JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

GLOBAL RESEARCH TRENDS IN CYBERSECURITY FOR GOVERNMENT AND PUBLIC SECTOR SYSTEM

Angel Cylo Real
La Consolacion University Philippines
Malolos Bulacan, Philippines
Email: cylo11388@gmail.com

Jessa Bil Brogada
La Consolacion University Philippines
Malolos, Bulacan, Philippines
Email: brogadajessa@gmail.com

John Joshua B. Sazon
La Consolacion University Philippines
Malolos, Bulacan, Philippines
Email: johnjoshuasazon@gmail.com

Roxanne Caroll SP. Baoy
La Consolacion University Philippines
Malolos, Bulacan, Philippines
Email: roxannecarollbaoy@yahoo.com

Jayson A. Batoon
La Consolacion University Philippines
Malolos, Bulacan, Philippines
Email: jayson.batoon@email.lcup.edu.ph

Corresponding Author

Angel Cylo Real
La Consolacion University Philippines
Malolos Bulacan, Philippines
Email: cylo11388@gmail.com

Abstract

This study conducts a bibliometric analysis of cybersecurity research in government and public sector systems to examine its intellectual structure, research trends, and thematic evolution. A dataset of 460 peer-reviewed journal articles published between 2017 and 2025 was retrieved from the Scopus database and analyzed using citation, co-citation, and co-word techniques. The results indicate substantial growth in scholarly output, reflecting increasing prioritization of cybersecurity in digital government initiatives. Citation analysis identifies key contributors and influential publications across developed and emerging economies. Co-citation analysis reveals knowledge clusters centered on human behavior, information systems governance, and security policy compliance. Co-word analysis highlights themes including artificial intelligence, blockchain, digital transformation, privacy, and risk management. Findings underscore the interdisciplinary nature of cybersecurity

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

research, integrating technological, organizational, and governance dimensions. This study maps the knowledge base and identifies emerging research directions, providing insights for future research and development of resilient and secure public sector systems.

Keywords: *Cybersecurity, Digital government, Bibliometric analysis, Information systems, Public sector, Risk management.*

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Introduction

Cybersecurity in government and public sector systems extends well beyond setting firewall rules or training employees on strong passwords and safe online habits. The concept of e-government cybersecurity encompasses the methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyberattacks and unauthorized access (Alketbi et al., 2018). Cybersecurity is a set of protective measures used to secure digital systems and their data from malicious actions by attackers or harmful software (Khando et al., 2021). It generally encompasses the technologies, policies, human behavior, and organizational practices that protect computer systems, networks, and digital information from misuse, unauthorized access, attacks, or policy violations (Beretas, 2024). Cybersecurity has become increasingly important for government and public sector organizations as digital technologies and e-government services continue to expand. It focuses on protecting data, networks, and information systems from risks, threats, and vulnerabilities through appropriate governance frameworks, security mechanisms, and management practices that ensure the availability, privacy, and integrity of information (Khando et al., 2021; Aslan et al., 2023). As governments increasingly rely on digital infrastructure to deliver public services, strengthening cybersecurity strategies is essential to maintaining secure and reliable systems (Vial, 2021). Bibliometric analysis is a useful method for assessing the scope of academic contributions and identifying emerging trends in scholarly discourse (Donthu et al., 2021). Therefore, this study examines the evolution of cybersecurity research in digital government.

This study offers a comprehensive bibliometric analysis, particularly citation, co-citation, and co-word analysis, which have proven useful in tracing the evolution and developmental trajectory of scholarly research across disciplines. Bibliometric techniques allow researchers to visualize the overall landscape of their field, as demonstrated in the examination of the cybersecurity capabilities of individual farms' communication networks, which sought to identify deficiencies in network setups and practices and to highlight the need for improved cybersecurity measures, awareness, and guidance to better protect agricultural communication systems against threats and vulnerabilities (Nikander et al., 2020). More importantly, an investigation into the role of security, including cybersecurity perceptions, trust, and privacy in the adoption and use of e-government services, helped identify the factors that influence end users' perceptions and behavioral intentions toward e-government security (Alharbi, Papadaki, & Dowland, 2017).

Present Study

This study aims to conduct a comprehensive bibliometric analysis of the academic literature on cybersecurity in government and public sector systems. With governments' increasing reliance on digital technologies and e-government platforms, cybersecurity has become a critical component for protecting public information systems, digital infrastructure, and citizen data. Despite the growing number of studies in this field, there remains a need to systematically map the intellectual structure, research trends, and emerging themes within the cybersecurity domain in digital government contexts. Therefore, this study examines the development and patterns of scholarly publications to provide a deeper understanding of the evolution and current state of cybersecurity research in the public sector.

1. **Citation Analysis:** To identify the most influential publications, journals, authors, institutions, and countries contributing to cybersecurity research in government and public sector systems.
2. **Co-Citation Analysis:** To analyze the intellectual structure of the field by examining relationships among highly cited publications and identifying key research clusters that shape cybersecurity and digital government.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

3. **Co-Word Analysis:** To explore the thematic structure of the field by analyzing keyword co-occurrence patterns and identifying major research topics, technological trends, and emerging areas in cybersecurity for government systems.

Literature Review

Cybersecurity has become a critical component of modern governance as governments increasingly adopt digital technologies to deliver services and manage public information. As e-government platforms expand, protecting digital infrastructure, networks, and sensitive citizen data has become a major priority for public-sector institutions. Cybersecurity refers to the technologies, policies, and practices used to safeguard information systems from threats such as malware, ransomware, phishing, and unauthorized access (Khando et al., 2021; Aslan et al., 2023). With the rapid digitalization of government services, public institutions are increasingly exposed to cyber risks that can disrupt operations, compromise sensitive data, and undermine public trust. As a result, cybersecurity strategies have become essential for maintaining the confidentiality, integrity, and availability of government information systems.

Recent studies emphasize that cybersecurity in government environments requires a combination of technological capabilities and effective governance frameworks. According to Vial (2021), digital transformation in organizations involves integrating advanced technologies into strategic management processes to improve efficiency and service delivery. In the context of public administration, digital transformation initiatives must also incorporate robust security measures to protect digital infrastructure and maintain citizen trust. Similarly, Twizeyimana and Andersson (2019) highlight that the success of digital government initiatives depends on their ability to generate public value, including transparency, service reliability, and secure information management. These perspectives suggest that cybersecurity should be integrated into broader digital governance strategies to ensure the sustainability of e-government systems.

Another important perspective in the literature focuses on human and organizational factors that influence cybersecurity practices. Research indicates that employee awareness and behavior significantly affect the effectiveness of organizational security systems. Hadlington (2017) emphasizes that human factors, such as attitudes toward cybersecurity and online behavior, can increase or reduce vulnerability to cyber threats. Additionally, emerging technologies such as artificial intelligence and advanced data analytics are increasingly being used to strengthen cybersecurity capabilities and improve threat detection in complex digital environments (Aslan et al., 2023). Together, these studies demonstrate that effective cybersecurity in the public sector requires the integration of technological innovation, governance mechanisms, and human behavioral considerations.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Methodology

This study employs a quantitative bibliometric approach to examine the intellectual structure, research development, and thematic evolution of cybersecurity in government and public sector systems. Bibliometric analysis is widely used to evaluate research trends, influential publications, collaboration patterns, and knowledge structures within a specific field through the use of bibliographic metadata such as citations, keywords, authors, and sources (Donthu et al., 2021; Kumar, George, & PS, 2023; Pessin, Yamane, & Siman, 2022). In this study, bibliometric techniques were applied to identify the major contributors, the most influential publications, and emerging themes in cybersecurity, e-government, digital government, and public sector information security. Following established bibliometric procedures, the study was carried out in several stages, including database selection, search string formulation, data screening, data analysis, and visualization of bibliometric networks using VOSviewer (Baas et al., 2020; Donthu et al., 2021).

Bibliometric Approach

This study adopts a quantitative bibliometric approach to map the research landscape of cybersecurity in government and public sector systems. Bibliometrics is a powerful statistical method used to assess scientific productivity and identify patterns of knowledge accumulation within a research domain by examining publication outputs, citation counts, co-citation relationships, and keyword co-occurrences (Donthu et al., 2021). By focusing on objective bibliographic indicators, this approach allows for the discovery of intellectual structures and thematic developments in the field. It also provides a retrospective overview of how cybersecurity research in digital government has evolved over time, particularly regarding information security governance, risk management, and technological innovation (Kumar, George, & PS, 2023; Pessin, Yamane, & Siman, 2022).

Data Collection Using Scopus

The primary data for this research were retrieved from the Scopus database, widely recognized as one of the most comprehensive and reputable sources of peer-reviewed scholarly literature and bibliometric studies (Baas et al., 2020). A targeted search query was developed to capture publications on cybersecurity in government and public-sector systems. The search string used was: TITLE-ABS-KEY (“cybersecurity” OR “cyber security”) AND TITLE-ABS-KEY (“e-government” OR “digital government”). This search strategy was designed to include studies addressing both the security dimension and the digital government context of the research topic. The initial search yielded 558 documents in Scopus. The search was limited to the 2017 to 2025 period to ensure that the dataset reflects recent developments and contemporary scholarly discussions in the field. This time frame was selected because it captures the growing research interest in cybersecurity as governments increasingly adopt digital transformation and e-government platforms (Khando et al., 2021; Aslan et al., 2023; Vial, 2021).

Screening Process

To ensure the quality and relevance of the final dataset, a rigorous screening process was applied to the initial search results. The document type was limited to journal articles only, while conference papers, book chapters, reviews, and other non-article publications were excluded. This process was intended to focus the analysis on peer-reviewed journal publications that provide more developed and validated scholarly contributions. After applying the inclusion criteria, the dataset was reduced from 558 documents to 460 journal articles. This refined sample formed the basis for the bibliometric analysis. The screening process helps improve dataset consistency and enhances the reliability of the findings by ensuring that only relevant and high-quality studies are included in the analysis (Donthu et al., 2021).

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Data Analysis and Visualization

The final dataset was analyzed using VOSviewer software for bibliometric mapping and visualization. VOSviewer is a widely used tool for constructing and visualizing bibliometric networks based on citation, co-citation, and keyword co-occurrence data. In this study, the software was used to perform citation, co-citation, and co-word analyses to map the intellectual and thematic structure of cybersecurity research in government and public-sector systems. These techniques enabled the identification of key documents, influential authors, productive countries, highly cited sources, and recurring research themes. The use of VOSviewer also enabled graphical representations of bibliometric relationships through network maps and cluster visualizations, thereby providing a clearer understanding of the field's structure and development (McAllister et al., 2022).

Citation Analysis

Citation analysis was conducted to identify the most influential publications, authors, sources, and countries within the dataset. This technique measures the impact of scholarly works by the number of times they have been cited in other publications. In the present study, citation analysis identified the leading documents and contributors in cybersecurity research on government and public-sector systems. The results highlighted the strong influence of blockchain studies on e-government, information security awareness, artificial intelligence, machine learning, and digital transformation. Citation analysis is particularly useful for revealing the research that has shaped the field and identifying the most visible contributors to scholarly knowledge production (Donthu et al., 2021).

Co-citation Analysis

Co-citation analysis was employed to map the intellectual structure of the field by examining how frequently two documents are cited together in subsequent studies. This technique helps reveal the foundational knowledge base and the major schools of thought that underpin a research domain. Using VOSviewer, the co-citation analysis in this study generated clusters of highly related references, showing the underlying conceptual groupings within the literature. The resulting clusters reflected major themes, including human behavior and institutional factors in cybersecurity, security policy compliance, digital transformation in organizations, information systems governance, and e-government service adoption. Through this method, the study was able to uncover the “invisible college” of authors and works that collectively influence cybersecurity scholarship in digital government settings (Bulgurcu et al., 2010; Herath & Rao, 2009; Hu et al., 2012; Siponen et al., 2014; Safa et al., 2016).

Co-word Analysis

The conceptual evolution of the field was examined through co-word analysis, which analyzes the co-occurrence of keywords in titles, abstracts, and author-provided keyword lists. Using VOSviewer, this process generated thematic clusters that reflect the major research topics and emerging trends within the literature. In this study, co-word analysis identified recurring terms such as cybersecurity, e-government, information security, public sector, digital transformation, artificial intelligence, blockchain, privacy, cloud computing, machine learning, and risk management. These patterns demonstrate that the field is both multidisciplinary and rapidly evolving, combining technological, organizational, and governance-related concerns. Co-word analysis is particularly useful in identifying how concepts are linked across publications and in revealing the thematic direction of a field over time (Donthu et al., 2021; Vial, 2021; Aslan et al., 2023).

Table 1 presents the key search keywords used in the study along with their corresponding justifications. The selected terms were carefully chosen to ensure comprehensive coverage of the research domain, capturing both

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

the core concepts of cybersecurity and the evolving context of digital government. By combining these keywords, the study encompasses a wide range of relevant publications and provides a balanced representation of the intersection of cybersecurity and public-sector digital transformation.

Table 1: Search string in Scopus database

No	Keywords	Justification
1	"cybersecurity" OR "cyber security"	To capture a broad range of publications related to cybersecurity. These terms refer to the practice of protecting systems, networks, and data from digital attacks. It is used in defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
2	"e-government" OR "digital government"	To capture a broad range of publications on governments using ICTs to digitize and improve existing, often siloed, government services, with a focus on efficiency, such as online tax filing or permit applications. This terminology refers to a more advanced, holistic approach that uses technology to transform public value, foster open data, enhance citizen engagement, and integrate systems across agencies for a seamless, user-centric experience.

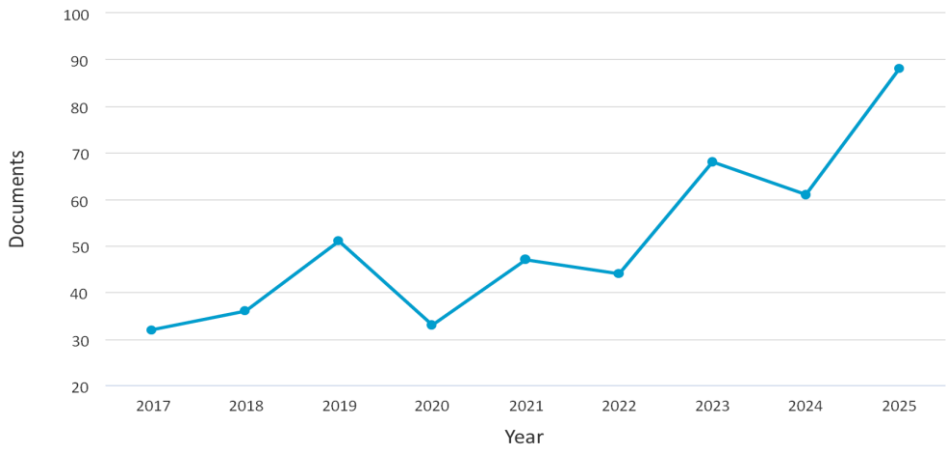
JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Results and Analysis

This section discusses the key patterns identified in the bibliometric analysis. The findings reveal a structured research landscape, with a central cluster representing the most influential and well-established studies. This core emphasizes the role of human behavior, organizational practices, and governance in cybersecurity. Smaller clusters indicate emerging and specialized research areas, reflecting the field's growing diversity. The presence of connections between clusters suggests increasing interdisciplinary integration. Variations in cluster size and density highlight different levels of maturity, with core areas being more developed than peripheral ones. The results show a shift toward more comprehensive and socio-organizational approaches to cybersecurity.

Figure 1 illustrates the initial search process, which identified 558 documents across the selected databases. This broad set of results reflects the extensive body of literature related to the research topic. To ensure the dataset's relevance and quality, specific inclusion criteria were applied. Only peer-reviewed journal publications were retained, excluding conference papers, book chapters, and other non-journal sources. In addition, the publication period was restricted to the years 2017 to 2025 in order to capture recent developments while ensuring coverage of complete calendar years. These filtering steps were necessary to refine the dataset and maintain consistency in the analysis. After applying these criteria, the final dataset comprised 460 journal articles, which served as the basis for subsequent bibliometric and content analyses in this study.

Figure 1. Citation analysis of cybersecurity



Citation Analysis

Table 2 shows that, from the 460 cited references, 52 met the threshold of at least 10 citations, with the top 10 documents emerging as the most influential in the field. Hou's study on blockchain in e-government leads with 226 citations, followed by works focusing on information security awareness and blockchain applications, highlighting the dominance of security and digital transformation themes. Notably, the top three papers account for more than half of the total citations, underscoring their foundational impact on the literature. Meanwhile, the remaining highly cited works reflect emerging areas such as artificial intelligence, machine learning, and digital inclusion. The findings reveal a concentration of influence in a few seminal works, alongside a diversity of perspectives that shape the evolving discourse on e-government and cybersecurity.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Table 2: Top 10 document Citation analysis

Rank	Author	Title	Citation
1.	Hou, Heng	The application of blockchain technology in e-government in China	226
2.	Khando, Khando	Enhancing employees' information security awareness in private and public organizations: A systematic literature review	179
3.	Alketbi, Ahmed	Blockchain for government services—Use cases, security benefits, and challenges	172
4.	Warkentin, Merrill	Using the security triad to assess blockchain technology in public sector applications	147
5.	Elisa, Noe	A framework for a blockchain-based, secure, and privacy-preserving e-government system	106
6.	Rawindaran, Nisha	Machine learning cybersecurity adoption in small and medium enterprises in developed countries	71
7.	Nikander, Jussi	Requirements for cybersecurity in agricultural communication networks	66
8.	Alharbi, Nawaf	The impact of security and its antecedents on the intention to use e-government services	60
9.	Djatmiko, Gatot Hery	Digital transformation and social inclusion in public services: A qualitative analysis of e-government adoption for marginalized communities in sustainable governance	53
10.	Al-Besher, Abdulaziz	Use of artificial intelligence to enhance e-government services	52

Table 3 shows that a search of the Scopus database yielded 293 sources that met the threshold, of which 5 met the minimum requirement of 11 documents. The compilation of the top 10 sources indicates a growing demand for cybersecurity research. Although this research area began to gain attention in 2017, the number of relevant publications has increased significantly since then. As shown in Table 3, both the number of published articles and citation counts from 2017 to 2025 exhibit a clear upward trend, reflecting growing interest and development of cybersecurity research within the academic community.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Table 3: Top 10 sources Citation analysis

Rank	Publications	Documents
1	acm international conference proceeding series	63
2	ceur workshop proceedings	18
3	communications in computer and information science	33
4	european conference on information warfare and security, eccws	9
5	information and computer security	107
6	international journal of advanced computer science and applications	71
7	lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)	26
8	lecture notes in networks and systems	21
9	procedia computer science	15
10	proceedings of the annual hawaii international conference on system sciences	18

Table 4 shows that the top 10 author citation analysis was conducted from a total of 1,198 authors, of which only three met the minimum threshold of 28 documents. The network analysis highlights the leading authors based on citation counts and their contributions to the field. The results indicate that Gao Shang recorded the highest number of citations with 188, followed by Martin Karlsson with 46 citations. Meanwhile, Annika Andreasson recorded 11 citations, representing the lowest count among those included in the top 10 but still demonstrating notable scholarly impact. The citation distribution presented in Table 4 reflects a concentration of influence among a few key authors, while still acknowledging the contributions of other researchers within the network.

Table 4: Top 10 authors' citation analysis

ID	Author	Document	Citations
1	gao, shang	3	188
2	karlsson, martin	3	46
3	baskerville, richard	3	29
4	fleron, benedicte	3	29
5	pries-heje, jan	3	29

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

6	ioannidis, sotiris	3	20
7	alghenaim, mohammed fahad	3	18
8	jonathan, gideon mekonnen	4	15
9	bakar, nur azaliah abu	3	14
10	andreasson, annika	4	11

Table 5 shows the analysis of publication counts by country, where out of 88 countries, only 12 met the minimum threshold of 10 documents. The top 10 countries emerge as the most significant contributors to the field. China leads with 24 documents and 482 citations, followed by the United Kingdom and Saudi Arabia, both demonstrating high citation impact despite having fewer documents compared to India and Indonesia. Malaysia and the United States also exhibit strong research productivity, while Jordan and Ukraine contribute smaller yet notable shares. The findings presented in Table 5 highlight China's dominance in citation impact, alongside the high publication output of India and Indonesia. The distribution further reflects balanced contributions from both Western and Asian countries, indicating a diverse and globally engaged research landscape in cybersecurity within government and public sector systems.

Table 5: Top 10 countries Citation analysis

Rank	Country	Documents	Citations
1	china	24	482
2	india	32	226
3	indonesia	35	165
4	jordan	12	68
5	malaysia	38	151
6	saudi arabia	19	338
7	sweden	25	330
8	ukraine	16	58
9	united kingdom	33	449
10	united states	34	309

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Co-citation Analysis

Table 6 shows the results of the co-citation analysis conducted as a bibliometric method to map the intellectual structure of the research field by examining how frequently two documents are cited together in subsequent studies. Using a citation threshold of 90, only three references met the minimum requirement out of 13,912 cited references. The results identify the top ten co-cited references, which share the same citation sources and exhibit equal total link strength. This pattern indicates a strong conceptual linkage among these works, suggesting that they are frequently used together to support related arguments or frameworks within the literature. The findings presented in Table 6 emphasize the presence of closely connected foundational studies that contribute to the core knowledge base of the field.

Table 6: Top 10 documents with the highest co-citation and total link strength

Documents	Citation	Total link strength
Khatib, R., & Barki, H. (2022). How different rewards tend to influence employee non-compliance with information security policies. *Information & Computer Security*, *30*(1), 97-116.	3	34
Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM*, *63*(12), 64-80.	3	34
Álvarez-García, D., Núñez, J. C., González-Castro, P., Rodríguez, C., & Cerezo, R. (2019). The effect of parental control on cyber-victimization in adolescence: The mediating role of impulsivity and high-risk behaviors. *Frontiers in psychology*, *10*, 1159.	3	34
Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT professional*, *12*(1), 24-31.	3	34
Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.	3	34
Perez, J. O., Cohen-Jarvie, D., & Drew, D. (2021). ICT and women's careers: Using grassroots ICT to expand women's participation in nontraditional careers. In *Technology and Women's Empowerment* (pp. 134-150). Routledge.	3	34
Heimer, K. (1996). Gender, interaction, and delinquency: Testing a theory of differential social control. *Social psychology quarterly*, 39-61.	3	34
Krishnan, S., Teo, T. S., & Lymm, J. (2017). Determinants of electronic participation and electronic government maturity: Insights from cross-country data. *International Journal of Information Management*, *37*(4), 297-312.	3	34
Gujarati, D. N. (2021). *Essentials of econometrics*. Sage Publications.	3	34
Hagan, J., Gillis, A. R., & Simpson, J. (1985). The class structure of gender and delinquency: Toward a power-control theory of common delinquent behavior. *American journal of sociology*, *90*(6), 1151-1178.	3	34

Source: Author interpretation based on VOSviewer analysis

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Figure 2 presents the co-citation network of cybersecurity research in government and public sector systems. This type of analysis shows how frequently different scholarly works are cited together, allowing us to identify the intellectual structure and major research streams in the field. The visualization reveals several clusters, each representing a group of closely related studies that share common themes, theories, or research interests. These clusters indicate that cybersecurity research is not a single unified topic but a multidisciplinary field composed of interconnected domains.

Figure 2: Co-citation analysis of cybersecurity

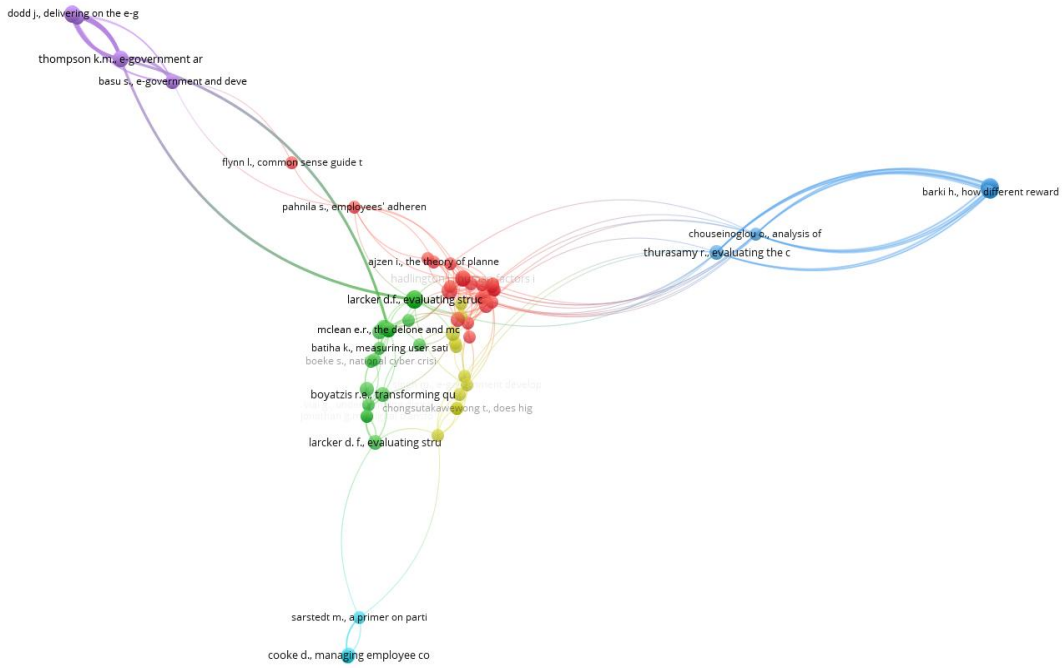


Table 7 presents the co-citation clusters that illustrate the intellectual structure of cybersecurity research in governance and public-sector contexts. The clustering results reveal interconnected themes derived from frequently co-cited references, showing how key studies are grouped based on shared conceptual relationships. As shown in Table 7, the variation in cluster sizes reflects different levels of research concentration, with larger clusters indicating more established areas and smaller clusters representing more specialized or emerging topics. The presence of multiple clusters highlights the multidisciplinary nature of cybersecurity research, incorporating perspectives from governance, organizational behavior, information systems, and risk management. The representative publications in each cluster demonstrate the enduring influence of foundational works that continue to shape current research directions. Differences in citation patterns and link strengths further suggest that some areas are more developed, while others continue to evolve. As illustrated in Table 7, these findings indicate a structured yet dynamic body of knowledge that supports cybersecurity research in digital government and public-sector systems.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Cluster 1 (Red) Human Behavior and Institutional Factors in Cybersecurity and Digital Governance has 22 publications. The interaction between human behavior, organizational practices, and governance structures in shaping cybersecurity awareness and digital governance initiatives is the primary focus of this cluster. Foundational sociological studies provide early theoretical insights into behavioral patterns associated with risk and rule compliance. For instance, Hagan et al. (1985) introduced the power-control theory to explain gender differences in delinquent behavior, while Heimer (1996) examined how social control and gender interact to influence deviant behavior. These perspectives have been widely applied to understand behavioral tendencies in digital environments, including cybersecurity risk and policy compliance. Several publications emphasize the role of individual awareness and behavioral factors in ensuring information security compliance. Bulgurcu et al. (2010) highlighted the importance of rational beliefs and awareness in influencing employees' adherence to information security policies. Similarly, Khatib and Barki (2022) explored how organizational reward systems may influence employee behavior, sometimes encouraging non-compliance with security policies. Research by Maasberg et al. (2020) further examined psychological traits associated with insider threats, particularly those related to the dark triad. Complementing these perspectives, Öğütçü et al. (2016) analyzed personal information security behavior and awareness, emphasizing that user-level practices remain critical in preventing security breaches. Another important theme within this cluster concerns gender participation and diversity in technology and cybersecurity fields. Studies such as Bagchi-Sen et al. (2010) examined the challenges and opportunities women face in cybersecurity careers, while Hoogendoorn et al. (2013) demonstrated that gender diversity can positively influence team performance and innovation within organizations. The cluster also highlights research on digital governance and institutional readiness. Several publications examine the development and implementation of e-government initiatives, particularly in developing countries (Basu, 2004; Ndou, 2004; Jaeger & Thompson, 2003). These studies emphasize that successful digital governance requires not only technological infrastructure but also effective policies, organizational readiness, and active public participation.

Cluster 2 (green) Human Factors, Security Policy Compliance, and Digital Transformation in Organizations contains 16 publications and is labeled "Human Factors, Security Policy Compliance, and Digital Transformation in Organizations." This cluster primarily focuses on the role of human behavior, organizational culture, and theoretical frameworks in shaping information security compliance and digital transformation initiatives. The literature highlights that cybersecurity is not solely a technological issue but also a behavioral and organizational challenge. Early studies emphasized the importance of psychological and motivational factors in influencing employees' compliance with information security policies. For example, Herath and Rao (2009) introduced a framework integrating protection motivation and deterrence theories to explain why employees comply with organizational security policies. Similarly, D'Arcy et al. (2009) demonstrated that awareness of security countermeasures can reduce information systems misuse by strengthening deterrence mechanisms within organizations. Several publications in this cluster further explore how organizational culture and leadership influence security behavior. Hu et al. (2012) emphasized the critical role of top management support and organizational culture in ensuring employee compliance with security policies. Complementing this perspective, Lebek et al. (2014) provided a comprehensive theory-based literature review on information security awareness and behavior, highlighting that security awareness programs are essential for promoting responsible user behavior in organizations. Human behavioral factors also play a significant role in cybersecurity risk, as demonstrated by Hadlington (2017), who examined how impulsivity, internet addiction, and attitudes toward cybersecurity contribute to risky online behavior. The cluster also includes methodological contributions and analytical approaches used in cybersecurity and information systems research. For instance, Braun and Clarke (2006) and Boyatzis (1998) discussed thematic analysis techniques widely applied in qualitative research, while Fornell and Larcker (1981) introduced methods for evaluating structural equation models in empirical studies. Several publications address the broader context of digital transformation and e-government adoption. Vial (2021) reviewed the concept of digital transformation and its research agenda, while Zheng et al. (2013) examined

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

institutional and organizational factors influencing e-government adoption. Jonathan (2020) further identified critical success factors in digital transformation initiatives within the public sector.

Cluster 3 (blue) Information Systems Governance, Security Policy Compliance, and E-Government Service Adoption contains 13 publications. The publications in this cluster focus on theoretical frameworks and organizational strategies that support information systems governance, security policy compliance, and the adoption of e-government services. Much of the literature emphasizes how organizational alignment, governance structures, and behavioral theories influence the success of digital initiatives. For instance, Luftman et al. (2017) highlighted the importance of aligning information technology with business strategies to improve organizational performance. Similarly, Posthumus and Von Solms (2004) proposed a governance framework for information security that integrates organizational policies, management structures, and technological safeguards to ensure effective security management. Behavioral and theoretical perspectives also play a critical role in understanding security policy compliance and technology adoption. Ajzen (1991) introduced the Theory of Planned Behavior, which has been widely applied to explain how attitudes, subjective norms, and perceived behavioral control influence individual intentions and actions. Building on behavioral perspectives, Siponen and Vance (2010) examined how employees justify violations of information security policies through neutralization techniques, while Siponen et al. (2014) explored factors that influence employees' adherence to organizational security policies. The cluster also includes studies related to the adoption and evaluation of e-government services. Carter and Bélanger (2005) examined the role of citizen trust, innovation, and acceptance factors in determining the utilization of e-government services. Similarly, Alawneh et al. (2013) analyzed user satisfaction with e-government services, highlighting the importance of service quality and usability in public sector digital initiatives. Zhao et al. (2015) further explored the reciprocal relationship between e-government development and the digital economy, demonstrating how digital governance can stimulate economic growth and technological advancement. In addition, methodological and analytical approaches are represented in this cluster. Sarstedt et al. (2021) discussed the use of partial least squares structural equation modeling for analyzing complex relationships in information systems research. Together, these publications highlight the importance of governance frameworks, behavioral theories, and analytical methods in supporting secure and effective digital government and information systems initiatives.

Cluster 4 (yellow) Information Security Compliance and E-Government Governance contains 11 publications, the studies in this cluster primarily examine the behavioral, organizational, and governance factors that influence information security policy compliance and the development of secure e-government systems. A significant portion of the literature focuses on how employees' attitudes and organizational environments shape compliance with security policies. For example, Safa et al. (2016) proposed an information security policy compliance model that highlights the influence of organizational commitment, awareness, and social pressures in promoting secure employee behavior. Similarly, Safa et al. (2015) explored the formation of information security conscious care behavior in organizations, emphasizing that employee awareness, training, and organizational culture play crucial roles in strengthening security practices. Another theme within this cluster involves the measurement and analysis of employee compliance with information security policies. Karlsson et al. (2017) examined the importance of value pluralism in understanding employee compliance behavior, suggesting that different employee values and motivations may influence adherence to organizational security rules. Complementing these behavioral perspectives, Donalds and Osei-Bryson (2020) analyzed how individual decision styles and psychological factors affect cybersecurity compliance behavior in organizational contexts. The cluster also highlights research related to governance and security challenges in e-government systems. Bélanger and Carter (2008) emphasized the role of trust and perceived risk in influencing citizens' adoption of e-government services. Similarly, Twizeyimana and Andersson (2019) reviewed the concept of public value in e-government initiatives, highlighting the importance of transparency, efficiency, and citizen engagement. In

addition, Zhao and Zhao (2010) assessed security vulnerabilities in state e-government websites, demonstrating the need for stronger security mechanisms in digital public services. Thompson et al. (2020) further examined whether higher levels of e-government adoption necessarily lead to stronger cybersecurity, highlighting the importance of governance and policy frameworks. Methodological contributions are also represented in this cluster. Walsham (1995) discussed interpretive case study methods in information systems research, while Hair et al. (2019) provided guidance on the use of PLS-SEM in empirical research. The cluster emphasizes integrating behavioral, organizational, and governance perspectives to address cybersecurity and e-government challenges.

Cluster 5 (Purple) Information Security Management and Digital Governance in Organizational and Government Contexts has 9 publications. The integration of information security practices with digital governance and organizational management is the primary focus of this cluster. Several studies emphasize the importance of understanding end-user behavior and organizational culture in maintaining effective cybersecurity practices. For instance, Stanton et al. (2005) examined end-user security behaviors, highlighting that employees play a crucial role in protecting organizational information systems. Similarly, Hu et al. (2012) emphasized the importance of top management support and organizational culture in ensuring compliance with information security policies. Another key theme in this cluster is the need for comprehensive and holistic approaches to information security management. Soomro et al. (2016) argued that organizations must adopt integrated strategies that combine technological, managerial, and behavioral aspects to effectively manage information security risks. In addition, research on digital transformation has highlighted how public institutions adapt to technological change. Mergel et al. (2019) explored how digital transformation is defined and implemented in government organizations, emphasizing the evolving nature of public-sector digitalization. Several publications also focus on the role of information and communication technologies (ICTs) in strengthening governance, transparency, and public services. Bertot et al. (2010) demonstrated how e-government and social media can enhance transparency and reduce corruption by promoting open government initiatives. Similarly, Wu (2014) examined the protection of personal data in e-government systems through a cross-country analysis, emphasizing the need for robust data protection policies. Complementing these perspectives, Glyptis et al. (2020) explored the challenges faced by project managers during e-government implementation, particularly in small countries where institutional capacity and resources may be limited. Methodological contributions also appear within this cluster. Cronbach (1951) introduced the widely used coefficient alpha for measuring reliability in research instruments, while Oates et al. (2022) provided guidance on research methods in information systems and computing. The publications in this cluster highlight the importance of organizational management, governance frameworks, and methodological rigor in supporting secure and effective digital transformation initiatives.

Cluster 6 (Cyan) Cybersecurity Threats, Insider Risk Management, and E-Government Governance Frameworks has 5 publications; the focus of this cluster centers on understanding cybersecurity threats, governance mechanisms, and strategic responses in both organizational and public-sector environments. A key theme among these publications is the identification and analysis of cybersecurity vulnerabilities and threat landscapes. Aslan et al. (2023) provided a comprehensive review of cybersecurity vulnerabilities, threats, and attack mechanisms, highlighting the evolving complexity of cyber threats and the need for proactive security solutions. Such analyses contribute to the development of more robust defensive strategies and inform organizations about emerging risks in digital environments. Another important aspect addressed in this cluster involves insider threats and risk mitigation strategies. Silowash et al. (2012) developed practical guidelines for mitigating insider threats, emphasizing that internal actors remain one of the most significant sources of cybersecurity incidents. Their work highlights the importance of monitoring systems, organizational policies, and employee awareness in reducing insider-related vulnerabilities. These perspectives reinforce the notion that cybersecurity risks are not solely technological but also involve human and organizational factors. The cluster also highlights governance and policy frameworks that guide the implementation of information systems and

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

cybersecurity strategies in the public sector. Cordella and Iannacci (2010) introduced the e-government enactment framework, which explains how institutional, organizational, and technological factors interact in implementing digital government initiatives. Similarly, Pandey and Gupta (2017) examined challenges in government-to-government (G2G) e-government projects using stakeholder theory, demonstrating how conflicting stakeholder interests can hinder project progress. Cybersecurity governance at the national level is also discussed within this cluster. Boeke (2018) analyzed different approaches to national cyber crisis management across European countries, highlighting variations in governance structures, policy responses, and coordination mechanisms. Collectively, the publications in this cluster emphasize the importance of integrating cybersecurity threat analysis, insider risk management, and governance frameworks to effectively address security challenges in modern digital systems.

Table 7: Co-citation clusters on Cybersecurity

Cluster	Citations	Count	Representative publications
1 (red)	Human Behavior and Institutional Factors in Cybersecurity and Digital Governance	22	Hagan et al. (1985); Heimer (1996); Bulgurcu et al. (2010); Khatib and Barki (2022); Maasberg et al. (2020); Öğütçü et al. (2016); Bagchi-Sen et al. (2010); Hoogendoorn et al. (2013); Basu (2004); Ndou (2004); Jaeger & Thompson (2003).
2 (Green)	Human Factors, Security Policy Compliance, and Digital Transformation in Organizations	16	Herath & Rao (2009); D'Arcy et al. (2009); Hu et al. (2012); Lebek et al. (2014); Hadlington (2017); Braun & Clarke (2006); Boyatzis (1998); Fornell & Larcker (1981); Vial (2021); Zheng et al. (2013); Jonathan (2020).
3 (Blue)	Information Systems Governance, Security Policy Compliance, and E-Government Service Adoption	13	Luftman et al. (2017); Posthumus & Von Solms (2004); Ajzen (1991); Siponen & Vance (2010); Siponen et al. (2014); Carter & Bélanger (2005); Alawneh et al. (2013); Zhao et al. (2015); Sarstedt et al. (2021).
4 (yellow)	Information Security Compliance and E-Government Governance	11	Safa et al. (2016); Safa et al. (2015); Karlsson et al. (2017); Donalds & Osei-Bryson (2020); Bélanger & Carter (2008); Twizeyimana & Andersson (2019); Zhao & Zhao (2010); Thompson et al. (2020); Walsham (1995); Hair et al. (2019).
5 (violet)	Information Security Management and Digital Governance in Organizational and Government Contexts	9	Stanton et al. (2005); Hu et al. (2012); Soomro et al. (2016); Mergel et al. (2019); Bertot et al. (2010); Wu (2014); Glyptis et al. (2020); Cronbach (1951); Oates et al. (2022).
6 (Cyan)	Cybersecurity Threats, Insider Risk Management, and E-Government Governance Frameworks	5S	Aslan et al. (2023); Silowash et al. (2012); Cordella & Iannacci (2010); Pandey & Gupta (2017); Boeke (2018).

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Co-word Analysis

Table 8 shows that out of 2,884 keywords in the co-word analysis, applying a co-occurrence threshold of 9 resulted in a total of 62 cited occurrences. The top fifteen keywords are identified based on co-occurrence frequency and total link strength. The most frequently occurring keyword is cybersecurity, with 130 occurrences and a total link strength of 110, highlighting that the field's primary focus is on protecting digital systems, networks, and information from threats. Closely related is e-government, which recorded 102 occurrences and a total link strength of 79, indicating that much of the research centers on the digital transformation of public services and the integration of cybersecurity safeguards into online government platforms. The total link strength values presented in Table 8 demonstrate that these topics are not only frequent but also highly interconnected, suggesting a multidisciplinary and integrated approach to cybersecurity research in government and public services.

Table 8: Top 15 keywords in the co-occurrence of keywords analysis

Rank	Keyword	Occurrences	Total link strength
1.	cybersecurity	130	110
2.	e-government	102	79
3.	information security	72	50
4.	public sector	33	34
5.	artificial intelligence	18	26
6.	blockchain	16	22
7.	digital transformation	24	22
8.	security	14	16
9.	privacy	12	15
10.	government	9	13
11.	cloud computing	10	11
12.	machine learning	10	10
13.	big data	7	9
14.	risk management	8	8
15.	cybercrime	7	7

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Figure 3: Co-word analysis of Cybersecurity

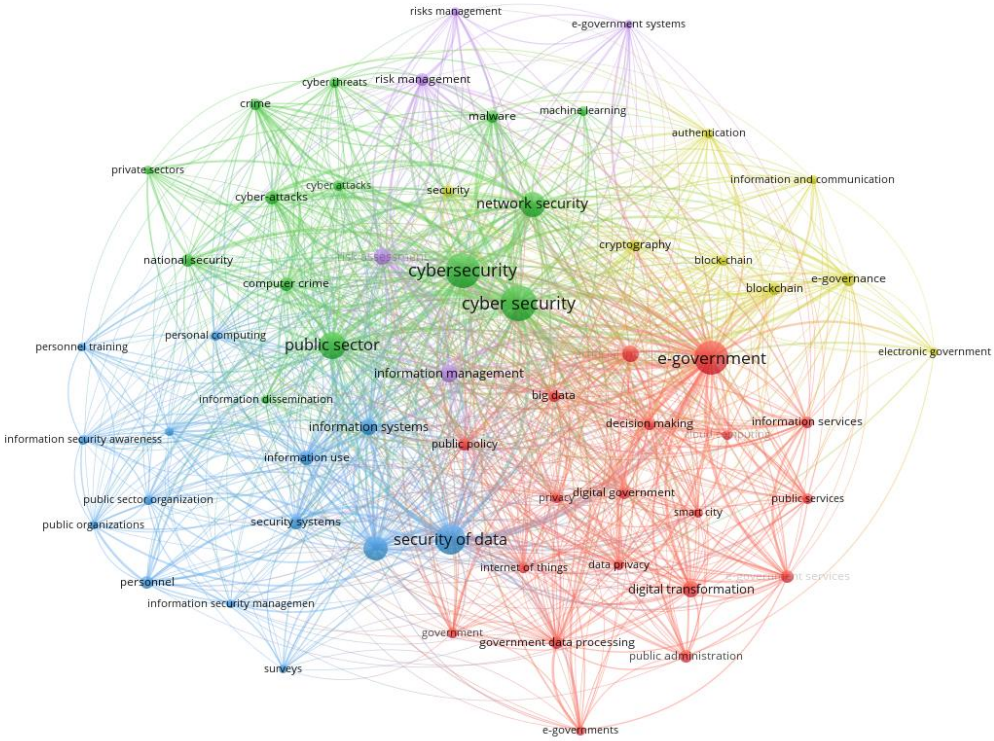


Table 9 presents the results of the co-word analysis, highlighting the major thematic clusters that characterize cybersecurity research in digital governance and public-sector contexts. By examining keyword co-occurrence, this analysis identifies key research areas and emerging trends, revealing how topics are conceptually related in the literature. As shown in Table 9, the clusters reflect the multidimensional nature of cybersecurity, encompassing technological innovations, governance frameworks, and organizational practices.

Cluster 1 (Red) Intelligent Cybersecurity Technologies and Data-Driven Security Systems includes the keywords artificial intelligence, big data, cloud computing, and machine learning, which represent the technological foundations supporting modern cybersecurity infrastructures. These emerging technologies enable more advanced and automated approaches to detecting and responding to cyber threats. For instance, Vial (2021) emphasized that digital transformation is largely driven by the adoption of advanced digital technologies that reshape organizational processes and capabilities. In contrast, Luftman et al. (2017) focused on the importance of aligning information technology strategies with organizational goals to maximize the value of technological innovation. While Vial (2021) highlights the transformative potential of emerging technologies in reshaping digital systems, Luftman et al. (2017) emphasize the strategic alignment required to successfully integrate these technologies within organizations. Together, these perspectives suggest that technologies such as artificial intelligence, big data analytics, and cloud computing not only enhance cybersecurity capabilities but also contribute to broader organizational digital transformation.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Cluster 2 (Green) Information Security Governance in Digital Government Services consists of the keywords e-government, information security, and risk management, which focus on protecting digital public services and managing cybersecurity risks in government information systems. The literature in this cluster highlights the importance of governance frameworks and institutional strategies for ensuring the security of digital government platforms. Posthumus and Von Solms (2004) proposed a comprehensive governance framework for information security, emphasizing that effective security management requires integrating policies, organizational structures, and technological safeguards. Similarly, Soomro et al. (2016) argued that information security management must adopt a holistic approach that combines technological, managerial, and behavioral components. While Posthumus and Von Solms (2004) primarily emphasize governance structures and policy frameworks, Soomro et al. (2016) focus on the broader integration of security management practices across organizational levels. Together, these studies underline that effective risk management in e-government systems requires coordinated governance mechanisms and comprehensive security strategies.

Cluster 3 (Blue) Digital Government Transformation and Public Sector Innovation contains the keywords digital transformation, government, and public sector, emphasizing how digital technologies are reshaping public administration and service delivery. Research in this cluster highlights that digital transformation initiatives are central to improving efficiency, transparency, and citizen engagement in government services. For example, Zhao et al. (2015) examined the relationship between e-government development and the digital economy, suggesting that digital government initiatives can stimulate broader economic and technological growth. In comparison, Zheng et al. (2013) focused on the organizational and institutional factors influencing the adoption of e-government systems in public administration. While Zhao et al. (2015) emphasize the broader socio-economic impact of digital government development, Zheng et al. (2013) highlight the internal organizational readiness required for successful adoption. These complementary perspectives demonstrate that digital transformation in the public sector depends on both institutional capacity and the wider digital ecosystem that supports government innovation.

Cluster 4 (Yellow) Blockchain-Based Privacy and Secure Data Infrastructure includes the keywords blockchain, privacy, and security, highlighting emerging technological solutions aimed at enhancing the protection of digital government systems. Research within this cluster emphasizes the role of advanced technologies in ensuring secure data management and protecting sensitive government information. For example, studies on e-government adoption emphasize that trust and perceived risk play a critical role in citizens' willingness to use digital government platforms (Bélanger & Carter, 2008). Their findings suggest that strong privacy protection and reliable security mechanisms are essential for building trust in digital public services. Similarly, Safa et al. (2016) highlighted the importance of information security policy compliance within organizations, arguing that effective cybersecurity requires both technological safeguards and institutional policies that guide secure behavior. While Bélanger and Carter (2008) focus on citizen trust and adoption of secure e-government systems, Safa et al. (2016) emphasize organizational compliance and internal security practices. Together, these studies illustrate that technological innovations such as blockchain and privacy-enhancing systems must be complemented by strong governance and security policies to ensure the protection of digital government infrastructures.

Cluster 5 (Purple) Cyber Threat Landscape and Organizational Cybersecurity Practices consists of the keywords cybercrime and cybersecurity, representing the central research focus on cyber threats and organizational responses to security risks. Research in this cluster primarily examines how institutions and individuals respond to cybersecurity challenges. For instance, Hu et al. (2012) investigated how organizational management and policy enforcement influence employee compliance with information security policies. Their findings highlight the critical role of leadership support, monitoring mechanisms, and security awareness

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

programs in strengthening cybersecurity practices. In comparison, Stanton et al. (2005) focused on the role of end-user behavior in maintaining information security, emphasizing that individual actions and awareness significantly influence the effectiveness of security systems. While Hu et al. (2012) emphasize organizational and managerial factors, Stanton et al. (2005) highlight individual user behavior as a key determinant of cybersecurity effectiveness. Together, these studies demonstrate that addressing cybercrime requires both institutional governance and responsible user behavior to ensure comprehensive protection against cyber threats.

Table 9: Co-word analysis on Cybersecurity

Cluster No and colour	Words	Number of keywords	Representative Keywords
1 (red)	Intelligent Cybersecurity Technologies and Data-Driven Security Systems	19	artificial intelligence, cloud computing, machine learning, big data
2 (green)	Information Security Governance in Digital Government Services	14	e-government, information security, risk management
3 (blue)	Digital Government Transformation and Public Sector Innovation	14	public sector, digital transformation, government
4 (yellow)	Blockchain-Based Privacy and Secure Data Infrastructure	8	blockchain, security, privacy
5 (violet)	Cyber Threat Landscape and Organizational Cybersecurity Practices	5	cybersecurity, cybercrime

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Discussion

The results of this bibliometric analysis provide a comprehensive overview of the evolving research landscape on cybersecurity in government and public-sector systems. The findings indicate a growing body of literature that reflects the increasing importance of cybersecurity as governments continue to adopt digital technologies and implement e-government services. The analysis of keyword co-occurrence reveals several interconnected thematic clusters that highlight the multidimensional nature of cybersecurity research in the public sector. One of the dominant themes identified is the integration of emerging technologies, such as artificial intelligence, machine learning, big data, and cloud computing, into cybersecurity frameworks. These technologies are increasingly being explored as mechanisms to strengthen threat detection, improve data analysis, and enhance system protection in government infrastructure. The growing emphasis on digital technologies aligns with broader trends in public-sector digital transformation, where governments aim to improve efficiency, transparency, and service delivery through advanced technological solutions (Mergel et al., 2019; Vial, 2021).

Another significant cluster focuses on governance-related themes, including e-government, information security, and risk management. This finding highlights that cybersecurity challenges in government systems extend beyond technical solutions and require institutional policies, regulatory frameworks, and strategic management approaches. Previous studies emphasize that effective cybersecurity implementation in public organizations requires strong governance structures, security policies, and compliance mechanisms to ensure adherence to security standards (Siponen et al., 2014; Safa et al., 2016). The analysis also reveals the growing importance of human and organizational factors in cybersecurity research. Concepts such as security awareness, behavioral compliance, and organizational culture frequently appear in the literature, indicating that employees play a critical role in maintaining institutional information security. Prior research demonstrates that employee compliance with security policies is strongly influenced by awareness programs, organizational culture, and management support (Hu et al., 2012; Bulgurcu et al., 2010).

Furthermore, themes such as privacy, blockchain, and cybercrime reflect increasing concerns regarding data protection and digital trust in government platforms. As governments expand digital services, protecting citizens' personal information and ensuring secure digital interactions have become essential components of modern public administration (Bélanger & Carter, 2008; Twizeyimana & Andersson, 2019). The findings suggest that cybersecurity research in government systems is becoming increasingly interdisciplinary, integrating technological innovation, governance frameworks, and human behavioral considerations.

Implications

The findings of this bibliometric analysis provide several important implications for research, policy development, and government practice. The results highlight the need for governments to prioritize cybersecurity as a fundamental component of digital transformation initiatives. As public sector institutions increasingly rely on digital infrastructure and online service delivery, security strategies must be integrated into the design and implementation of e-government systems to protect sensitive information and ensure the continuity of public services.

The study also emphasizes the importance of adopting a holistic cybersecurity approach that combines technological solutions with organizational governance and human behavioral considerations. Emerging technologies such as artificial intelligence and machine learning offer promising tools for detecting cyber threats; however, effective cybersecurity management also depends on strong institutional policies, risk management frameworks, and security awareness programs within organizations (Safa et al., 2015).

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

Another implication highlights the importance of strengthening information security awareness and training initiatives among employees. Human error and non-compliance with security policies remain major contributors to cybersecurity vulnerabilities in organizations. Continuous training programs and awareness campaigns can support responsible cybersecurity practices among public sector personnel (Herath & Rao, 2009; Donalds & Osei-Bryson, 2020).

This study also contributes to the literature by mapping the intellectual structure and thematic development of cybersecurity research in government systems. The bibliometric insights may guide future research by identifying emerging topics, research gaps, and opportunities for interdisciplinary collaboration in cybersecurity and digital government studies.

Conclusion and Limitations

This study presents a bibliometric analysis of cybersecurity research in government and public sector systems, emphasizing the increasing need to secure digital infrastructures as e-government adoption expands. By examining 460 journal articles from the Scopus database published between 2017 and 2025, the study maps the intellectual structure, key contributors, and major thematic trends in the field. The use of citation, co-citation, and co-word analyses enables the identification of influential publications, leading scholars, and emerging research areas related to cybersecurity in digital governance.

The findings indicate a clear growth in scholarly attention, reflecting the urgency of protecting government information systems and sensitive citizen data. The results also reveal that cybersecurity research in the public sector is multidisciplinary, incorporating technological, organizational, and human dimensions. Key themes include the application of advanced technologies such as artificial intelligence, blockchain, big data, and cloud computing, alongside issues of governance, risk management, policy compliance, and user awareness. These insights highlight the importance of integrating technical innovation with institutional frameworks and behavioral factors to strengthen cybersecurity practices.

Despite these contributions, the study has limitations. It relies solely on Scopus-indexed journal articles, which may exclude relevant studies from other databases. The selected timeframe may also overlook earlier foundational work or recent unpublished research. Furthermore, bibliometric methods depend on citation data, which may not fully capture the qualitative impact or practical relevance of individual studies. The accuracy of the findings is also influenced by database indexing and metadata quality. Future research can address these limitations by incorporating multiple data sources, extending the timeframe, and integrating qualitative approaches to provide a more comprehensive understanding of cybersecurity in government systems.

Recommendations

Based on the findings of the bibliometric analysis, it is recommended that governments adopt comprehensive, integrated cybersecurity frameworks that combine technological solutions, organizational practices, and governance mechanisms to effectively secure digital public-sector systems. Cybersecurity should be embedded in broader digital transformation strategies to protect information systems and ensure the continuity of e-government services. Additionally, public sector institutions must prioritize continuous cybersecurity awareness and training programs, as human factors remain a major source of vulnerability; strengthening employee knowledge, behavior, and compliance with security policies can significantly reduce cyber risks.

Furthermore, governments are encouraged to leverage emerging technologies such as artificial intelligence, machine learning, blockchain, and cloud computing to enhance threat detection, automate security processes, and improve data protection capabilities. Alongside technological advancements, the development and enforcement of robust cybersecurity governance frameworks, policies, and regulatory standards are essential to ensure coordinated and consistent security practices across agencies. Future research should also promote interdisciplinary collaboration and expand methodological approaches by incorporating multiple data sources and qualitative analyses to provide deeper insights into cybersecurity challenges in government systems. Finally, prioritizing data privacy and strengthening citizen trust through transparent and secure handling of information are critical for the successful adoption and sustainability of digital government service.

Declarations

Ethics Declaration

Ethics Declaration: not applicable.

This study is a bibliometric analysis based exclusively on secondary data retrieved from publicly available scientific databases. It does not involve human participants, animals, or any form of intervention requiring ethical approval.

Consent to Publish Declaration

Consent to Publish Declaration: not applicable.

Consent to Participate Declaration

Consent to Participate Declaration: not applicable.

Funding

This research received no external funding.

Data Availability Statement

Not applicable. This study is a bibliometric analysis based exclusively on secondary data retrieved from publicly available scientific databases.

Acknowledgements

The authors express their gratitude to their colleagues and academic mentors who provided valuable insights into bibliometric research and software development education. Special thanks are extended to institutional staff and collaborators for their support during data collection and manuscript preparation.

Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
Advancing Knowledge. Inspiring Innovation. Achieving the SDGs.
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 3 Pages 489-517

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alawneh, A., Al-Refai, H., & Batiha, K. (2013). Measuring user satisfaction from e-government services: Lessons from Jordan. *Government Information Quarterly, 30*(3), 277–288. https://doi.org/10.1016/j.giq.2013.03.001

Al-Besher, A., & Kumar, K. (2022). *Use of artificial intelligence to enhance e-government services*. *Measurement: Sensors, 24*, 100484. https://doi.org/10.1016/j.measen.2022.100484

Alharbi, N., Papadaki, M., & Dowland, P. (2017). The impact of security and its antecedents on users' intention to use e-government services. *Procedia Computer Science, 113*, 644–651. https://doi.org/10.1016/j.procs.2017.08.329

Alketbi, A., Nasir, Q., & Talib, M. A. (2018). Blockchain for government services—Use cases, security benefits and challenges. In *2018 15th Learning and Technology Conference (L&T)* (pp. 112–119). IEEE. https://doi.org/10.1109/LT.2018.8368494

Álvarez-García, D., Núñez, J. C., González-Castro, P., Rodríguez, C., & Cerezo, R. (2019). The effect of parental control on cyber-victimization in adolescence: The mediating role of impulsivity and high-risk behaviors. *Frontiers in Psychology, 10*, Article 1159. https://doi.org/10.3389/fpsyg.2019.01159

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333

Baas, J., Schotten, M., Plume, A., Côté, G., & Karimi, R. (2020). Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies. *Quantitative Science Studies, 1*(1), 377–386. https://doi.org/10.1162/qss_a_00030

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT Professional, 12*(1), 24–31. https://doi.org/10.1109/MITP.2010.39

Basu, S. (2004). E-government and developing countries: An overview. *International Review of Law, Computers & Technology, 18*(1), 109–132. https://doi.org/10.1080/13600860410001674779

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165–176. https://doi.org/10.1016/j.jsis.2007.12.002

Beretas, C. (2024). Information systems security, detection and recovery from cyber attacks. *Universal Library of Engineering Technology, 1*(1). https://ulopenaccess.com/ulpages/fulltextUlete?PublishID=ULETE20240101_005

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly, 27*(3), 264–271. https://doi.org/10.1016/j.giq.2010.03.001

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance, 31*(3), 449–464. https://doi.org/10.1111/gove.12307

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Sage. https://books.google.com/books?id=_rfClWRhIKAC

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5–25. https://doi.org/10.1111/j.1365-2575.2005.00183.x

Cordella, A., & Iannacci, F. (2010). Information systems in the public sector: The e-government enactment framework. *Journal of Strategic Information Systems, 19*(1), 52–66. https://doi.org/10.1016/j.jsis.2010.01.001

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297–334. https://doi.org/10.1007/BF02310555

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse. *Information Systems Research, 20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior. *International Journal of Information Management, 51*, 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

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

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Gujarati, D. N. (2021). *Essentials of econometrics*. Sage Publications. https://books.google.com/books?id=2CI_EAAAQBAJ

Hadlington, L. (2017). Human factors in cybersecurity. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hagan, J., Gillis, A. R., & Simpson, J. (1985). The class structure of gender and delinquency. *American Journal of Sociology, 90*(6), 1151–1178. https://doi.org/10.1086/228208

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Heimer, K. (1996). Gender, interaction, and delinquency. *Social Psychology Quarterly, 59*(1), 39–61. https://doi.org/10.2307/2787118

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hoogendoorn, S., Oosterbeek, H., & Van Praag, M. (2013). The impact of gender diversity on the performance of business teams: Evidence from a field experiment. *Management Science, 59*(7), 1514–1528. https://doi.org/10.1287/mnsc.1120.1674

Hou, H. (2017). The application of blockchain technology in e-government in China. *Computer Law & Security Review, 33*(3), 351–358. https://doi.org/10.1016/j.clsr.2017.03.016

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies. *Decision Sciences, 43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Jaeger, P. T., & Thompson, K. M. (2003). E-government around the world: Lessons, challenges, and future directions. *Government Information Quarterly, 20*(4), 389–394. https://doi.org/10.1016/j.giq.2003.08.001

Jonathan, G. M. (2020). Digital transformation in the public sector: Identifying critical success factors. In A. Anttiroiko & A.-V. Anttiroiko (Eds.), *Information systems: 16th European, Mediterranean, and Middle Eastern conference, EMCIS 2019* (pp. 223–235). Springer. https://doi.org/10.1007/978-3-030-44322-1_18

Karlsson, F., Karlsson, M., & Åström, J. (2017). Measuring employees' compliance. *Information & Computer Security, 25*(3), 279–299. https://doi.org/10.1108/ICS-05-2016-0030

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Khatib, R., & Barki, H. (2022). Rewards and non-compliance with information security policies. *Information & Computer Security, 30*(1), 97–116. https://doi.org/10.1108/ICS-01-2021-0012

Kumar, M., George, R. J., & PS, A. (2023). Bibliometric analysis for medical research. Indian Journal of Psychological Medicine, 45(3), 277–282. https://journals.sagepub.com/doi/full/10.1177/02537176221103617

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior. *Management Research Review, 37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Luftman, J., Lyytinen, K., & Ben Zvi, T. (2017). Enhancing the measurement of information technology (IT) business alignment and its influence on company performance. *Journal of Information Technology, 32*(1), 26–46. https://doi.org/10.1057/jit.2015.23

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cybersecurity. *Communications of the ACM, 63*(12), 64–80. https://doi.org/10.1145/3427228

McAllister, J. T., Lennertz, L., & Atencio Mojica, Z. (2022). Mapping a discipline: A guide to using VOSviewer for bibliometric and visual analysis. *Science & Technology Libraries, 41*(3), 319–348. https://doi.org/10.1080/0194262X.2021.1998645

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation. *Government Information Quarterly, 36*(4), 101385. https://doi.org/10.1016/j.giq.2019.06.002

Ndou, V. (2004). E-government for developing countries. *Electronic Journal of Information Systems in Developing Countries, 18*(1), 1–24. https://doi.org/10.1002/j.1681-4835.2004.tb00117.x

Nikander, J., Manninen, K., & Laajalahti, A. (2020). Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture, 179*, 105776. https://doi.org/10.1016/j.compag.2020.105776

Oates, B. J., Griffiths, M., & McLean, R. (2022). *Researching information systems and computing* (2nd ed.). Sage. https://sk.sagepub.com/book/mono/researching-information-systems-and-computing-2e

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Pandey, V., & Gupta, S. (2017). Understanding G2G e-government project impasse: A stakeholder theory perspective. *Information Development, 33*(5), 466–481. https://doi.org/10.1177/0266666916657582

Pessin, V. Z., Yamane, L. H., & Siman, R. R. (2022). Smart bibliometrics: An integrated method of science mapping and bibliometric analysis. *Scientometrics, 127*(6), 3695–3718. https://doi.org/10.1007/s11192-022-04406-6

Posthumus, S., & Von Solms, R. (2004). A framework for governance of information security. *Computers & Security, 23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2015). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications, 20*, 47–55. https://doi.org/10.1016/j.jisa.2014.10.001

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model. *Computers & Security, 56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.002

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial least squares structural equation modeling. In C. Homburg, M. Klarmann, & A. Vomberg (Eds.), *Handbook of market research* (pp. 587–632). Springer. https://doi.org/10.1007/978-3-319-57413-4_15

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J., Flynn, L., & White, J. (2012). *Common sense guide to mitigating insider threats* (4th ed.). Software Engineering Institute, Carnegie Mellon University. https://www.sei.cmu.edu/documents/1226/2012_005_001_34033.pdf

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502. https://doi.org/10.2307/25750688

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies. *Information & Management, 51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach. *International Journal of Information Management, 36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Thompson, N., Mullins, J., & Chatterjee, S. (2020). Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quarterly, 37*(2), 101408. https://doi.org/10.1016/j.giq.2019.101408

Twizeyimana, J. D., & Andersson, A. (2019). The public value of e-government. *Government Information Quarterly, 36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

Vial, G. (2021). Understanding digital transformation. *Journal of Strategic Information Systems*, 30(2). https://doi.org/10.1016/j.jsis.2021.101626

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems, 4*(2), 74–81. https://doi.org/10.1057/ejis.1995.9

Warkentin, M., & Orgeron, C. (2020). *Using the security triad to assess blockchain technology in public sector applications*. *International Journal of Information Management, 52*, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Wu, Y. (2014). Protecting personal data in e-government. *Government Information Quarterly, 31*(1), 150–159. https://doi.org/10.1016/j.giq.2013.07.003

Zhao, F., Wallis, J., & Singh, M. (2015). E-government development and the digital economy. *Internet Research, 25*(5), 734–766. https://doi.org/10.1108/IntR-02-2014-0055

Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly, 27*(1), 49–56. https://doi.org/10.1016/j.giq.2009.07.004

Zheng, D., Chen, J., Huang, L., & Zhang, C. (2013). E-government adoption in public administration organizations. *European Journal of Information Systems, 22*(2), 221–234. https://doi.org/10.1057/ejis.2012.40