VOL. 77 STUDIA POLITOLOGICZNE
DOI: 10.33896/SPolit.2025.77.10

Dorota Domalewska[*], *Aleksandra Gasztold*[**], *Rubén Arcos*[***]

Mapping the Role of Social Sciences in Cybersecurity Research[****]

Key words: *cybersecurity, social cybersecurity, human-centric approach to cybersecurity, cyber threats, social sciences*

Abstract: *The rapid evolution of cyberspace and the growing engagement of individuals in digital environments have led to a paradigm shift in cybersecurity research towards a human-centric approach. This perspective acknowledges the complexity of cybersecurity threats and their far-reaching impact on individuals, communities and society as a whole. Cybersecurity therefore needs to be studied from a multidisciplinary perspective. With a dataset of 8,330 articles from the Scopus database, this study uses bibliometric analysis and co-occurrence techniques to map the field of social cybersecurity, examine research trends and assess the overall state of cybersecurity from the perspective of social sciences. VOSviewer software was used to create network maps to illustrate the relationships between key terms and to present the advancement of thematic areas in cybersecurity research. The study reveals a significant expansion in the field of social cybersecurity,*

[*] ORCID ID: https://orcid.org/0000-0002-1788-1591; associate professor, War Studies University. E-mail: d.domalewska@akademia.mil.pl.

[**] ORCID ID: https://orcid.org/0000-0002-9114-1604; associate professor, University of Warsaw. E-mail: a.gasztold@uw.edu.pl.

[***] ORCID ID: https://orcid.org/0000-0002-9665-5874; associate professor, University Rey Juan Carlos. E-mail: ruben.arcos@urjc.es.

[****] Acknowledgements: The study was partly funded by the University of Warsaw. Additionally, it was conducted as part of a project funded by the Minister of Education and Science's program "Science for Society II." The publication was co-financed by the state budget under this program (project number NdS-II/SP/0381/2024/01 with a total project value of 450,938 PLN).

moving from conventional topics related to cyber threats, such as malware and phishing, to more nuanced areas like social media and disinformation. The analysis of major research themes in social cybersecurity research indicates that cybersecurity has been integrated with various domains such as ethics, psychology, education, and law. This paper makes an important contribution by offering an overview of social cybersecurity research, an analysis of research trends and a roadmap for future research and policy development aimed at protecting the digital ecosystem through a holistic understanding of human factors in cybersecurity.

Introduction

As cyberspace evolves and individuals increasingly engage in digital environments, there is a growing need for a human-centric approach to understanding cybersecurity challenges. This perspective takes into consideration the intricate nature of cybersecurity threats and their significant implications for individuals, communities and society as a whole[1]. The emergence and consolidation of the cyberspace as a political, economic and socio-cultural environment in which individuals engage in a diverse set of different social practices and interactions with others requires the adaptation of interdisciplinary approaches from social and behavioral sciences. Cyberspace has been responsible for important changes in both the symbolic and behavioral relationships between individuals, communities and states. Furthermore, communicative interactions in digital environments and how humans seek, process and produce information that circulates in cyberspace have an increased impact on political deliberations on public issues, political attitudes and decision-making. Political and economic behavior regularly takes place in cyberspace. Inter and intra-state political conflicts are also waged in the cyber domain, and economic competition is expressed and conducted there. Criminal activities are perpetrated through both cyber-dependent and cyber-enabled cybercrime[2]. Cyber threat actors not only exploit the vulnerabilities of computer systems and software but also the vulnerabilities of individuals that use the systems. Moreover, the vulnerabilities (e.g., political, economic, social) of communities, states and international alliances are usually exploited by malicious threat actors in disinformation and propaganda campaigns to advance

1 K. Mitnick, W. Simon, *The Art of Deception: Controlling the Human Element of Security*, New York 2002; D. Domalewska, A. Gasztold, A. Wrońska, *Humans in the Cyber Loop. Perspectives on Social Cybersecurity*, Leiden 2025.

2 C. Murphy, *Understanding Cybercrime*, European Parliamentary Research Service, March 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf. (10.09.2024).

their political objectives. As demonstrated by the COVID-19 pandemic, public health can be heavily impacted by infodemics and the exposure of individuals to mis- and disinformation that affects their behavior.

The integration of a human-centric approach in analyzing social issues, particularly in the context of technological advancements, is essential in order to foster inclusive and equitable development. The human-centric approach to cybersecurity has been proposed as an alternative to the dominant "cybersecurity as a national security issue" approach by putting instead human rights "at the epicenter"[3]. The protection of fundamental rights and freedoms enshrined in the constitutions of advanced democracies against threat actors is also a national security issue. As new technologies emerge, they invariably reshape social dynamics and impact communities in diverse ways. Adopting a human-centric framework ensures that the needs, values and experiences of individuals and communities are prioritized in the design and implementation of these technologies. This approach not only enhances the relevance and usability of technological solutions but also mitigates potential adverse effects that may arise from neglecting the human element. Cybersecurity is also an issue of cyber and digital competencies in which higher education institutions are required to play an important role in equipping individuals with the necessary knowledge and skills to sail safely the seas of cyberspace. The human-centric perspective also encourages interdisciplinary collaboration and facilitates dialogue among technologists, social scientists, policymakers, and the communities affected by these innovations. Digital disinformation and online hate speech constitute just some examples of the phenomena in cyberspace that require the contribution of interdisciplinary approaches from social sciences in order to be understood and addressed. The human-centric approach is also embedded in European policy documents such as the EU's Cybersecurity Strategy for the Digital Decade:

> Shaping international standards in the areas of emerging technologies and the core internet architecture in line with EU values is essential to ensure that the Internet remains global and open, that technologies are human-centric, privacy-focused, and that their use is lawful, safe and ethical[4].

Likewise, the Council of the European Union's Conclusions on Cyber Diplomacy called upon the EU and its member states to promote and protect human rights and freedoms in cyberspace, recalling the crucial need to pro-

[3] A. Liaropoulos, *A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia*, «Journal of Information Warfare» 2015, Vol. 14, № 4, p. 16.

[4] European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*, 2020, p. 20, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0, (2.08.2024).

mote a secure cyberspace that respects democratic values, human rights and the rule of law[5].

This paper adopts a bibliometric analysis of cybersecurity research in the social sciences to investigate trends and understand the existing body of research in the field. Despite the growing importance of social cybersecurity, little attention has been paid to the analysis of its development, progress and challenges. Bibliometric studies carried out so far have focused on specific aspects of cybersecurity, such as its relationship with sustainable development[6], the Internet of Things from a social science perspective[7] and behavioral cybersecurity[8]. However, to date, no study has comprehensively investigated trends in social cybersecurity research. This paper aims to fill that gap by conducting a systematic, quantitative analysis to map the field of social cybersecurity.

Bibliometric analysis is a method used to quantitatively examine scientific literature to identify trends and patterns in a particular discipline. It applies data mining, statistical methods and mathematical techniques to analyze bibliographic data, such as citations, authorship and keywords, to assess the impact and dissemination of research. Therefore, bibliometric analysis maps the research field and visualizes both past and emerging trends. The findings of this study will offer insights for social scientists and cybersecurity experts, helping them identify key research themes and emerging trends in the field.

Methodology

The aim of this paper is to map the field of social cybersecurity, examine research trends and the overall state of cybersecurity from the perspective of social sciences. By employing quantitative bibliometric analysis of existing literature, the following research questions have been addressed: (1) What are

5 Council of the European Union, *Draft Council Conclusions on Cyber Diplomacy* 2015, https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf, (3.08.2024).

6 A. Sulich, T. Zema, L. Kulhanek, *Towards a Secure Future: A Bibliometric Analysis of the Relations Between Cybersecurity and Sustainable Development*, «Procedia Computer Science» 2023, Vol. 225, DOI: 10.1016/j.procs.2023.10.133.

7 Y. R. Leong, F. P. Tajudeen, W. C. Yeong, *Bibliometric and Content Analysis of the Internet of Things Research: A Social Science Perspective*, «Online Information Review» 2021, Vol. 45, № 6, DOI: 10.1108/OIR-08-2020-0358.

8 S. Sajikumar, N. Ajithkumar, *Understanding the Emergence and Significance of Behavioral Cybersecurity: A Bibliometric Analysis*, «Multidisciplinary Reviews» 2024, Vol. 6, DOI: 10.31893/multirev.2023ss102.

the major research themes in social cybersecurity research documented in scholarly publications? (2) What are the collaboration patterns in the field of social cybersecurity? The database of academic publications was created by retrieving scholarly papers indexed in the Scopus repository. The search was conducted using the keywords "cybersecurity AND 'social studies' OR 'social sciences.'" The retrieval date for the dataset was August 2, 2024, yielding a total of 8,330 papers. All bibliographic information was collected (author, titles, abstract, source, volume, page, publication year, and cited reference). The search was intentionally limited to the Scopus database as it is a well-established repository known for its high-quality, peer-reviewed academic publications. Confining the scope of our research helped to avoid biases that might have arisen from overlapping databases.

The analysis was carried out with VOSviewer (version 1.6.20), a tool for data mining, mapping and the visualization of research clusters. Furthermore, the investigation was complemented by performance analysis from Scopus to enrich our understanding of research outputs. The bibliometric analysis focused on two main aspects: keyword co-occurrence and authorship mapping. Keyword co-occurrence analysis explores the relationships among various terms in the dataset, providing insights into thematic concentrations and research trends. Authorship mapping, facilitated by VOSviewer, offers a visualization of co-authorship networks, elucidating the interconnectedness of authors and the geographical spread of contributions. Performance analysis drawn from Scopus also offered a chronological overview of research outputs, illustrating the annual publication trends. Finally, the analysis included a detailed breakdown of the disciplinary distribution of the papers.

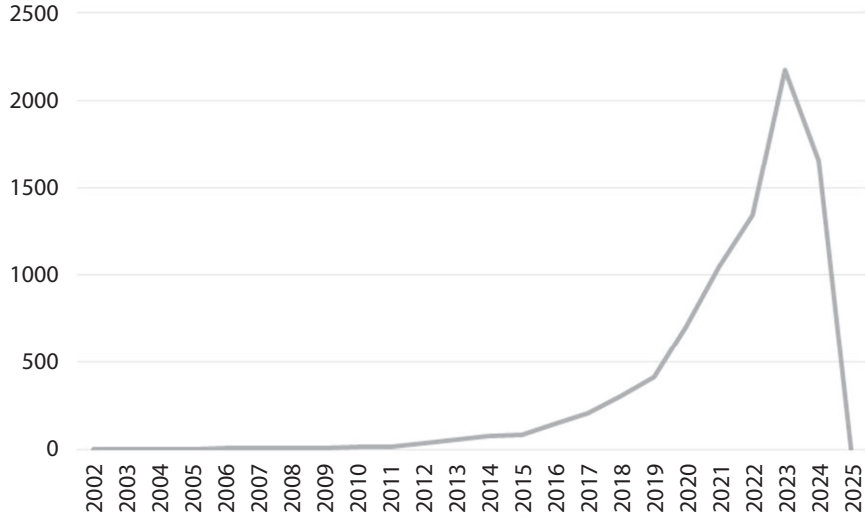
Results

A year-by-year analysis of scholarly publications was conducted first. Figure 1 shows the annual publication rate of papers from 2002 to 2025. Excluding two years with no articles (2004 and 2005), the lowest publication rate was one paper in 2002 and 2003, 6 papers in 2006 and 7 papers in 2009. A peak occurred in 2023 with 2178 articles published. As of August 2024, we have recorded 1658 papers for the year and 4 papers for 2025, and we anticipate that more will be published before the year concludes.

The trajectory of research in social cybersecurity reveals a substantial growth from virtually no research in the early 2000s to a significant surge during the COVID-19 pandemic. One of the earliest studies is a paper by Smith and

Rupp[9], quoted 72 times. It discusses how a new generation of business leaders and fast-moving companies are challenging traditional corporate structures with the internet playing a key role in transforming various sectors of the economy. It calls for informed and sensible practices to address cybersecurity risks and intellectual property challenges in the evolving internet-driven economy.

Figure 1. Annual publication growth of papers related to cybersecurity from the perspective of social sciences



Source: retrieved from Scopus.

The research interest expanded through the 2010s. The growing interest correlates with the digital transformation of organizations and businesses, which amplified the complexity and frequency of cybersecurity challenges. In 2010, 13 papers were published focused on a diverse set of cybersecurity topics, including the economics of identity management[10], legal[11], strategic challenges in ambient intelligence and privacy protections[12], and the synthesis

[9] A. D. Smith, W. T. Rupp, *Issues in Cybersecurity: Understanding the Potential Risks Associated with Hackers/Crackers*, «Information Management & Computer Security» 2002, Vol. 10, № 4, DOI: 10.1108/09685220210436976.

[10] M. Casassa Mont et al., *Economics of Identity and Access Management: a Case Study on Enterprise Business Services*, «HP Laboratories Technical Report HPL-2010-10.» 2010.

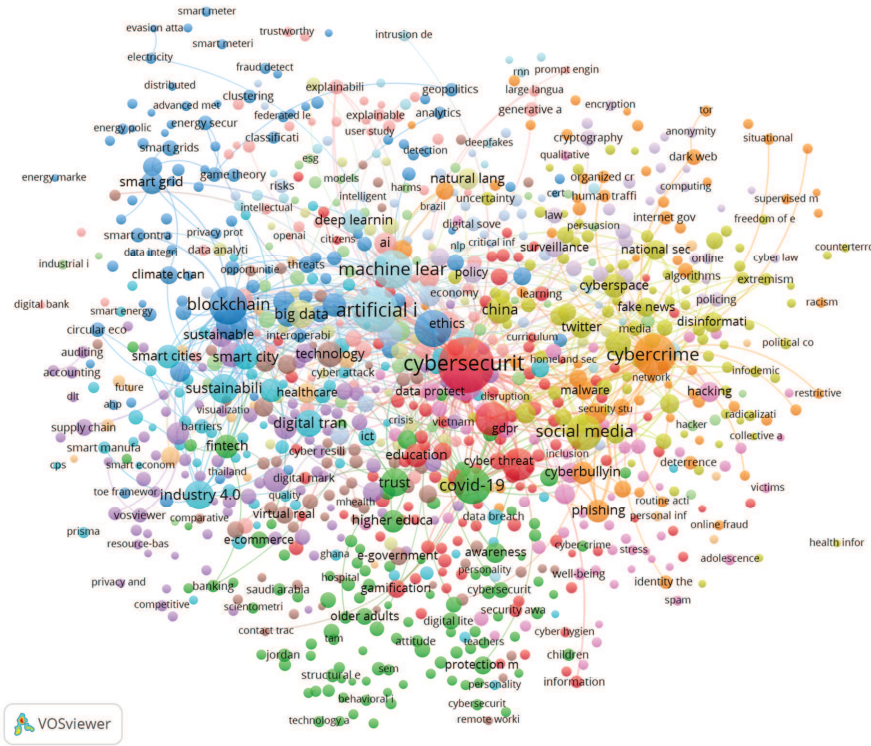
[11] H. Brechbühl et al., *Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*, «Information Technology for Development» 2010, Vol. 16, № 1, DOI: 10.1002/itdj.20096.

[12] C. Akrivopoulou, A. Psygkas (eds), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, IGI Global 2011.

of modeling for critical infrastructure[13]. An accelerating increase in research took place in 2016 due to a growing recognition of cyber threats. A surge occurred in 2021 with the publication of 2,178 papers, which indicates there was a critical focus on cybersecurity in response to increased digital dependency because of the COVID-19 pandemic and partly as a reflection of technological and societal changes that were taking place at that time.

The next stage of data analysis involved network visualization with VOSviewer, which was employed to examine the co-occurrence of keywords across various academic disciplines (Figure 2). Initially, we identified 17,801 keywords, a number too large for effective analysis. To refine our focus, we set a threshold and limited our examination to keywords that appeared at least four times. This approach resulted in 1,348 keywords that were subsequently grouped into 16 distinct clusters. By examining the keywords in each

Figure 2. Co-occurrence map of keywords across all disciplines



Source: retrieved from VOSviewer.

[13] G. Satumtira, L. Dueñas-Osorio, *Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research*, [in:] K. Gopalakrishnan, S. Peeta (eds), *Sustainable and Resilient Critical Infrastructure Systems*, Berlin–Heidelberg 2010.

cluster, we determined the unique thematic focus of each research theme. Four clusters were particularly dominant, illustrating the core areas of current research: the cybersecurity and cybercrime cluster (orange and yellow), the AI and machine learning cluster (dark blue and green), the smart cities and technology cluster (turguoise and blue), and the data protection and privacy cluster (yellow and red). The visualization presents these clusters with varying sizes of circles and text. Their prominence indicates the strength of their co-occurrence with other keywords while the distance between items and the connecting lines illustrate the strength of relationships among the keywords.

The cybersecurity and cybercrime cluster (represented by red, orange and yellow in the visualization) is the dominant cluster. It includes the research area focused on cyber threats and defense mechanisms in cyberspace. It consists of a range of topics related to cybercrime (363[14]), phishing (73), hacking (58), social engineering (46), malware (36), fraud (33), dark web (29), ransomware (29), data breaches (26), scams (16), and organized crime (12), which indicate a focus on malicious activities and their countermeasures. These topics reflect research concerns about system vulnerabilities, especially those that exploit human factors through complex social-engineering tactics. The most quoted author in this area (see Figure 4) is Holt et al.[15] from Michigan State University, whose work is related to cybercrime. Other highly cited research includes Leukfeldt and Yar[16] and Lallie et al.[17]

A considerable focus in the cybersecurity and cybercrime cluster is placed on disinformation (42), misinformation (37) and fake news (35). A large number of these keywords occurs in the context of the COVID-19 pandemic (236). This reflects the research trend when, during the pandemic, cybercrime expanded into areas that affect public opinion and health and safety. In particular, there

---

14 The co-occurrence data provided in the brackets indicate the frequency of each term's appearance in the dataset. It is important to note that these figures might not accurately represent the visual prominence of the circles in the VOSviewer diagram due to our manual calculation of variations for each keyword. For instance, terms such as hacker, hackers, hacking, and hacktivism were aggregated manually, which is not automatically reflected by VOSviewer. Furthermore, the coding colors overlap and the same color can represent two different categories.

15 T. J. Holt, G. W. Burruss, A. M. Bossler, *Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World*, «Journal of Crime and Justice» 2010, Vol. 33, № 2, DOI: 10.1080/0735648X.2010.9721287.

16 E. R. Leukfeldt, M. Yar, *Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis*, «Deviant Behavior» 2016, Vol. 37, № 3, DOI: 10.1080/01639625.2015.1012409.

17 H. S. Lallie et al., *Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Qyber-Attacks during the Pandemic*, «Computers & Security» 2021, Vol. 105, DOI: 10.1016/j.cose.2021.102248.

was a significant increase in the spread of disinformation and fake news that affected public health responses and safety. Cybercriminals and malicious actors used the situation to sow confusion, scam individuals and propagate false treatments or conspiracy theories. The most influential research in this area includes Alieva et al.[18], Hellinger[19] and Ng et al.[20]

Other dominant keywords in the cluster include social media (240) co-occurring with cyberbullying (53), which reveals a significant relationship between technical vulnerabilities and social aspects, as illustrated by research carried out by Lipschultz[21] and Zhang[22]. Moreover, the topic of education (61) stands out in this cluster. It closely interacts with themes like cyberbullying, researched by Rajbhandari and Rana[23]; cybercrime prevention, investigated by Burns at al.[24] and Willison et al.[25]; and data protection, analyzed by Hutchings and Holt[26]. The evolution of research trends reflects a significant emphasis on understanding the psychological and social dimensions of cybersecurity, particularly how emotional responses and social media interactions contribute to vulnerabilities such as cyberbullying and insider threats. The studies recommend developing tailored strategies, including emotional resilience programs and stricter cyber laws, to address the challenges. It is clear that over time, the increasing concern over the human impact of cyber threats has catalyzed research into preventive measures that blend both technological and educational approaches. The shift reflects an evolving approach to cybersecurity that

---

18 I. Alieva, J. D. Moffitt, K. M. Carley, *How Disinformation Operations against Russian Opposition Leader Alexei Navalny Influence the International Audience on Twitter*, «Social Network Analysis and Mining» 2022, Vol. 12, № 1, DOI: 10.1007/s13278-022-00908-6.

19 D. C. Hellinger, *Conspiracies and Conspiracy Theories in the Age of Trump*, Cham 2019.

20 L. H. X. Ng, I. J. Cruickshank, K. M. Carley, *Cross-Platform Information Spread During the January 6th Capitol Riots*, «Social Network Analysis and Mining» 2022, Vol. 12, № 1, DOI: 10.1007/s13278-022-00937-1.

21 J. H. Lipschultz, *Social Media Communication. Concepts, Practices, Data, Law and Ethics*, New York 2020.

22 S. Zhang et al., *Workplace Cyberbullying: A Criminological and Routine Activity Perspective*, «Journal of Information Technology» 2022, Vol. 37, № 1, DOI: 10.1177/02683962211027888.

23 J. Rajbhandari, K. Rana, *Cyberbullying on Social Media: an Analysis of Teachers' Unheard Voices and Coping Strategies in Nepal*, «International Journal of Bullying Prevention» 2023, Vol. 5, № 2, DOI: 10.1007/s42380-022-00121-1.

24 A. J. Burns et al., *The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Security-Based Precaution Taking*, «Information Systems Research» 2019, Vol. 30, № 4, DOI: 10.1287/isre.2019.0860.

25 R. Willison, P. B. Lowry, R. Paternoster, *A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research*, «Journal of the Association for Information Systems» 2018, Vol. 19, № 12.

26 A. Hutchings, T. J. Holt, *The Online Stolen Data Market: Disruption and Intervention Approaches*, «Global Crime» 2017, Vol. 18, № 1, DOI: 10.1080/17440572.2016.1197123.

considers human factors and societal norms. A large body of research, therefore, focuses on preventive measures and educational strategies, as exemplified by Catal and Tekinerdogan[27], Chua et al.[28] and Hutchings et al.[29]

The dark blue and green cluster stands for Artificial Intelligence and machine learning. It addresses the development and implications of AI and machine learning technologies, as over time more advanced computational techniques were developed. Apart from a strong focus on keywords such as AI (94), natural language processing (57), and deep learning (69), ethical considerations stand out with the co-occurrence of keywords such as trust (98) and awareness (46). This reflects the growing academic research on ethical AI, particularly responsible development and deployment of AI systems, with several prominent papers by Dwidevi[30], Tsamados et al.[31] and Stahl et al.[32] These papers highlight the importance of integrating human rights principles and ethical considerations into the development and implementation of AI to ensure it contributes positively to society. They suggest that AI technologies should not only be designed with technical efficiency in mind but must also be aligned with broader societal values such as fairness, accountability and respect for individual rights[33]. Comprehensive governance needs to be developed to address the potential biases embedded in AI systems, ensure transparency in how algorithms operate and actively mitigate risks associated with the misuse of AI, such as privacy violations and the spread of misinformation.

The keyword COVID-19 (236 co-occurrences) forms a significant link between the AI and machine learning cluster, particularly interrelating with disinformation and fake news. This complex interplay of themes has significant implications for both cybersecurity and public health information integrity.

---

27 C. Catal, B. Tekinerdogan, *Aligning Education for the Life Sciences Domain to Support Digitalization and Industry 4.0*, «Procedia Computer Science» 2019, Vol. 158, DOI: 10.1016/j.procs.2019.09.032.

28 Y. T. Chua et al., *Identifying Unintended Harms of Cybersecurity Countermeasures*, [in:] *2019 APWG Symposium on Electronic Crime Research (eCrime)*, Pittsburgh, PA, USA 2019.

29 A. Hutchings, R. Clayton, R. Anderson, *Taking down websites to prevent crime*, [in:] *2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, ON 2016.

30 Y. K. Dwivedi et al., *Opinion Paper: "So What If ChatGPT Wrote It?" Multidisciplinary Perspectives on Opportunities, Challenges and Implications of Generative Conversational AI for Research, Practice and Policy*, «International Journal of Information Management» 2023, Vol. 71, DOI: 10.1016/j.ijinfomgt.2023.102642.

31 A. Tsamados et al., *The Ethics of Algorithms: Key Problems and Solutions*, [in:] L. Floridi (ed.), *Ethics, Governance, and Policies in Artificial Intelligence*, Cham 2021.

32 B. C. Stahl et al., *Artificial Intelligence for Human Flourishing – Beyond Principles for Machine Learning*, «Journal of Business Research» 2021, Vol. 124, DOI: 10.1016/j.jbusres.2020.11.030.

33 A. Brantly, *Utopia Lost – Human Rights in a Digital World*, «Applied Cybersecurity & Internet Governance» 2022, Vol. 1, № 1, DOI: 10.5604/01.3001.0016.1238.

During the pandemic, AI technologies were extensively used to investigate the escalation of cybercrime, fraud trends and the adaptation of cybercrime markets, e.g.: Ascher and Umoja[34], Vu et al.[35] and Kemp et al.[36] Consequently, the expansive role of AI can be noticed in research connecting the topics of technology, security, ethics, and health.

The turquoise and blue cluster is dedicated to smart cities and technology with the focus on strengthening urban infrastructure to better withstand cyber threats. Prominent keywords in this cluster include blockchain (270), IoT (231), and smart cities (147), each forming an important area of research. Studies here typically examine the vulnerabilities associated with smart devices and networks in urban settings, e.g. Visvizi and Lytras [37], and how blockchain technology can be used to secure transactions and data exchanges in a decentralized manner, e.g. Sun Yin et al.,[38] Ali et al.[39] and Moosavi et al.[40]. The most cited paper is by Ghazal et al.[41] on the machine learning approaches in smart cities with IoT in the healthcare sector.

The yellow and red area consists of topics related to data protection and privacy (87). It interrelates with keywords such as social media (240), China (87) and GDPR (38). The General Data Protection Regulation (GDPR) is the European Union regulation that has set a global standard for data protection and triggered substantial research in this area as the regulation has increased awareness of privacy rights among consumers and businesses, brought about numerous changes in data protection policies, and had a spill-over effect on other countries. A large body of research in this cluster focuses on social media. Following the Russian intervention in the 2016 U.S. presidential elec-

---

34 D. L. Ascher, S. Umoja Noble, *Unmasking Hate on Twitter: Disrupting Anonymity by Tracking Trolls*, [in:] S. J. Brison, K. Gelber (eds), *Free Speech in the Digital Age*, New York 2019.

35 A. V. Vu et al., *Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras*, [in:] *Proceedings of the ACM Internet Measurement Conference*, Virtual Event USA 2020.

36 S. Kemp et al., *Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19*, «Journal of Contemporary Criminal Justice» 2021, Vol. 37, № 4, DOI: 10.1177/10439862211027986.

37 A. Visvizi, M. D. Lytras (eds), *Smart Cities: Issues and Challenges*, Amsterdam 2019.

38 H. H. Sun Yin et al., *Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain*, «Journal of Management Information Systems» 2019, Vol. 36, № 1, DOI: 10.1080/07421222.2018.1550550.

39 O. Ali et al., *A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities*, «IEEE Access» 2021, Vol. 9, DOI: 10.1109/ACCESS.2021.3050241.

40 J. Moosavi et al., *Blockchain in Supply Chain Management: A Review, Bibliometric, and Network Analysis*, «Environmental Science and Pollution Research» 2021, DOI: 10.1007/s11356-021-13094-3, http://link.springer.com/10.1007/s11356-021-13094-3.

41 T. M. Ghazal et al., *IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare – A Review*, «Future Internet» 2021, Vol. 13, № 8, DOI: 10.3390/fi13080218.

tions, social media platforms have been the focus of research studies examining their data collection methods and the implications for personal privacy. For example, Lowry et al.[42] suggest there is a broader need to re-examine the understanding of information systems and artefacts, particularly in relation to security and privacy concerns, and propose specific improvements to strengthen research methodologies and theoretical frameworks in this area. A large body of research has also focused on China's unique data privacy regulations together with state surveillance and governance strategies (e.g., Smith Ochoa et al.[43] and Howells and Henry[44]).

The analysis of research trends illustrates the evolution of cybersecurity research. The field now explores broader social implications and human-related harms alongside technological breaches. The significant interconnectedness of research clusters and the patterns of keyword co-occurrence reveal a comprehensive approach to cybersecurity that integrates technical, human, policy, and educational dimensions. The interdisciplinarity of research studies reflects the field's expansion beyond its traditional technological roots into areas encompassed by social sciences, humanities and legal studies. The complexity of modern cyber threats requires an integrated approach that addresses both technological vulnerabilities and human elements, including business strategies and policy frameworks. The broad engagement of various disciplines proves that cybersecurity is not limited to technical challenges but is a societal issue with a growing body of cybersecurity research focusing on public awareness and education, ethical considerations and policy impacts. Of particular concern are conditions and variables at the level of the individual (micro), social groups (meso), as well as entire systems (macro) requiring interdisciplinary research. The keyword analysis carried out so far points to the interdisciplinary nature of cybersecurity research. To further explore this aspect, we analyzed discipline distribution with data directly retrieved from Scopus. The database offers a breakdown into disciplines by assigning journals to subject areas based on their focus, further analyzing the content of individual papers through titles, abstracts, keywords, and citations, and using algorithms that examine keyword relevance and citation networks in defined fields. The analysis allows us to identify which fields are most actively engaged with cybersecurity issues.

---

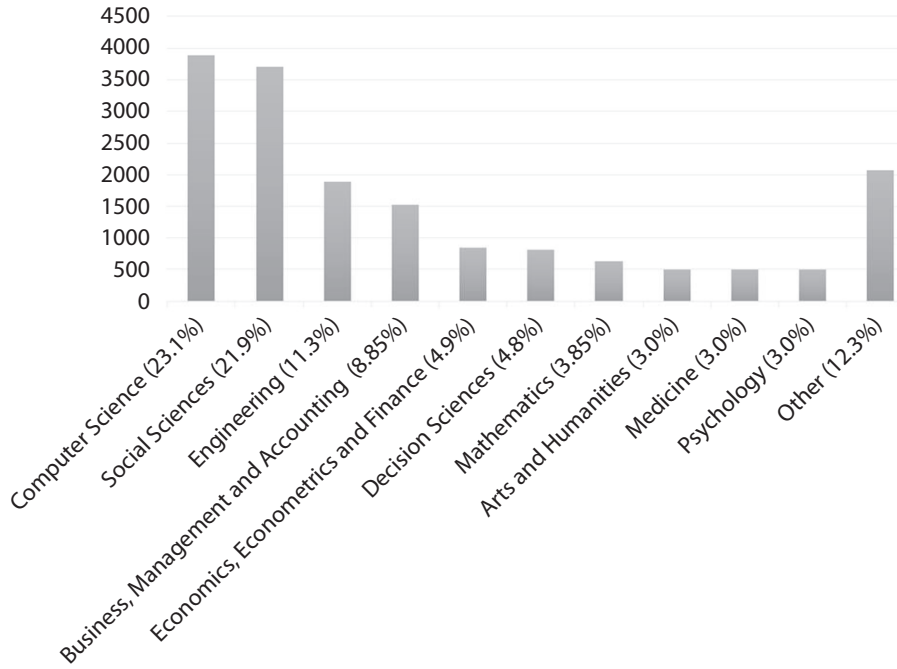
42 P. B. Lowry, T. Dinev, R. Willison, *Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda*, «European Journal of Information Systems» 2017, Vol. 26, № 6, DOI: 10.1057/s41303-017-0066-x.

43 C. Smith Ochoa, F. Gadinger, T. Yildiz, *Surveillance under Dispute: Conceptualising Narrative Legitimation Politics*, «European Journal of International Security» 2021, Vol. 6, № 2, DOI: 10.1017/eis.2020.23.

44 L. Howells, L. A. Henry, *Varieties of Digital Authoritarianism*, «Communist and Post-Communist Studies» 2021, Vol. 54, № 4, DOI: 10.1525/j.postcomstud.2021.54.4.1.

Figure 3. illustrates the multidisciplinary nature of cybersecurity research (even though the keyword search has already been limited to social sciences / social studies). Technology driven disciplines dominate (computer science is the leading discipline, engineering ranked third), which proves its foundational role in cybersecurity research. Research in this area focuses on AI, machine learning, blockchain, cybercrime, ICT, and IoT – technologies that are crucial for developing effective defense mechanisms and predictive models.

Figure 3. Breakdown of the disciplinary distribution in cybersecurity research



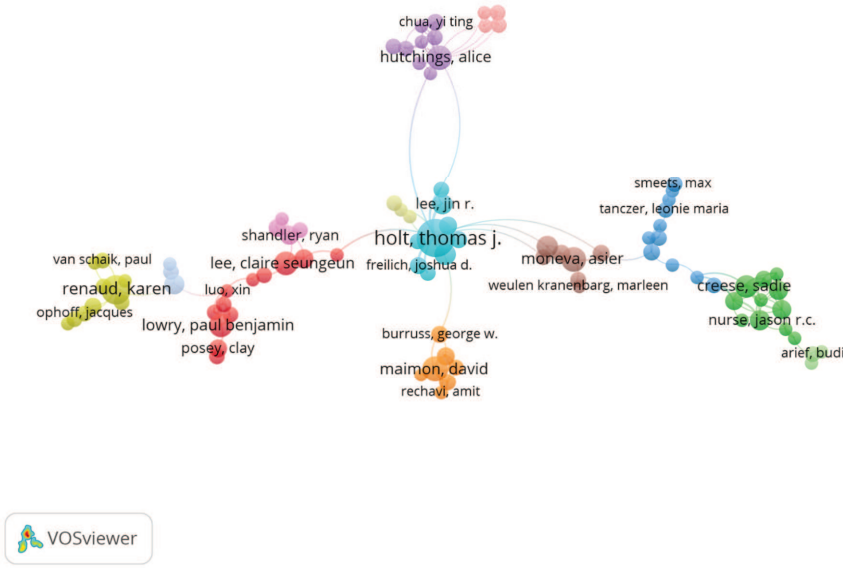
Source: retrieved from Scopus.

There is considerable involvement of social sciences and business studies, which indicates a shift towards understanding cybersecurity as a complex societal challenge. In fact, business-related research emerged in 2010, which reflects an early recognition of the economic and strategic impacts of cybersecurity in the business sector. It also proves that social cybersecurity is very much related with the field of management sciences. Another interesting finding is the prominent role of the arts and humanities and psychology in cybersecurity research. It points to an expanding scope of inquiry that considers ethical, psychological and cultural dimensions of cybersecurity. The diverse engagement of several disciplines also suggests that effective cybersecurity

strategies require a holistic approach that integrates both technical solutions and a deep understanding of human behavior, societal values and ethical considerations. The multidisciplinary approach not only enhances the effectiveness of cybersecurity measures but also ensures they are sustainable, culturally sensitive, ethically sound, and align with broader social norms and values.

Next, we conducted an analysis of the cooperation network (co-authorship and citation analysis) to explore connections between authors. In this network, the size of a node corresponds to the number of times an author has been cited, while links represent collaborations that have resulted in joint publications. This methodology enables us to visualize research trends and identify influential researchers in the field. A total of 22,032 authors have contributed to research in cybersecurity from a social sciences perspective. We limited our focus to authors who have published at least three documents indexed in the Scopus database and at least one of their papers has received a minimum of two citations. This approach helped us identify 724 authors who met these criteria.

Figure 4. Distribution of authors across all fields



Source: retrieved from VOSviewer.

The reference network is segmented into eight distinct co-citation clusters that represent different subfields or thematic groups in cybersecurity research. Central figures like Thomas J. Holt from the School of Criminal Justice at Michigan State University, Karen Renaud from the University of Strathclyde, Paul Benjamin Lowry from Virginia Tech, David Maimon from Georgia State Univer-

sity, Asier Moneva from the Netherlands Institute for the Study of Crime and Law Enforcement, and Sadie Creese from the University of Oxford dominate in their clusters. Out of the 22,032 authors analyzed, only 93 had significant interconnections through collaboration or citation networks. This is an important finding that shows a large degree of fragmentation in the field as many researchers work independently or in small, disconnected groups. Fragmentation could also indicate a diversity of research agendas and methodologies that do not always overlap or engage with each other. On the other hand, a considerable number of independent authors may represent emerging researchers or niche topics. This could imply that the field is notable for a wide range of theoretical and methodological approaches, which do not always interact or converge. Such fragmentation can lead to challenges in forming a cohesive understanding or advancing unified theories in the field. This interpretation, however, seems unlikely given the low citation impact observed in the field.

Out of the 22,032 authors analyzed, only 3% (724 authors) had at least one paper published with at least 2 citations, which indicates that there are a small number of researchers with significant influence in the field. Few studies have impacted research and were able to contribute to the advancement of the field. Such a low citation rate not only points to a disconnect between research output and its practical or scholarly influence but also may suggest that the field of social cybersecurity is still developing (as indicated by the research output timeline displayed in Figure 1). For the social cybersecurity field to grow, there is a need for more focused and impactful research directions. An independent area of focus, which requires further inquiry, is the gender gap in cybersecurity research, as in other fields related to security[45]. Although the number of women entering the IT industry and cybersecurity research is steadily increasing, the gender gap remains significant. It is essential to examine whether women are sufficiently represented in research, as issues such as the wage gap, academic promotions and enduring stereotypes continue to hinder gender equality. It is also worth investigating how initiatives such as scholarships, mentoring programs and project funding that emphasize gender balance encourage women to pursue cybersecurity careers. However, the issue of women's representativeness in cyber security research is broader, as threats in the digital sphere disproportionately affect women and marginalized groups[46].

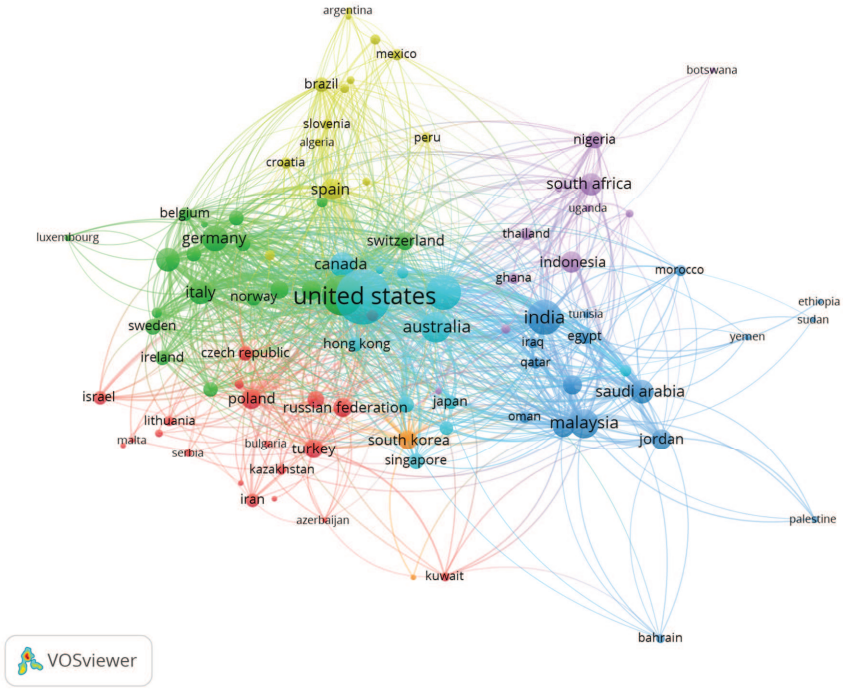
---

[45] M. Rost Rublee et al., *Do You Feel Welcome? Gendered Experiences in International Security Studies*, «Journal of Global Security Studies» 2020, Vol. 5, № 1, DOI: 10.1093/jogss/ogz053.

[46] J. Slupska, *Safe at Home: Towards a Feminist Critique of Cybersecurity*, «St Antony's International Review» 2019, Vol. 15, № 1, pp. 83–100; S. Shoker, *Making Gender Visible*

Figure 5 illustrates the cooperation network based on co-authorship between countries. The size of each node represents the number of articles published by those countries.

Figure 5. Geographical distribution map



Source: retrieved from VOSviewer.

The top 3 countries include the United States, India and Malaysia. The analysis also revealed the largest cooperation clusters could be found in these countries.

Discussion and conclusion

This study provides a comprehensive analysis of research trends and the overall state of cybersecurity from the perspective of social sciences, which was the main aim of the study. Two research questions guided the inquiry (1) What are the major research themes in social cybersecurity research as

in Digital ICTs and International Security, «SRRN Paper» 2020, March 23, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4170993 (3.08.2024).

documented in scholarly publications indexed in Scopus? (2) What are the collaboration patterns in the field of social cybersecurity? Through a bibliometric analysis of scholarly papers retrieved from the Scopus database, we investigated scientific outputs in the field. The analysis of keyword distribution shows a significant expansion in the social cybersecurity field, moving from conventional topics related to cyber threats, such as malware and phishing, to more nuanced areas like social media and disinformation.

Keywords related to purely technical issues, such as artificial intelligence, machine learning and natural language processing, frequently co-occur with a variety of other keywords not directly related to technical issues, such as smart cities, COVID-19, education and social media. During the COVID-19 pandemic, an increase in cyber threats was seen as many areas of life moved to digital platforms for health information, remote work and education. The protection from these threats, however, to a great extent, concerns the integrity of information threatened by the ever-increasing disinformation and phishing scams. A large body of research has drawn public attention to the negative effects of social media on mental health, democratic processes and public trust. Social platforms facilitated rapid dissemination of misinformation, increased social and political divisions and enabled the manipulation of public opinion on a vast scale as cyber criminals and political actors tried to exploit the crisis for their advantage. Many cyberattacks during this time were strategies of information warfare, deliberately spreading false information to manipulate public opinion and destabilize electoral processes. The term "fake news" itself, widely recognized and popularized during the 2016 US presidential election, points to the strategic use of misleading content in cyber operations.

The analysis of major research themes in social cybersecurity research indicates that cybersecurity has been integrated with various domains such as ethics, psychology, education, and law. The expansion of cybersecurity research to ethical and privacy implications indicates evolution towards more responsible use of technology that focuses on protecting privacy and ensuring the ethical use of AI. Education is crucial for cybersecurity research because increased awareness of cyber threats and the need to enhance societal resilience are important strategies for establishing security. Well-informed communities significantly contribute to the proactive defence against cyber incidents. Finally, a growing focus on regulations such as GDPR reflects a trend towards stronger data protection and privacy standards. The integration of legal analysis into cybersecurity research reflects the development of legislation designed to enhance cybersecurity, increase transparency and ensure accountability across various sectors.

The analysis also examines collaboration networks in cybersecurity research. It reveals significant fragmentation as most authors work independently or in small, disconnected groups. Much research is not widely cited, which suggests that the vast majority of research carried out in the field had minimal impact. The lack of a cohesive research community implies the need for more focused and impactful research to effectively advance the field of social cybersecurity. Furthermore, significant fragmentation and the limited impact of studies indicate an opportunity for cross-disciplinary engagement and innovation. By encouraging researchers to build collaborations, the field can be enriched through the integration of diverse perspectives and expertise.

There is still a scarcity of publications on national security. Topics such as cyberterrorism, hybrid warfare and related security challenges have not emerged as significant areas of focus. There is, therefore, a need to expand research into how cyber threats integrate with national security measures and the implications for policy and practice. Research in this area is crucial in order to develop a comprehensive understanding of the broader security architecture and increase resilience against complex threats on a national scale.

The study results are subject to several limitations. First, the analysis was limited to the papers retrieved from the Scopus database. Although it is an extensive repository of high-ranking peer-reviewed research, it does not include all scholarly publications. Therefore, relevant research published in non-Scopus-indexed journals could have been excluded from the analysis. Second, the study focused on co-occurrence keywords in the dataset, which may not fully describe the entire scope of research themes or the nuances of how topics are discussed in the literature, particularly if different terminology is used across disciplines.

References

Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, IGI Global 2011.

Ali O., Jaradat A., Kulakli A., Abuhalimeh A., *A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities*, «IEEE Access» 2021, Vol. 9, DOI: 10.1109/ACCESS.2021.3050241.

Alieva I., Moffitt J. D., Carley K. M., *How Disinformation Operations Against Russian Opposition Leader Alexei Navalny Influence the International Audience on Twitter*, «Social Network Analysis and Mining» 2022, Vol. 12, № 1, DOI: 10.1007/s13278-022-00908-6.

Ascher D. L., Umoja Noble S., *Unmasking Hate on Twitter: Disrupting Anonymity by Tracking Trolls*, [in:] S. J. Brison, K. Gelber (eds.), *Free Speech in the Digital Age*, New York 2019.

Brantly A., *Utopia Lost – Human Rights in a Digital World*, «Applied Cybersecurity & Internet Governance» 2022, Vol. 1, № 1, DOI: 10.5604/01.3001.0016.1238.

Brechbühl H., Bruce R., Dynes S., Johnson M. E., *Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*, «Information Technology for Development» 2010, Vol. 16, № 1, DOI: 10.1002/itdj.20096.

Burns A. J., Roberts T. L., Posey C., Lowry P. B., *The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Security-Based Precaution Taking*, «Information Systems Research» 2019, Vol. 30, № 4, DOI: 10.1287/isre.2019.0860.

Casassa Mont M., Beres Y., Pym D., Shiu S., *Economics of Identity and Access Management: a Case Study on Enterprise Business Services*, «HP Laboratories Technical Report HPL» 2010, № 10.

Catal C., Tekinerdogan B., *Aligning Education for the Life Sciences Domain to Support Digitalization and Industry 4.0*, «Procedia Computer Science» 2019, Vol. 158, DOI: 10.1016/j.procs.2019.09.032.

Chua Y. T., et al., *Identifying Unintended Harms of Cybersecurity Countermeasures*, [in:] *2019 APWG Symposium on Electronic Crime Research (eCrime)*, Pittsburgh, PA, USA 2019.

Council of the European Union, *Draft Council Conclusions on Cyber Diplomacy*, 2015, https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

Dwivedi Y. K., et al., *Opinion Paper: "So What if ChatGPT Wrote it?" Multidisciplinary Perspectives on Opportunities, Challenges and Implications of Generative Conversational AI for Research, Practice and Policy*, «International Journal of Information Management» 2023, Vol. 71, DOI: 10.1016/j.ijinfomgt.2023.102642.

Domalewska D., Gasztold A., Wrońska A., *Humans in the Cyber Loop. Perspectives on Social Cybersecurity*, Leiden 2025.

European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*, 2020, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

Ghazal T. M., et al., *IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare – A Review*, «Future Internet» 2021, Vol. 13, № 8, DOI: 10.3390/fi13080218.

Hellinger D. C., *Conspiracies and Conspiracy Theories in the Age of Trump*, Cham 2019.

Holt T. J., Burruss G. W., Bossler A. M., *Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World*, «Journal of Crime and Justice» 2010, Vol. 33, № 2, DOI: 10.1080/0735648X.2010.9721287.

Howells L., Henry L. A., *Varieties of Digital Authoritarianism*, «Communist and Post-Communist Studies» 2021, Vol. 54, № 4, DOI: 10.1525/j.postcomstud.2021.54.4.1.

Hutchings A., Clayton R., Anderson R., *Taking down websites to prevent crime*, [in:] *2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, ON 2016.

Hutchings A., Holt T. J., *The online stolen data market: disruption and intervention approaches*, «Global Crime» 2017, Vol. 18, № 1, DOI: 10.1080/17440572.2016.1197123.

Kemp S., et al., *Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19*, «Journal of Contemporary Criminal Justice» 2021, Vol. 37, № 4, DOI: 10.1177/10439862211027986.

Lallie H. S., et al., *Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic*, «Computers & Security» 2021, Vol. 105, DOI: 10.1016/j.cose.2021.102248.

Leong Y. R., Tajudeen F. P., Yeong W. C., *Bibliometric and Content Analysis of the Internet of Things Research: A Social Science Perspective*, «Online Information Review» 2021, Vol. 45, № 6, DOI: 10.1108/OIR-08-2020-0358.

Leukfeldt E. R., Yar M., *Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis*, «Deviant Behavior» 2016, Vol. 37, № 3, DOI: 10.1080/01639625.2015.1012409.

Liaropoulos A., *A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia*, «Journal of Information Warfare» 2015, Vol. 14, № 4.

Lipschultz J. H., *Social Media Communication. Concepts, Practices, Data, Law and Ethics*, New York 2020.

Lowry P. B., Dinev T., Willison R., *Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda*, «European Journal of Information Systems» 2017, Vol. 26, № 6, DOI: 10.1057/s41303-017-0066-x.

Mitnick K., Simon W., *The Art of deception: Controlling the Human Element of Security*, New York 2002.

Moosavi J., Naeni L. M., Fathollahi-Fard A. M., Fiore U., *Blockchain in Supply Chain Management: A Review, Bibliometric, and Network Analysis*, «Environmental Science and Pollution Research» 2021, DOI: 10.1007/s11356-021-13094-3, http://link.springer.com/10.1007/s11356-021-13094-3.

Murphy C., *Understanding Cybercrime*, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf.

Ng L. H. X., Cruickshank I. J., Carley K. M., *Cross-Platform Information Spread During the January 6th Capitol Riots*, «Social Network Analysis and Mining» 2022, Vol. 12, № 1, DOI: 10.1007/s13278-022-00937-1.

Rajbhandari J., Rana K., *Cyberbullying on Social Media: an Analysis of Teachers' Unheard Voices and Coping Strategies in Nepal*, «International Journal of Bullying Prevention» 2023, Vol. 5, № 2, DOI: 10.1007/s42380-022-00121-1.

Rost Rublee M., et al., *Do You Feel Welcome? Gendered Experiences in International Security Studies*, «Journal of Global Security Studies» 2020, Vol. 5, Issue 1, DOI: 10.1093/jogss/ogz053.

Sajikumar S., Ajithkumar N., *Understanding the emergence and significance of behavioral cybersecurity: A bibliometric analysis*, «Multidisciplinary Reviews» 2024, Vol. 6, DOI: 10.31893/multirev.2023ss102.

Satumtira G., Dueñas-Osorio L., *Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research*, [in:] K. Gopalakrishnan, S. Peeta (eds.), *Sustainable and Resilient Critical Infrastructure Systems*, Berlin–Heidelberg 2010.

Shoker S., *Making Gender Visible in Digital ICTs and International Security*, «SRRN Paper» 2020, March 23.

Slupska J., *Safe at Home: Towards a Feminist Critique of Cybersecurity*, «St Antony's International Review» 2019, Vol. 15, No. 1.

Smith A. D., Rupp W. T., *Issues in Cybersecurity: Understanding the Potential Risks Associated with Hackers/ rackers*, «Information Management & Computer Security» 2002, Vol. 10, № 4, DOI: 10.1108/09685220210436976.

Smith Ochoa C., Gadinger F., Yildiz T., *Surveillance under Dispute: Conceptualising Narrative Legitimation Politics*, «European Journal of International Security» 2021, Vol. 6, № 2, DOI: 10.1017/eis.2020.23.

Stahl B. C., et al., *Artificial Intelligence for Human Flourishing – Beyond Principles for Machine Learning*, «Journal of Business Research» 2021, Vol. 124, DOI: 10.1016/j.jbusres.2020.11.030.

Sulich A., Zema T., Kulhanek L., *Towards a Secure Future: A Bibliometric Analysis of the Relations Between Cybersecurity and Sustainable Development*, «Procedia Computer Science» 2023, Vol. 225, DOI: 10.1016/j.procs.2023.10.133.

Sun Yin H. H., et al., *Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain*, «Journal of Management Information Systems» 2019, Vol. 36, № 1, DOI: 10.1080/07421222.2018.1550550.

Tsamados A., et al., *The Ethics of Algorithms: Key Problems and Solutions*, [in:] L. Floridi (eds.), *Ethics, Governance, and Policies in Artificial Intelligence*, Cham 2021.

Visvizi A., Lytras M. D. (eds.), *Smart Cities: Issues and Challenges*, Amsterdam 2019.

Vu A. V., et al., *Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras*, [in:] *Proceedings of the ACM Internet Measurement Conference*, Virtual Event USA 2020.

Willison R., Lowry P. B., Paternoster R., *A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research*, «Journal of the Association for Information Systems» 2018, Vol. 19, № 12.

Zhang S., Leidner D., Cao X., Liu N., *Workplace Cyberbullying: A Criminological and Routine Activity Perspective*, «Journal of Information Technology» 2022, Vol. 37, № 1, DOI: 10.1177/02683962211027888.