PERSEPSI: Communication Journal e-ISSN 2623-2669
Vol. 9, No. 1, 2026, 36-52
DOI: https://doi.org/10.30596/persepsi.v9i1.29815

Exploring Cybersecurity Issues in Social Media: Evidence from Bibliometric Analysis

Gusti Naufal Rizky Perdana[1]*, Bambang Irawan[2], Cathas Teguh Prakoso[3], Yaen Miftakhul Laily[4]
[1,2,3]Public Administration Study Program, Universitas Mulawarman, Indonesia
[4]Public Administration Study Program, Universitas Jember, Indonesia
[*1]*Correspondence Author: gustinaufalrp@fisip.unmul.ac.id*

Abstract

The growth of social media has created significant opportunities while also intensifying cybersecurity challenges such as data privacy risks, misinformation, and user behavior manipulation. This study maps the landscape of social media cybersecurity research from 2004 to 2025 by analyzing publication trends, research collaborations, and dominant thematic clusters. A bibliometric approach was applied to Scopus-indexed publications using VOSviewer and Biblioshiny to examine keyword co-occurrence, institutional networks, and geographic distributions. The findings reveal a shift from purely technical security approaches toward socio-technical perspectives integrating user behavior, artificial intelligence, and machine learning. Six major research clusters were identified, covering AI-based analytics, data protection, trust and transparency, cyber threats, technology policy, and healthcare applications. These results provide insights for strengthening cybersecurity strategies in the global social media ecosystem.

Keywords: cybersecurity, social media, data privacy, social cybersecurity, Bibliometric Analysis

INTRODUCTION

Over the past decade, the global communication landscape has undergone a profound transformation driven by the rapid expansion of social media (Jarman et al., 2021). The integration of social media into daily life reached unprecedented levels during the COVID-19 pandemic, which triggered a surge in digital device usage and internet accessibility (Bozzola et al., 2022; Armutcu et al., 2023). This phenomenon has significantly altered human paradigms of accessing, interacting with, and consuming information (Shanmugasundaram & Tamilarasu, 2023). As an ecosystem of internet- and mobile-based applications, social media enables individuals to both produce and distribute content autonomously (user-generated content) (Cataldo et al., 2021). Its core characteristics—providing instantaneous and continuous access to information—position social media as a fundamental technology shaping the dynamics of the modern world (Alodat et al., 2023; McCarthy et al., 2023). Beyond mere communication tools, social media platforms offer spaces for individuals to express ideas and cultivate intellectual interests through dynamic information exchange (Aggarwal et al., 2022; Vrontis et al., 2022). Nevertheless, widespread usage often occurs without users' awareness of the long-term impacts of their digital activities (Polanco-Levicán & Salvo-Garrido, 2022).

Although social media platforms have become established channels for information dissemination and public opinion expression (Perdana et al., 2023), their proliferation entails significant dual consequences. On one hand, increased social media engagement raises concerns regarding users' psychological well-being (Ostic et al., 2021); on the other hand, these platforms have become catalysts for the spread of misinformation and conspiracy theories (Enders et al., 2023). This situation is exacerbated by low digital literacy, with many users remaining unaware of the importance of privacy protection and account security in both online and offline interactions (Chang et al., 2023). Within the electronic participation ecosystem, cybersecurity serves as a critical instrument for safeguarding system sustainability through personal data protection and the mitigation of fraud and false information (Ahangama, 2023). While advancements in instant messaging and social media technologies enable more efficient data exchange, they inherently introduce new threat vectors that compromise data integrity and facilitate information misuse (Alharbi & Tassaddiq, 2021). Fundamentally, humans remain the most vulnerable point in the cybersecurity chain amid these technological complexities (Alrobaian et al., 2023). Given that cyber threats now encompass physical infrastructure, information systems networks, and sensitive social media data (Zeng, 2022), large-scale security breaches have unsurprisingly become a central concern in global media discourse (Jerman Blažič & Jerman Blažič, 2022).

Previous research on social media cybersecurity spans a wide spectrum, from individual behavioral aspects to organizational frameworks. Tran et al. (2023) highlighted that user engagement on digital platforms influences their security compliance attitudes, though gaps persist between protective intentions and actual behaviors. To address vulnerabilities at the institutional level, Ben Salamah et al. (2023) emphasized the need for formalized risk management via adaptive training frameworks to align security policies with employees' specific requirements. This focus on human and organizational factors demonstrates that cybersecurity effectiveness heavily relies on user literacy and preparedness to confront evolving risks.

Simultaneously, research developments have targeted technical threat mitigation and more complex information governance. Singhal et al. (2023) revealed that social media can serve as a vector for technological misinformation, undermining threat intelligence systems, while Belli et al. (2023) examined regulatory efforts across countries to establish responsible platform governance. Complementing these approaches, Alrabea et al. (2024) underscored the crucial role of artificial intelligence and machine learning algorithms in detecting dynamic patterns of cyberattacks on social networks. Overall, the current research body demonstrates a convergence between behavioral awareness, regulatory policy, and technological innovation in securing social media ecosystems. Additionally, studies on cybersecurity within the context of digital government indicate a significant upward trend in research output over the years (Perwitasari et al., 2025).

Despite numerous studies exploring social media cybersecurity from behavioral, technical, and policy perspectives separately, literature providing a holistic view of the field's evolution and intellectual structure remains limited. Most prior studies are fragmented, focusing on specific cases or technologies, leaving gaps in understanding global research trends and future directions. This study aims to address these gaps by employing bibliometric analysis to map the landscape of social media cybersecurity research. Unlike conventional

literature reviews, this approach offers objectivity through the visualization of large-scale data, including geographic distribution, inter-institutional collaboration, and the identification of emerging and declining thematic clusters. Consequently, this chapter provides a unique, comprehensive roadmap to guide researchers and practitioners in identifying underexplored research areas.

Specifically, this study seeks to systematically deconstruct and map the intellectual landscape of social media cybersecurity through comprehensive bibliometric analysis. It aims to identify publication growth trajectories, map global researcher collaboration networks, and detect thematic evolution within the academic discourse. Furthermore, the study intends to uncover research voids and pinpoint critical emerging trends, such as the integration of artificial intelligence and ethical privacy challenges, thereby offering a more structured overview than existing narrative literature reviews.

Critically, this research delivers dual contributions to both knowledge development and professional practice. For academics, it serves as an intellectual navigation tool that validates the paradigm shift from purely technical approaches to more complex socio-technical perspectives, assisting new researchers in positioning their studies within the most relevant topics. From a practical standpoint, the chapter synthesizes macro-level data that can inform policymakers and cybersecurity practitioners, enabling them to understand dominant threat patterns and prioritize resource allocation toward the most vulnerable areas of the social media ecosystem. By providing a data-driven roadmap, this study effectively bridges the gap between academic theory and strategic needs in addressing asymmetric cyber threats in the digital era.

METHOD

This study employs a bibliometric analysis method to comprehensively map the research landscape of cybersecurity on social media. Bibliometric analysis was selected due to its widespread use and systematic approach for examining and analyzing large-scale scientific data (Donthu et al., 2021). The research procedure strictly follows the four-stage framework proposed by Öztürk et al. (2024) to ensure transparency and validity of the findings, which includes: (1) defining the research aim, (2) collecting data on relevant literature, (3) analyzing and visualizing the data, and (4) interpreting the findings and results (see Figure 1).

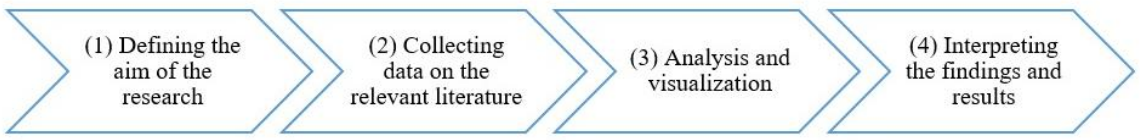

Figure 1. Stages of Bibliometric Analysis (Öztürk et al., 2024)

The first stage involves defining the aim of the research, which is to identify the intellectual structure, publication growth trends, and global thematic evolution concerning threats and data protection on social platforms. The second stage is data collection, conducted through the Scopus database. Scopus was chosen due to its reputation as a high-quality scientific database encompassing multidisciplinary literature in computer science and social sciences. A comprehensive search strategy was applied to titles, abstracts, and

keywords, combining terms related to social media, social networks, and online social networks with cybersecurity, information security, data privacy, cyberattacks, and cybercrime terminologies.

To ensure data quality and relevance, strict inclusion and exclusion criteria were applied. The search was limited to documents published between 2003 and 2025 to capture the evolution of research since the early popularity of social media. Document types were restricted to journal articles, conference proceedings, and book chapters to ensure that the analyzed data had undergone peer review. Additionally, only documents published in English were included to standardize linguistic analysis in science mapping. This procedure yielded 5,924 documents, which were exported in CSV format for subsequent processing.

The third stage is analysis and visualization, where the collected data were processed using VOSviewer and Biblioshiny (R-Package). Analytical techniques included performance analysis to evaluate contributions of authors, organizations, and countries, and science mapping through co-word analysis. Visualization was conducted using three main models: network visualization to examine relationships between topics, overlay visualization to observe temporal research developments, and density visualization to identify the most intensively studied research areas as well as potential future research opportunities. Finally, in the stage of interpreting the findings and results, all visualizations were critically analyzed to synthesize key findings and address the research questions, thereby providing a comprehensive overview of the current state of social media cybersecurity research.

RESULT AND DISCUSSION

Publication Trends in Social Media Cybersecurity Research

The analysis of annual publication trends demonstrates a significant increase in academic interest in social media cybersecurity between 2004 and 2025. In the early phase (2004–2008), the number of publications was very limited, reflecting the initial stage of social media development as an emerging online communication phenomenon that began to transform information-sharing patterns (H. Chen et al., 2004). As social media usage expanded within organizational and business contexts, researchers increasingly focused on issues of privacy protection and information access control (Carminati & Ferrari, 2008a). A surge in publications was observed from 2009, peaking between 2010 and 2011, coinciding with the rise of the digital society that demanded clearer policy frameworks to safeguard privacy, access rights, and user identity. During the 2012–2018 period, publication growth remained relatively stable, indicating that social media had increasingly been recognized as a critical infrastructure with multiple security vulnerabilities. Although slight fluctuations occurred between 2019 and 2021, research activity surged again from 2023, reaching a peak in 2024. This increase was driven by the acceleration of post-pandemic digital transformation and the emergence of increasingly complex and sophisticated cyber threats, which can no longer be effectively addressed through traditional security approaches, thereby prompting the need for more adaptive and innovative protection strategies (Aslan et al., 2023).

Overall, these trends reflect a shift in research focus from purely technical aspects toward a more holistic socio-technical approach, emphasizing user behavior and awareness as key elements in cybersecurity systems. Given the high volume of publications through 2025,

PERSEPSI: Communication Journal e-ISSN 2623-2669
Vol. 9, No. 1, 2026, 36-52
DOI: https://doi.org/10.30596/persepsi.v9i1.29815

it can be concluded that social media cybersecurity remains a strategic and highly relevant issue in navigating the evolving dynamics of digital ecosystems.

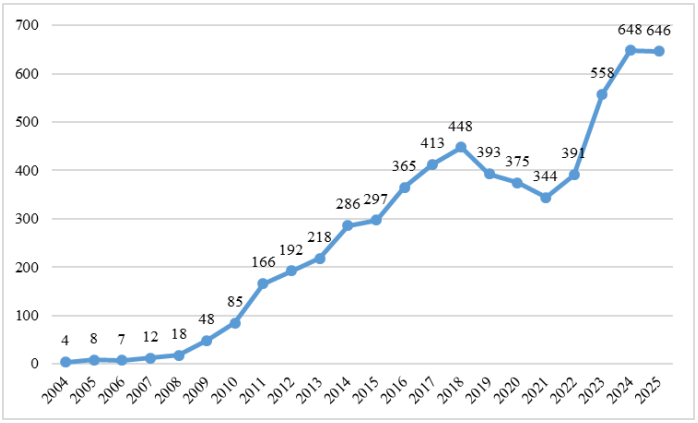

Figure 2. Research Trends in Social Media Cybersecurity (Scopus Database, 2026)

Leading Contributors: Key Authors, Affiliations, and Countries

The analysis of leading authors highlights several key figures who have played a pivotal role in shaping the research direction of social media cybersecurity (see Figure 3). Carley, K.M. emerges as the most productive author with 17 publications, underscoring their contribution to examining the relationship between social interactions and cyber risks. This aligns with Carley's conceptualization of social cybersecurity, which explains how socially and digitally connected individuals can be manipulated through online platforms (Carley, 2020). Following closely, Ferrari, E. has contributed 15 publications consistently addressing access control and privacy protection issues in web-based social networks, particularly within organizational and business contexts (Carminati & Ferrari, 2008b). Significant contributions are also made by Dang-Pham, D. and Yu, P.S. with 14 publications each, as well as Carminati, B. and Li, H. with 13 publications, positioning cybersecurity as a socio-technical issue involving human-technology interactions. Other authors, including Zhu, X., Imine, A., Pittayachawan, S., Such, J.M., and Yu, S., further reinforce this discourse. Overall, the dominance of these authors indicates that data protection, privacy, and user behavior remain central research themes, reflecting the growing complexity of cyber threats and the increasing demand for adaptive security strategies within the global digital ecosystem.

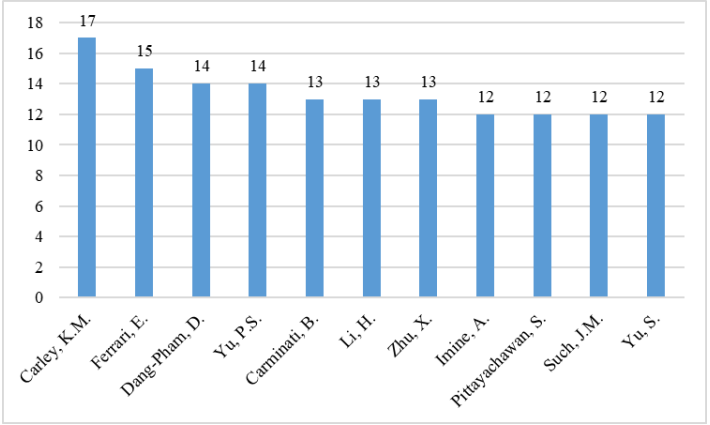

Figure 3. Top Authors in Social Media Cybersecurity Research (Scopus Database, 2026)

PERSEPSI: Communication Journal e-ISSN 2623-2669
Vol. 9, No. 1, 2026, 36-52
DOI: https://doi.org/10.30596/persepsi.v9i1.29815

The affiliation analysis indicates that social media cybersecurity research is predominantly led by higher education institutions and major research centers. Carnegie Mellon University emerges as the most productive institution with 52 publications, followed by the Chinese Academy of Sciences (49 publications) and Beijing University of Posts and Telecommunications (45 publications). This dominance reflects the central role of technology-based institutions in advancing cybersecurity research. Significant contributions are also observed from Xidian University (42 publications) and Shanghai Jiao Tong University (39 publications), which primarily focus on enhancing infrastructure and designing more secure systems. These findings suggest that technical aspects, such as system resilience and security architecture, remain a major concern in the literature. Meanwhile, the presence of Deakin University (37 publications), Tsinghua University, the Ministry of Education of the People's Republic of China (36 publications each), and Arizona State University (34 publications) underscores that cybersecurity has become a strategic agenda across nations. Overall, the distribution of affiliations indicates that addressing increasingly complex cyber threats requires strong research collaboration among leading technological centers globally.

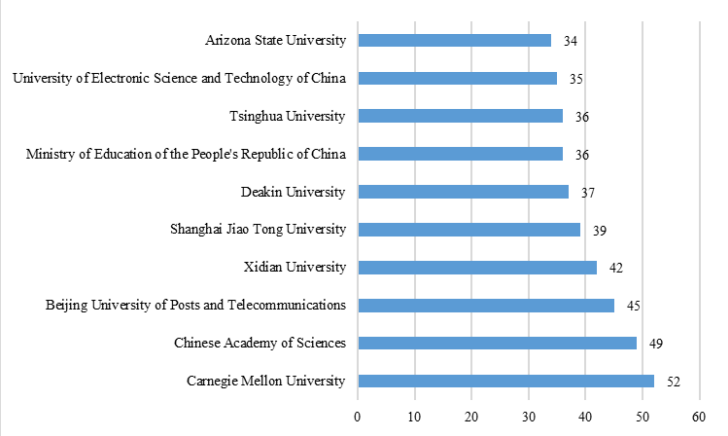

Figure 4. Top Affiliations in Social Media Cybersecurity Research (Scopus Database, 2026)

The analysis of geographical distribution reveals that social media cybersecurity research is dominated by countries with advanced technological ecosystems. The United States ranks first with 3,940 publications, reflecting sustained attention to issues of behavioral manipulation and security within socially embedded digital ecosystems. China follows with 3,378 publications, demonstrating strong research investment in developing secure system infrastructures to mitigate risks arising from technological complexity.

India ranks third with 2,712 publications, followed by the United Kingdom (820 publications) and Germany (670 publications), underscoring that cybersecurity has become a strategic priority across multiple regions. Significant contributions also come from Australia (641 publications), Italy (532 publications), and Canada (431 publications), which primarily focus on privacy and access control issues on social media platforms, particularly in organizational and business contexts. Completing the top ten contributors are Saudi Arabia and Spain, each with 378 publications, reflecting the global expansion of concern for cross-border cyber threats. Overall, this pattern indicates that social media cybersecurity research productivity is concentrated in countries with high technology adoption and an urgent need

for stronger, internationally coordinated data protection policies.

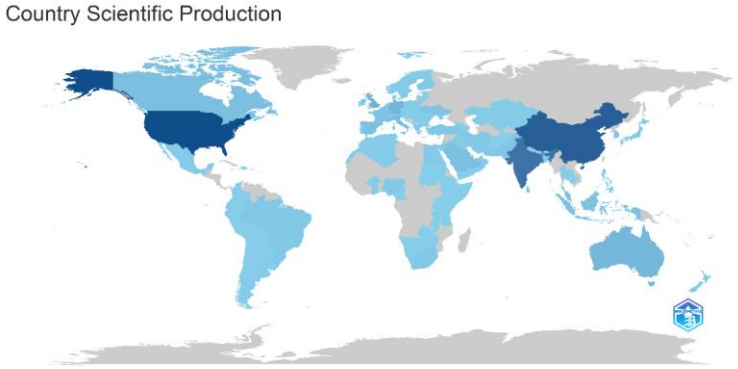

Figure 5. Countries with the Highest Output in Social Media Cybersecurity (Scopus Database, 2026)

Evolution of Research Themes and Trend Topics

The analysis of research topic trends from 2008 to 2024 demonstrates a progressive shift in academic focus, moving from basic technical approaches toward the integration of intelligent technologies within the context of social media and cybersecurity. In the early phase (2008–2012), research was dominated by the development of mathematical models and computer simulations to understand the emergence of Web 2.0 as a large-scale information exchange medium, where information technology—particularly social media—began to be recognized as a factor influencing the rationality and effectiveness of decision-making processes (Power & Phillips-Wren, 2011).

The subsequent period (2013–2018) marked a significant shift toward issues of personal data protection and access control mechanisms, driven by the increasing use of social networks for business purposes that required resource-sharing systems based on privacy-aware user relationships. During this stage, social media increasingly became recognized as critical infrastructure with complex technical and social vulnerabilities, necessitating systematic network security enhancements through the application of cryptography and stringent access controls to ensure that data could only be accessed by authorized entities (Lee & Wu, 2017).

Between 2019 and 2022, research paradigms shifted toward socio-technical approaches, placing human behavior at the center of cybersecurity defense, giving rise to the concept of social cybersecurity aimed at protecting the e-society from information manipulation and risky content-sharing practices that could undermine public trust. In this context, cybersecurity was no longer viewed solely as a technical issue but also closely linked to ethics, morality, and user responsibility in managing access, information security, and digital interactions (Wildauer & Silva, 2013).

The peak of this evolution occurred in 2023–2024, when research focused on the use of machine learning, large language models (LLMs), and predictive analytics as responses to next-generation cyber threats that are increasingly automated and sophisticated. Overall, this evolution underscores that social media cybersecurity research dynamically adapts to the complexities of the global digital ecosystem, with LLMs seen as having the potential to enhance defense through threat modeling, anomaly detection, and adaptive attack simulations

PERSEPSI: Communication Journal e-ISSN 2623-2669
Vol. 9, No. 1, 2026, 36-52
DOI: https://doi.org/10.30596/persepsi.v9i1.29815

to improve risk mitigation and system resilience against continuously evolving threats (Sarker, 2024).

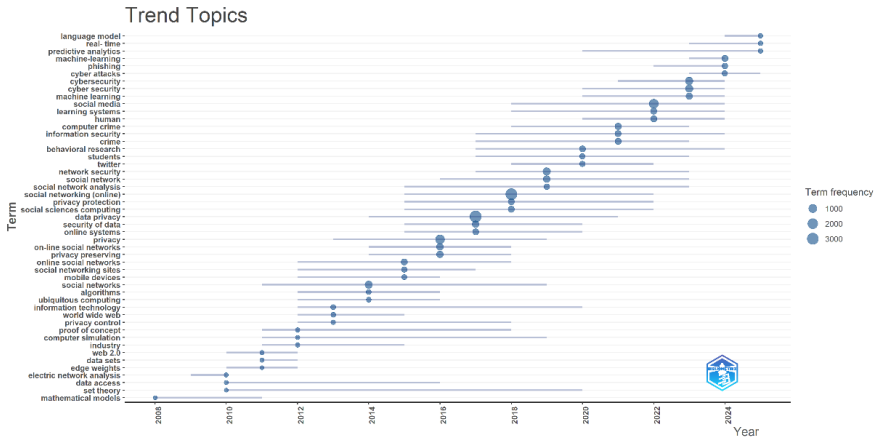

Figure 6. Evolution of Research Themes and Trending Topics in Social Media Cybersecurity (Scopus Database, 2026)

Co-occurrence Network Analysis: Mapping Intellectual Structure

The co-occurrence network analysis of keywords is a critical bibliometric method for mapping the intellectual structure and identifying interconnections among major topics in the social media cybersecurity literature. By analyzing frequently co-occurring keywords, this study identifies dominant knowledge domains and emerging trends. Based on the mapping results, the literature is broadly fragmented into six main clusters, reflecting distinct research focuses while maintaining systemic interconnections, ranging from artificial intelligence and data privacy to social cybersecurity policy. This mapping provides a visual representation of how core terms such as "privacy," "security," and "machine learning" function as central nodes connecting various more specific research subtopics across the globe.

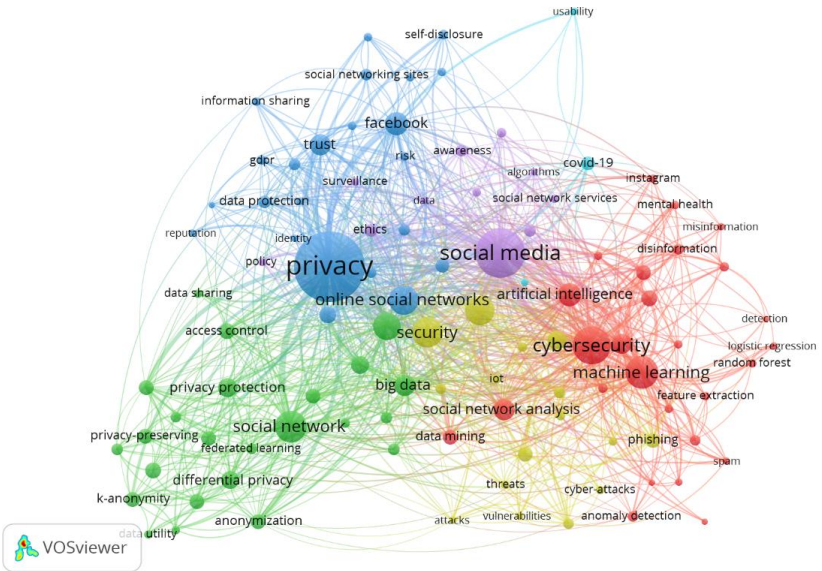

Figure 7. Network Analysis in Social Media Cybersecurity (Processed by the author using VosViewer, 2026)

PERSEPSI: Communication Journal e-ISSN 2623-2669
Vol. 9, No. 1, 2026, 36-52
DOI: https://doi.org/10.30596/persepsi.v9i1.29815

To provide a more detailed understanding of the specific composition of each research cluster, the data below summarizes the keywords constituting each cluster. This classification is based on the overall interconnections among terms within the literature database, enabling a comprehensive view of the depth and scope of each research domain.

Table 1. Keyword Clusters in Social Media Cybersecurity

Cluster	Item	Total
Cluster 1 (Red)	Anomaly detection; artificial intelligence; classification; cyber threat intelligence; cyberbullying cybersecurity; data mining; detection; disinformation; fake news; feature extraction; Instagram; logistic refression; machine learning; mental health; misinformation; natural language process; neural networks; open source intelligence; random forest; social media analytics; social network analysis; spam; text classification; text mining; topic modeling; twitter	27
Cluster 2 (Green)	Access control; anonymity; anonymization;big data; cloud computing; cryptogrphy; data privacy; data publishing; data security; data sharing; data utility; differential privacy; encryption; federated learnig; homomorphic encryption; k-anonymity; location privacy; mobile social networks; online social network; privacy preservation; privacy preserving; privacy protection; privacy-preserving; social network	24
Cluster 3 (Blue)	Authentication; blockchain; communication; data protection; facebook; ggdpr; identity; information disclosure; information sharing; online social networks; personal data; personal information; privacy; privacy concerns; privacy paradox; reputation; risk; self-dislourse; social network sites; social networking; social networking sites; transparency; trust	23
Cluster 4 (Yellow)	Attacks; cyber attacks; cyber crime; cyber threts; cyber-attacks; cybercrime; digital forensics; information security; internet of thigs; iot; malware; phising; secuiry; social engineering; threats; vulnerabilities	16
Cluster 5 (Purple)	Algorithms; awareness; data; education; ethics; internet; policy; social media; social network services; surveillance; technology; techologi	11
Cluster 6 (Light Blue)	Covif-19; healthcare; usability	3

Source: (Processed by the author using VosViewer, 2026)

Keyword and cluster analysis using VOSviewer reveals that the literature on social media cybersecurity is segmented into several principal thematic foci. Each cluster reflects a distinct research domain, ranging from technical security measures to privacy, user trust, and sector-specific applications, particularly in healthcare. The detailed discussion per cluster is

as follows:

Cluster 1 (Red) – AI-Based Cybersecurity and Social Media Analytics

This largest cluster, comprising 27 items, focuses on the integration of intelligent technologies to counter contemporary digital threats. Research emphasizes the use of machine learning, artificial intelligence, and anomaly detection to map interaction patterns on popular platforms such as Twitter and Instagram, enabling automated detection of cyber risks such as misinformation, fake news, and risky behaviors that compromise information integrity. Beyond technical aspects, this cluster explores psychological dimensions by analyzing the impact of social media usage on mental health, employing natural language processing (NLP) and neural networks for sentiment classification and cyberbullying detection. AI thus functions not only as a defensive tool but also as an analytical instrument to understand complex social and human behavioral phenomena in digital ecosystems. Consequently, AI and NLP applications across multilingual social media data can support national cyber threat indices and anomaly detection, fostering strategic decision-making for enhanced cyber preparedness, while adversarially informed AI-based approaches provide adaptive, automated, and resilient security systems (Sufi, 2023; Sarker, 2023).

Cluster 2 (Green) – Privacy and Data Protection in Social Networks

Comprising 24 items, this cluster emphasizes the development of technical infrastructures to ensure large-scale data privacy and security. Topics such as encryption, access control, and anonymity are fundamental in protecting information confidentiality amidst widespread mobile social network adoption. Advanced data protection technologies, including differential privacy and federated learning, are investigated to mitigate data leakage in cloud-based systems, alongside challenges in managing big data and implementing robust privacy policies. The primary aim is to balance data utility with strict personal data protection, granting users full control over sensitive information while complying with legal standards (Bonneau & Preibusch, 2010; Di Minin et al., 2021).

Cluster 3 (Blue) – Trust, Identity, and Transparency in Social Media

With 23 items, this cluster examines the sociological aspects of cybersecurity, particularly how trust is established and maintained in online interactions. Key topics include authentication, identity management, and blockchain applications to ensure information transparency and reliability. Studies explore the privacy paradox, reputation risks, and regulatory frameworks such as GDPR to enhance platform accountability. By integrating technical and behavioral dimensions, this cluster advocates for a transparent digital ecosystem where digital identity management is central to mitigating trust and reputational risks (Feher, 2015; Galpin & Flowerday, 2011).

Cluster 4 (Yellow) – Cyber Threats and Digital Attacks

Comprising 16 items, this cluster analyzes the anatomy of digital attacks and defense strategies, focusing on malware, phishing, and targeted attacks on IoT infrastructures. Social engineering exploiting human psychological vulnerabilities is highlighted, alongside the importance of digital forensics and early threat detection. This domain underlines the need for adaptive mitigation tools to strengthen information system resilience, especially in the context of smart cities and e-government implementation (Wirtz & Weyerer, 2017; Demertzi et al., 2023).

Cluster 5 (Purple) – Algorithms, Awareness, and Social Media Policy

This cluster includes 11 items addressing the role of regulation, ethics, and education in digital technology use. It emphasizes how social media algorithms shape user behavior and how government policies can govern digital surveillance practices. Research highlights that effective security requires not only technology but also high user awareness, ethical platform use, and digital literacy education. Transparent, inclusive policies are crucial to safeguard digital rights within increasingly complex e-societies (de Groot et al., 2023; Eg et al., 2023).

Cluster 6 (Light Blue) – Social Media in the Healthcare Sector

The smallest cluster, with three items, focuses on social media adaptation in global health crises, particularly the COVID-19 pandemic. It examines the use of social media for health information management, dissemination of accurate medical information, and ensuring usability for broad public access. Data privacy of sensitive health records and security challenges in digital health adoption are emphasized, highlighting the transformative role of social media in patient empowerment, institutional reputation, and healthcare communication, while navigating legal, ethical, and systemic constraints (Andersen et al., 2012; Pentescu et al., 2015; Chaudhri et al., 2021).

Temporal Analysis and Emerging Frontiers (Overlay Visualization)

Temporal analysis through overlay visualization provides a dynamic perspective on the evolution of social media cybersecurity research over the past decade, distinguishing between established topics that form the foundational research base and emerging frontier areas dominating current academic discourse. In the early period (purple to blue, approximately 2016–2018), research focused on structural and fundamental aspects of digital platforms, with keywords such as "Facebook," "privacy," "access control," and "trust" reflecting attention to user privacy frameworks, identity management, and information protection, aligned with the growing adoption of social media for both recreational and business purposes (Adjei et al., 2020).

During the transitional phase (green, around 2019–2021), research emphasis shifted toward large-scale data processing and system resilience, where terms such as "big data," "social network analysis," "data mining," and "security" became dominant. Scholars explored advanced privacy-preserving techniques, including differential privacy and federated learning, to mitigate data leakage risks in increasingly complex digital ecosystems, while maintaining privacy and data security remained a critical challenge (C. Chen et al., 2025).

The latest frontier (yellow, 2022 onward) marks a new era driven by artificial intelligence, with keywords like "machine learning," "artificial intelligence," "cybersecurity," "deep learning," and "anomaly detection" indicating the urgent need for automated solutions to detect sophisticated threats such as misinformation, cyberbullying, and spam accounts in real time. The appearance of terms such as "COVID-19" and "healthcare" highlights how the pandemic accelerated cybersecurity research in the public health sector, emphasizing the balance between platform usability and strict protection of medical data, thereby integrating digital technologies into healthcare delivery to manage the COVID-19 crisis—the most significant public health emergency since the 1918 influenza pandemic (Wang et al., 2021). Overall, this temporal analysis demonstrates the adaptive nature of social media cybersecurity research in response to technological developments and global crises, with future studies expected to increasingly leverage large language models and predictive analytics to build

PERSEPSI: Communication Journal e-ISSN 2623-2669
Vol. 9, No. 1, 2026, 36-52
DOI: https://doi.org/10.30596/persepsi.v9i1.29815

more resilient ecosystems capable of countering information manipulation and next-generation cyber threats.

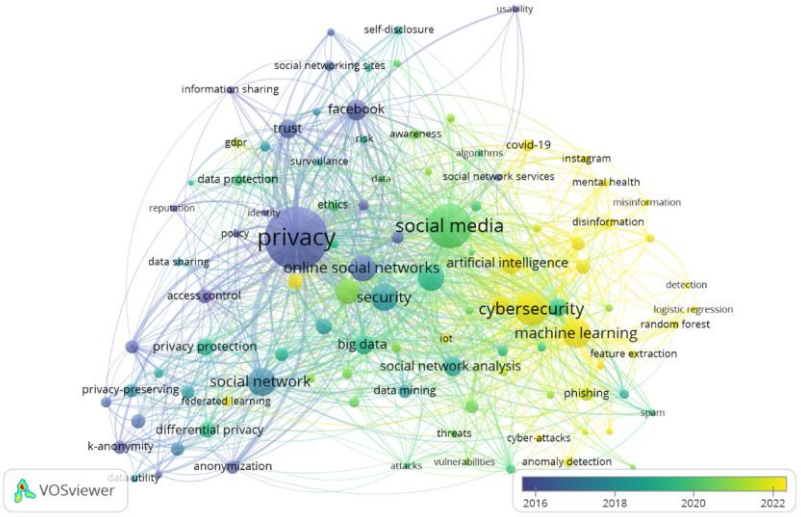

Figure 8. Overlay Analysis in Social Media Cybersecurity (Processed by the author using VosViewer, 2026)

Clustering and Research Intensity Analysis (Density Visualization)

Density visualization in bibliometric analysis aims to identify the most intensively researched areas and the main focal points within the scientific community, where the density map generated by VOSviewer represents research intensity through color brightness and label size. Bright yellow areas with large labels indicate highly concentrated publication activity, whereas darker areas represent topics that are less explored but remain connected within the intellectual network.

The analysis revealed three dominant research hubs in social media cybersecurity. The highest density was observed around the terms "Privacy" and "Social Media," highlighting that personal data protection and user privacy remain foundational in discussions of security on online social networks. Supporting topics such as "online social networks," "trust," and "access control" indicate that intensive research focuses on creating secure information-sharing mechanisms without compromising individual privacy, emphasizing that cybersecurity knowledge exchange can improve incident detection, prevention, and reduce duplication costs, while organizational concerns over privacy remain central when sharing data externally (Smith et al., 2012; Vakilinia et al., 2017).

The second hub is concentrated in the technical domain, including "Cybersecurity," "Machine Learning," and "Artificial Intelligence," reflecting a substantial shift toward data-driven security solutions. The integration of AI and ML enables automated threat detection, sentiment analysis, and mitigation of sophisticated attacks beyond traditional system capabilities (Mohamed, 2025). Medium-density areas such as "Security," "Big Data," and "Social Network Analysis" illustrate the use of large-scale data to map risks and understand attack structures on social media (Tsou, 2015). Peripheral topics like "COVID-19," "Healthcare," and "Ethics" represent emerging frontiers with fewer publications compared to privacy and AI. Overall, this density analysis confirms that the intellectual structure of social

PERSEPSI: Communication Journal e-ISSN 2623-2669
Vol. 9, No. 1, 2026, 36-52
DOI: https://doi.org/10.30596/persepsi.v9i1.29815

media cybersecurity relies on the synergy between privacy policies and advanced intelligent algorithms, with future research likely expanding the high-density areas through further integration of digital ethics and proactive automated security systems.

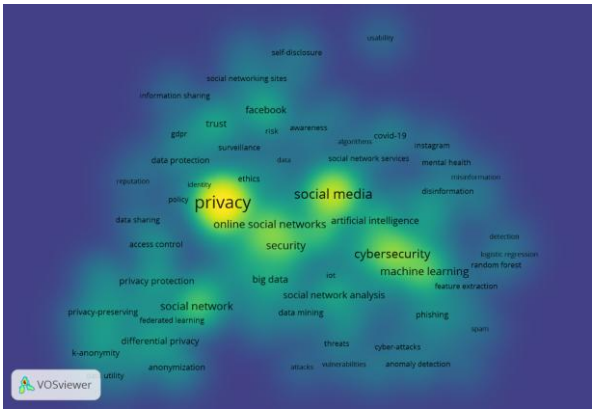

Figure 9. Density Analysis in Social Media Cybersecurity (Processed by the author using VosViewer, 2026)

CONCLUSION

Based on the bibliometric analysis, research on social media cybersecurity has shown significant development since 2004. Early studies primarily focused on technical aspects such as privacy and access control; over time, the focus has shifted toward socio-technical approaches that integrate user behavior, digital ethics, and intelligent technologies including machine learning, artificial intelligence, and Large Language Models (LLMs). The main research clusters encompass AI-based cybersecurity, data protection and privacy, trust and transparency, cyber threats, regulation and user awareness, and social media applications in the healthcare sector, highlighting that cybersecurity is a strategic issue requiring adaptive, collaborative, and proactive approaches.

However, this study has several limitations. The dataset was limited to specific literature sources and primarily relied on keyword and co-occurrence network analyses, leaving the qualitative context of individual studies underexplored. Differences in security practices at local and regional levels are also insufficiently addressed, limiting the generalizability of findings across diverse contexts. This underscores the need for more comprehensive research approaches, including the integration of empirical data and field studies to understand the dynamics of cybersecurity in various social and technical environments.

Future research should explore the integration of LLMs and predictive algorithms for real-time threat detection and mitigation, while emphasizing ethics, regulations, and user privacy rights. Cross-national and contextual studies could provide insights into diverse security practices and support the development of more effective, adaptive, and sustainable strategies. Ultimately, advancing social media cybersecurity research is expected to contribute to building a secure, transparent, and resilient digital ecosystem capable of countering emerging cyber threats.

REFERENCES

Adjei, J. K. et al. (2020). Digital Identity Management on Social Media: Exploring the

Factors That Influence Personal Information Disclosure on Social Media. In *Sustainability* (Vol. 12, Issue 23, p. 9994). https://doi.org/10.3390/su12239994

Aggarwal, K. et al. (2022). Role of social media in the COVID-19 pandemic: A literature review. *Data Mining Approaches for Big Data and Sentiment Analysis in Social Media*, 91–115.

Ahangama, S. (2023). Relating Social Media Diffusion, Education Level and Cybersecurity Protection Mechanisms to E-Participation Initiatives: Insights from a Cross-Country Analysis. *Information Systems Frontiers*, *25*(5), 1695–1711. https://doi.org/10.1007/s10796-023-10385-7

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. In *Big Data and Cognitive Computing* (Vol. 5, Issue 2, p. 23). https://doi.org/10.3390/bdcc5020023

Alodat, A. M. et al. (2023). Social Media Platforms and Political Participation: A Study of Jordanian Youth Engagement. In *Social Sciences* (Vol. 12, Issue 7, p. 402). https://doi.org/10.3390/socsci12070402

Alrabea, K. J. et al. (2024). Artificial intelligence and cybersecurity within a social media context: implications and insights for Kuwait. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-12-2023-0224

Alrobaian, S. et al. (2023). Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation. In *Big Data and Cognitive Computing* (Vol. 7, Issue 2, p. 73). https://doi.org/10.3390/bdcc7020073

Andersen, K. N. et al. (2012). Social media in public health care: Impact domain propositions. *Government Information Quarterly*, *29*(4), 462–469. https://doi.org/https://doi.org/10.1016/j.giq.2012.07.004

Armutcu, B. et al. (2023). Tourist behaviour: The role of digital marketing and social media. *Acta Psychologica*, *240*, 104025. https://doi.org/https://doi.org/10.1016/j.actpsy.2023.104025

Aslan, Ö. et al. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. In *Electronics* (Vol. 12, Issue 6, p. 1333). https://doi.org/10.3390/electronics12061333

Belli, L. et al. (2023). Online Content Regulation in the BRICS Countries: A Cybersecurity Approach to Responsible Social Media Platforms. *Luca Belli, Yasmin Curzi, Walter Gaspar. Responsible Behaviour in Cyberspace: Global Narratives and Practice. Brussels: Publication Office of the European Union.(2023)*.

Ben Salamah, F. et al. (2023). An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work. In *Applied Sciences* (Vol. 13, Issue 17, p. 9595). https://doi.org/10.3390/app13179595

Bonneau, J., & Preibusch, S. (2010). *The Privacy Jungle:On the Market for Data Protection in Social Networks BT - Economics of Information Security and Privacy* (T. Moore et al. (eds.); pp. 121–167). Springer US.

Bozzola, E. et al. (2022). The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks. In *International Journal of Environmental Research and Public Health* (Vol. 19, Issue 16, p. 9960). https://doi.org/10.3390/ijerph19169960

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and*

Mathematical Organization Theory, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Carminati, B., & Ferrari, E. (2008a). Access control and privacy in web-based social networks. *International Journal of Web Information Systems*, *4*(4), 395–415. https://doi.org/10.1108/17440080810919468

Carminati, B., & Ferrari, E. (2008b). *Privacy-Aware Collaborative Access Control in Web-Based Social Networks BT - Data and Applications Security XXII* (V. Atluri (ed.); pp. 81–96). Springer Berlin Heidelberg.

Cataldo, I. et al. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, *Volume 11-2020*. https://www.frontiersin.org/journals/psychiatry/articles/10.3389/fpsyt.2020.508595

Chang, V. et al. (2023). Cybersecurity for children: an investigation into the application of social media. *Enterprise Information Systems*, *17*(11), 2188122. https://doi.org/10.1080/17517575.2023.2188122

Chaudhri, V. et al. (2021). "CARE" in social media: perceptions of reputation in the healthcare sector. *Journal of Communication Management*, *25*(2), 125–141. https://doi.org/10.1108/JCOM-06-2020-0059

Chen, C. et al. (2025). Trustworthy federated learning: privacy, security, and beyond. *Knowledge and Information Systems*, *67*(3), 2321–2356. https://doi.org/10.1007/s10115-024-02285-2

Chen, H. et al. (2004). Crime data mining: a general framework and some examples. *Computer*, *37*(4), 50–56. https://doi.org/10.1109/MC.2004.1297301

de Groot, T. et al. (2023). Learning in and about a filtered universe: young people's awareness and control of algorithms in social media. *Learning, Media and Technology*, *48*(4), 701–713. https://doi.org/10.1080/17439884.2023.2253730

Demertzi, V. et al. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. In *Applied Sciences* (Vol. 13, Issue 2, p. 790). https://doi.org/10.3390/app13020790

Di Minin, E. et al. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation Biology*, *35*(2), 437–446. https://doi.org/https://doi.org/10.1111/cobi.13708

Donthu, N. et al. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*(March), 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Eg, R. et al. (2023). A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors. *Computers in Human Behavior Reports*, *9*, 100253. https://doi.org/https://doi.org/10.1016/j.chbr.2022.100253

Enders, A. M. et al. (2023). The Relationship Between Social Media Use and Beliefs in Conspiracy Theories and Misinformation. *Political Behavior*, *45*(2), 781–804. https://doi.org/10.1007/s11109-021-09734-6

Feher, K. (2015). Digital identity: The transparency of the self. In *Applied Psychology* (pp. 132–143). WORLD SCIENTIFIC. https://doi.org/doi:10.1142/9789814723398_0007

Galpin, R., & Flowerday, S. V. (2011). Online social networks: Enhancing user trust through effective controls and identity management. *2011 Information Security for South Africa*,

1–8. https://doi.org/10.1109/ISSA.2011.6027520

Jarman, Hannah K et al. (2021). Direct and indirect relationships between social media use and body satisfaction: A prospective study among adolescent boys and girls. *New Media & Society*, *26*(1), 292–312. https://doi.org/10.1177/14614448211058468

Jerman Blažič, B., & Jerman Blažič, A. (2022). Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. In *Sustainability* (Vol. 14, Issue 8, p. 4763). https://doi.org/10.3390/su14084763

Lee, N.-Y., & Wu, B.-H. (2017). Privacy Protection Technology and Access Control Mechanism for Medical Big Data. *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 424–429. https://doi.org/10.1109/IIAI-AAI.2017.34

McCarthy, S. et al. (2023). The dark side of digitalization and social media platform governance: a citizen engagement study. *Internet Research*, *33*(6), 2172–2204. https://doi.org/10.1108/INTR-03-2022-0142

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, *67*(8), 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

Ostic, D. et al. (2021). Effects of Social Media Use on Psychological Well-Being: A Mediated Model. *Frontiers in Psychology*, *Volume 12-2021*. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.678766

Öztürk, O. et al. (2024). How to design bibliometric research: an overview and a framework proposal. *Review of Managerial Science*, *18*(11), 3333–3361. https://doi.org/10.1007/s11846-024-00738-0

Pentescu, A. et al. (2015). Social Media's Impact on Healthcare Services. *Procedia Economics and Finance*, *27*, 646–651. https://doi.org/https://doi.org/10.1016/S2212-5671(15)01044-8

Perdana, G. N. R. et al. (2023). #PrayForKanjuruhan On Twitter: Public Response to the Kanjuruhan Stadium Disaster. *Nyimak Journal of Communication*, *7*(1), 89–107.

Perwitasari, D. R. et al. (2025). SECURING THE DIGITAL NATION: A RESEARCH EXPLORATION OF CYBERSECURITY IN E-GOVERNMENT. *GOVERNANCE: Jurnal Ilmiah Kajian Politik Lokal Dan Pembangunan*, *12*(1), 88–99.

Polanco-Levicán, K., & Salvo-Garrido, S. (2022). Understanding Social Media Literacy: A Systematic Review of the Concept and Its Competences. In *International Journal of Environmental Research and Public Health* (Vol. 19, Issue 14, p. 8807). https://doi.org/10.3390/ijerph19148807

Power, D. J., & Phillips-Wren, G. (2011). Impact of Social Media and Web 2.0 on Decision-Making. *Journal of Decision Systems*, *20*(3), 249–261. https://doi.org/10.3166/jds.20.249-261

Sarker, I. H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. *SECURITY AND PRIVACY*, *6*(5), e295. https://doi.org/https://doi.org/10.1002/spy2.295

Sarker, I. H. (2024). *Generative AI and Large Language Modeling in Cybersecurity BT - AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability* (I. H. Sarker (ed.); pp. 79–99). Springer Nature Switzerland.

https://doi.org/10.1007/978-3-031-54497-2_5

Shanmugasundaram, M., & Tamilarasu, A. (2023). The impact of digital technology, social media, and artificial intelligence on cognitive functions: a review. *Frontiers in Cognition*, *Volume 2-2023*. https://www.frontiersin.org/journals/cognition/articles/10.3389/fcogn.2023.1203077

Singhal, M. et al. (2023). Cybersecurity Misinformation Detection on Social Media: Case Studies on Phishing Reports and Zoom's Threat. *Proceedings of the International AAAI Conference on Web and Social Media*, *17*(1 SE-Full Papers), 796–807. https://doi.org/10.1609/icwsm.v17i1.22189

Smith, M. et al. (2012). Big data privacy issues in public social media. *2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, 1–6. https://doi.org/10.1109/DEST.2012.6227909

Sufi, F. (2023). A New Social Media-Driven Cyber Threat Intelligence. In *Electronics* (Vol. 12, Issue 5, p. 1242). https://doi.org/10.3390/electronics12051242

Tran, D. Van et al. (2023). Exploring the influence of government social media on cybersecurity compliance: employee attitudes, motivation and behaviors. *Journal of Asia Business Studies*, *18*(1), 204–223. https://doi.org/10.1108/JABS-09-2023-0343

Tsou, M.-H. (2015). Research challenges and opportunities in mapping social media and Big Data. *Cartography and Geographic Information Science*, *42*(sup1), 70–74. https://doi.org/10.1080/15230406.2015.1059251

Vakilinia, I. et al. (2017). Privacy-preserving cybersecurity information exchange mechanism. *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 1–7. https://doi.org/10.23919/SPECTS.2017.8046783

Vrontis, D. et al. (2022). Societal effects of social media in organizations: Reflective points deriving from a systematic literature review and a bibliometric meta-analysis. *European Management Journal*, *40*(2), 151–162. https://doi.org/https://doi.org/10.1016/j.emj.2022.01.007

Wang, Q. et al. (2021). Integrating Digital Technologies and Public Health to Fight Covid-19 Pandemic: Key Technologies, Applications, Challenges and Outlook of Digital Healthcare. In *International Journal of Environmental Research and Public Health* (Vol. 18, Issue 11, p. 6053). https://doi.org/10.3390/ijerph18116053

Wildauer, E. W., & Silva, F. P. H. da. (2013). Ethical, social, privacy, security and moral issues in an e-society. *2013 8th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6.

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. *International Journal of Public Administration*, *40*(13), 1085–1100. https://doi.org/10.1080/01900692.2016.1242614

Zeng, Y. (2022). AI Empowers Security Threats and Strategies for Cyber Attacks. *Procedia Computer Science*, *208*, 170–175. https://doi.org/https://doi.org/10.1016/j.procs.2022.10.025