Based on the article clusters, twelve underlying research themes for cybersecurity governance, compliance, and risk were identified. Frequency count on prominent author keywords, co-word analysis on article abstracts, and co-word analysis of terms within article titles, further allows us to investigate the underlying thematic

areas, and gradual change in these themes over the last few years (research question 2). Finally, to answer research question 3, performance analysis for various research constituents (authors, articles, institutions, countries, and journals) is carried out to identify the important actors in this discipline.

Discussion

The main theoretical contribution of research carried out in this study is the identification of the underlying research themes based on the existing cybersecurity research focused on governance, compliance, and risk. The investigation of the latent themes in the article corpus allows us to explore the recent past and present state of research. Based on our findings from author keyword co-occurrence analysis, there's a recent interest of cybersecurity researchers towards applying tools, techniques, and methodologies from cybersecurity discipline to novel domains such as artificial intelligence, IoT, smart cities, blockchain technology, supply chains, and autonomous vehicles. In the past, cybersecurity researchers have played a significant role in designing and implementing information security protocols for computer networks, cyber-physical systems, and critical infrastructures such as power grids. Hence, these researchers are in a unique position to use their expertise and experience to handle cybersecurity issues arising in the emerging novel domains.

The current state of cybersecurity research appears to have focused more on the technical aspects of information security without going too deeply into some of the interactions involving people, business organizations, and technology. With growing importance of securing data at various levels, and ever-increasing government regulations towards safeguarding user privacy, information systems researchers, with their extensive knowledge with data-related IT initiatives, are uniquely positioned to explore emerging cybersecurity issues and help society (individuals, businesses, and governments) mature their information security practices. Information systems scholars are not new to the idea that social and technological imperatives must coexist. Information systems researchers have a chance to contribute to this area of study since the field has extensive knowledge in socio-technical system design, adoption, and acceptance. Cyber security analytics is another area where significant contributions can be made by information systems researchers active in artificial intelligence and data science.

Limitations

There is substantial evidence of the limits of citations and bibliometric research; for instance, see (Nerur et al., 2008). The fact that the context in which citations occur is ignored and equal weightage given to them are foremost among these. However, bibliometric analyses based on citations are widely available and have proved extremely helpful in elucidating the conceptual underpinnings of numerous fields. Our study tries to improve on these shortcomings by analysis of author keywords, and co-word analysis of article titles, and abstracts, to explore the thematic areas inherent in the article corpus.

Conclusion

The goal of this study is to identify the underlying research themes for cybersecurity research focused on risk, compliance, and governance, along with investigating the gradual change in these themes and to identify the current state of research. Results reveal twelve article clusters – 1) cybersecurity for cyber-physical systems, 2) cybersecurity for Internet and IoT, 3) economics of information security, 4) international law and global cyberspace regulations, 5) behavioral information security, 6) cybersecurity

for supply chains, 7) cybersecurity for autonomous vehicles, 8) healthcare security and privacy, 9) securing (autonomous) maritime systems, 10) artificial intelligence and information security, 11) securing blockchain networks, IoT and cloud, and 12) cybersecurity-based on complex fuzzy logic and intuitionistic logic. Co-word analysis of terms from article titles shows a recent surge of interest of cybersecurity researchers towards contemporary topics such as artificial intelligence, IoT, blockchain, and autonomous vehicles. Finally, the most important research constituents are identified through performance analysis.

References

Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. *IEEE Access*, *8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443.

Ashok, A., Govindarasu, M., & Wang, J. (2017). Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. *Proceedings of the IEEE*, *105*(7), 1389–1407. https://doi.org/10.1109/JPROC.2017.2686394

Bachura, E., Valecha, R., Chen, R., & Rao, H. R. (2022). THE OPM DATA BREACH: AN INVESTIGATION OF SHARED EMOTIONAL REACTIONS ON TWITTER. *MIS Quarterly*, *46*(2).

Boyack, K. W., & Klavans, R. (2010). Co-citation analysis, bibliographic coupling, and direct citation: Which citation approach represents the research front most accurately? *Journal of the American Society for Information Science and Technology*, *61*(12), 2389–2404. https://doi.org/10.1002/asi.21419

Callon, M., Courtial, J.-P., Turner, W. A., & Bauin, S. (1983). From translations to problematic networks: An introduction to co-word analysis. *Social Science Information*, *22*(2), 191–235.

Charvet, F. F., Cooper, M. C., & Gardner, J. T. (2008). The intellectual structure of supply chain management: A bibliometric approach. *Journal of Business Logistics*, *29*(1), 47–73.

Chen, L., Baird, A., & Straub, D. W. (2019). An analysis of the evolving intellectual structure of health information systems research in the information systems discipline. *Journal of the Association for Information Systems*, *20*(8), 5.

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–554.

Ding, Y., Chowdhury, G. G., & Foo, S. (2001). Bibliometric cartography of information retrieval research by using co-word analysis. *Information Processing & Management*, *37*(6), 817–842.

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.

Donthu, N., Kumar, S., Pandey, N., & Gupta, P. (2021). Forty years of the International Journal of Information Management: A bibliometric analysis. *International Journal of Information Management*, *57*, 102307.

Ferreira, J. J., Fernandes, C. I., & Kraus, S. (2019). Entrepreneurship research: Mapping intellectual structures and research trends. *Review of Managerial Science*, *13*, 181–205.

Haggan, M. (2004). Research paper titles in literature, linguistics and science: Dimensions of attraction. *Journal of Pragmatics*, *36*(2), 293–317.

Hathaway, M., & Klimburg, A. (2012). Preliminary considerations: On national cyber security. *National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56–59.

Kessler, M. M. (1963). Bibliographic coupling between scientific papers. *American Documentation*, *14*(1), 10–25.

Kim, H. (2017). A Study on the Intellectual Structure of Data Science Using Co-Word Analysis. *Journal of the Korean Society for Information Management*, *34*(4), 101–126.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52–80.

Li, Z., Shahidehpour, M., & Aminifar, F. (2017). Cybersecurity in distributed power systems. *Proceedings of the IEEE*, *105*(7), 1367–1388.

Malin, M. V. (1968). Science Citation Index-a New Concept in Indexing. *Library Trends*, *16*(3), 374.

Mangalaraj, G., Singh, A., & Taneja, A. (2022). Probing the Past to Guide the Future IT Regulation Research: Topic Modeling and Co-word Analysis of SOX-IS Research. *Information Systems Management*, 1–14.

McCain, K. W. (1990). Mapping authors in intellectual space: A technical overview. *Journal of the American Society for Information Science*, *41*(6), 433.

Pilkington, A., & Meredith, J. (2009). The evolution of the intellectual structure of operations management—1980–2006: A citation/co-citation analysis. *Journal of Operations Management*, *27*(3), 185–202. https://doi.org/10.1016/j.jom.2008.08.001

Smith, L. C. (1981). *Citation analysis*.

Srivastava, P. R., Sharma, D. P., Kaur, I., Wamba, S. F., & Wang, W. Y. C. (2021). Intellectual structure and publication pattern in journal of global information management: A bibliometric analysis during 2002-2020. *Journal of Global Information Management (JGIM)*, *29*(4), 1–31.

Suiter, A. M., & Sarli, C. C. (2019). Selecting a journal for publication: Criteria to consider. *Missouri Medicine*, *116*(6), 461.

Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, *39*(1), 103–128.

van Eck, N. J., & Waltman, L. (2013). VOSviewer manual. *Leiden: Univeristeit Leiden*, *1*(1).

van Eck, N., & Waltman, L. (2009). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., & Li, K. (2020). A Survey of Intrusion Detection for In-Vehicle Networks. *IEEE Transactions on Intelligent Transportation Systems*, *21*(3), 919–933. https://doi.org/10.1109/TITS.2019.2908074

Yan, B.-N., Lee, T.-S., & Lee, T.-P. (2015). Mapping the intellectual structure of the Internet of Things (IoT) field (2000–2014): A co-word analysis. *Scientometrics*, *105*, 1285–1300.

Yan, E., & Ding, Y. (2012). Scholarly network similarities: How bibliographic coupling networks, citation networks, cocitation networks, topical networks, coauthorship networks, and coword networks relate to each other. *Journal of the American Society for Information Science and Technology*, *63*(7), 1313–1326. https://doi.org/10.1002/asi.22680

Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y., & Hu, B. (2018). A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems. *IEEE Transactions on Industrial Informatics*, *14*(6), 2497–2506. https://doi.org/10.1109/TII.2017.2768998

Zhao, D., & Strotmann, A. (2015). *Analysis and visualization of citation networks*. Morgan & Claypool.