Cybercrime: The Current State of Literature and Issues Facing CISOs

Caitlin Ferreira
ORCID: 0000-0001-9575-6676
Graduate School of Business University of Cape Town, Cape Town, South Africa
Email: caitlin.ferreira@uct.ac.za

Andrew Park
Gustavson School of Business, University of Victoria, Victoria, BC, Canada
Email: apark1@uvic.ca

Jan Kietzmann* (Corresponding author)
ORCID: 0000-0002-3576-994X
Gustavson School of Business, University of Victoria, Victoria, BC, Canada
Email: jkietzma@uvic.ca

Dionysios Demetis
Hull University Business School, University of Hull, UK
Email: D.Demetis@hull.ac.uk

Andrew Flostrand
Beedie School of Business, Simon Fraser University, Vancouver, Canada
Email: flostran@sfu.ca

Ian McCarthy
ORCID: 0000-0003-3330-0977
Beedie School of Business, Simon Fraser University, Vancouver, Canada
and
Luiss, Rome, Italy
Email: imccarth@sfu.ca

Leyland Pitt
ORCID: 0000-0002-3089-9184
Beedie School of Business, Simon Fraser University, Vancouver, Canada
Email: lpitt@sfu.ca

On behalf of all authors, the corresponding author acknowledges that there are no conflicts of interest to report.

Cybercrime: The Current State of Literature and Issues Facing CISOs

ABSTRACT

The meteoric rise in cybercrime in recent years has resulted in renewed efforts to stem the potential negative effects of these nefarious activities. The sheer amount of data gathered by organizations in a digital-first society makes them prime targets of cybercrime activity. As such, the role of the Chief Information Security Officer (CISO) has become one of strategic importance, safeguarding the integrity of the organization's digital assets. Given the economic impact of cybercrime, it has become critically important to understand the cybercrime-related issues that organizations face. We sought to identify these issues by conducting a bibliographic analysis of cybercrime research. The results identified the most prolific and impactful authors, journals and countries of publication, the most influential articles and trends in the literature on cybercrime. The research suggests that interest in the field is wide-reaching with the growth in publications stemming from diverse academic disciplines and geographies. The identified trends represent critical knowledge areas for the CISO that are likely to continue the expansion of the field.

Keywords: Cybercrime, bibliographic analysis, VOSviewer, CISO.

Cybercrime: The Current State of Literature and Issues Facing CISOs

Cybercrime is of grave concern in today's digital age. Cybercrime threats stem not only from its economic impact, but also from increasingly ubiquitous technologies allowing perpetrators to readily cooperate with one another, and the perpetual hazards to security and privacy for individuals and organizations alike. Research predicts that the cost of cybercrime will be approximately $10.5 trillion annually by 2025, up from $3 trillion in 2015[1]. This aligns with the World Economic Forum outlining the extent of cybercrime as the third largest global economy[2].

Cybercrime is typically defined as *"criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity"*[3]. These criminal activities target several different stakeholders including citizens, organizations, and governmental institutions. The Internet has had a significant impact on criminal activity primarily by creating more opportunities for traditional crimes, while growing opportunity for new digital crimes[4]. Unlike traditional crime, cybercrime is not limited to a specific geographic location, thus requiring a broader, global response to mounting issues relating to cybercrime[5].

Cybercriminals tend to use several different techniques to engage in these criminal activities and in many cases these crimes seek to exploit vulnerabilities in computer systems and networks. However, it is important to note that cybercrime is by no means a new phenomenon, but rather one that evolves with new technologies. The global pandemic and the subsequent, rapid digital shifts in the labor market have brought about far greater potential for cybercriminals. While the growing digitization across industries means that the traditional targets for cybercrime, including computers, networks and personal devices now extends to any digitally enabled device, including any smart devices, transportation networks and power grids[1].

Recently, there has been a rapid expansion of the cybercrime-related literature, which is likely aligned with the meteoric growth of cybercrime[6]. The increasing prevalence of cyberattacks has resulted in an increasing importance being place on the role of the Chief Information Security Office (CISO) in many organizations. The CISO, operating closely with the Chief Information Officer (CIO), needs to be equipped to adopt a range of strategic and tactical security measures to counteract any cyber threats faced by the organization[7]. While the primary role of the CISO is to identify any cyber threats and ensure that safeguards are put in place to protect the organization against such threats – this responsibility has broadened significantly in recent years. Today, the CISO is expected to be a critical outward-focused communicator that can influence key stakeholders and effect strategy at a broad-level[7]. The value of an organization primarily lies in their ability to safeguard their digital assets and ensure a heightened level of cyber resilience[1].

As the field of research continues to develop, it is imperative to better understand the intellectual landscape sustaining this growth in order to first, understand what is driving the expansion and

second, to identify trends that could potentially foreshadow the future direction of the field[8]. From a practitioner perspective, it is critical for the CISO to clearly understand the evolving issues that organizations face when it comes to cybercrime and from an academic perspective, it is critical that researchers within the Information Systems field understand these issues to further advance research. As such, this research seeks to identify the key research in scholarly journals related to cybercrime, including a consideration of the most prolific authors, journals and countries of publication, an analysis of keyword co-occurrence as well as an overview of the most influential research in the field.

METHODOLOGY

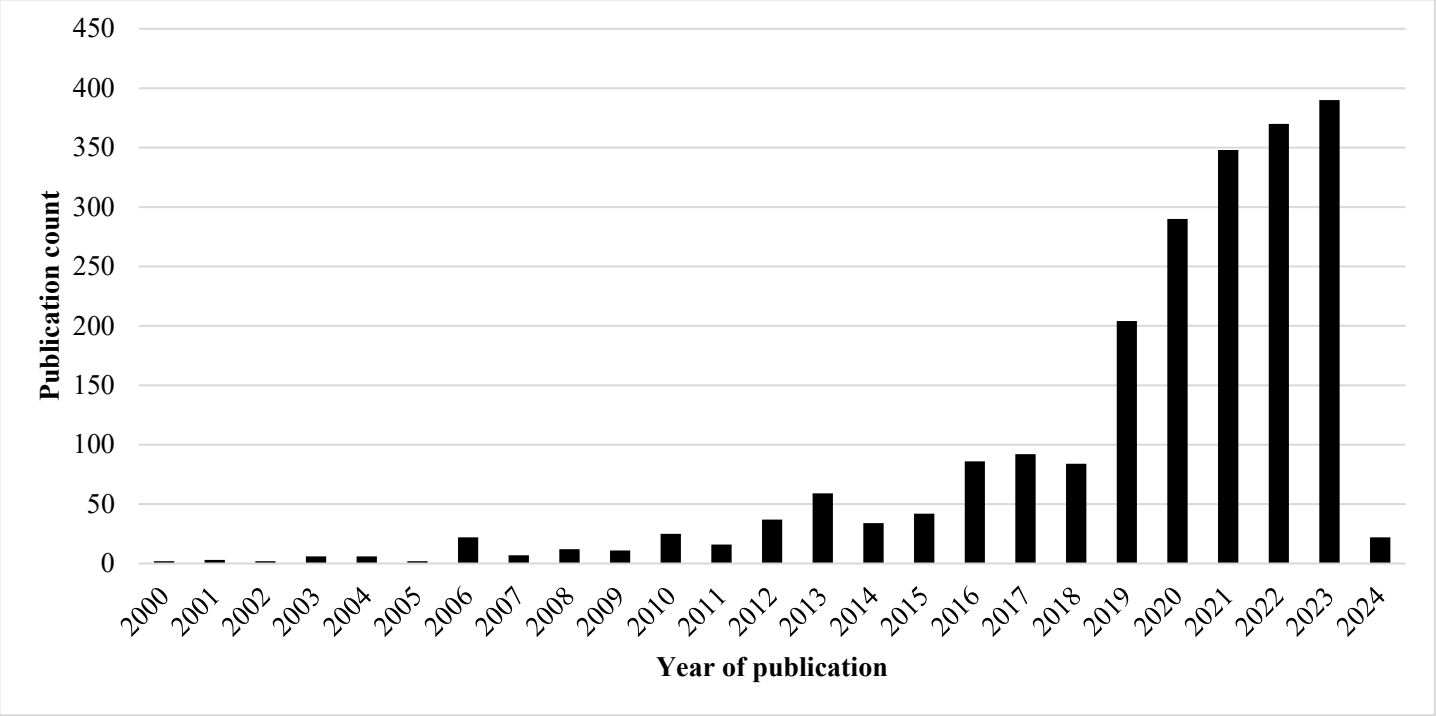
Academic articles were extracted from the Web of Science (hereafter WoS) bibliographic database. Two criteria were set for eligibility in the database for the analysis. First, only academic journal articles were included in the search, to exclude possible duplication whereby the same research had been published across different outlets. Second, articles had to use the term "cybercrim*" in the title, abstract or keywords of the article. The asterisk indicates that variations in the ending of the word "cybercrim" (i.e., cybercriminal and cybercrime) were permitted. Using these two criteria, a total of 2,283 articles were extracted and served as the database for this research. The data extracted from the WoS database was then used to craft bibliographic maps using the VOSviewer software. The VOSviewer software is a free tool that uses databases to graphically illustrate bibliographic networks[9].

RESULTS

Publication analysis

The results suggest that interest in the field of cybercrime appears relatively low and stable until approximately 2016, after which interest in the field begins to slowly increase, with rapid expansion from 2020 onwards. As evidenced in Figure 1, the years 2022 and 2023 represent the peak of interest in the field to date.

Figure 1: Total cybercrime-related articles in WoS database per year



The results further suggest that research pertaining to cybercrime has been published in a multitude of different academic disciplines, indicating an expansion in the relevance of the topic to diverse disciplines. The most prominent WoS category publishing cybercrime-related literature is criminology/penology (26.38% of publications), followed by computer science information systems (26.24% of publications), engineering and electronic (10.73% of publications), law (8.89% of publications) and telecommunications (8.84% of publications) over the 24-year period. Of interest is the inclusion of the social sciences, psychology, physical science, political science and sociology within the list of the top twenty publishers of cybercrime research.

Author networks

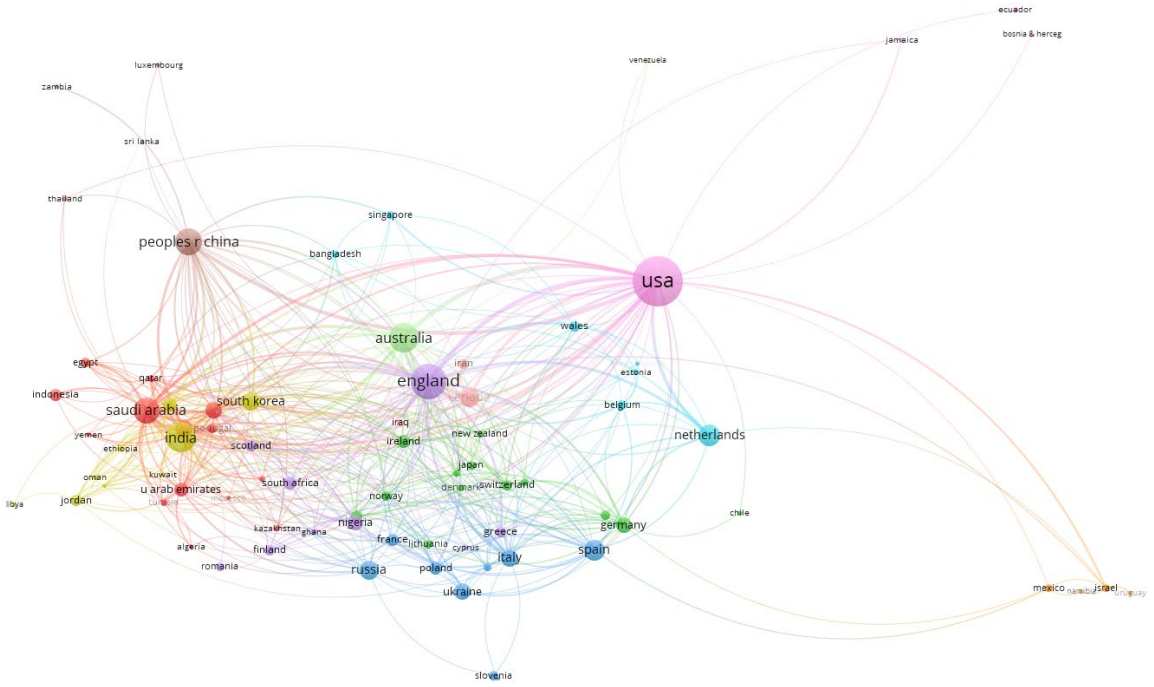
To determine critical thought leadership within the field, we considered the most prolific authors by examining the number of articles published per author. The results suggest that several authors had published multiple articles pertaining to cybercrime, with eleven authors publishing at least ten articles between 2000 and 2024. The most prolific author was Thomas Holt, a Professor in the School of Criminal Justice at Michigan State University with listed research interests in computer hacking, malware, and the use of the internet as a facilitator of criminal activity. Holt was noted as the most prolific (in terms of publications) and the most impactful (in terms of citations) author in the period - publishing 63 articles and achieving a total of 1305 citations (see Table 1). It is worth noting that Holt is the most prolific author in the field by a substantial margin. The second

most prolific author during the period was Alazab (17 publications), followed by Kshetri (16 publications), then Bossler (15 publications).

Country and journal networks

Considering the most prolific countries for the publication of cybercrime-related research, we find that much of the discourse is being shaped by the USA (507 publications), followed by England (260 publications), India (192 publications) and Australia (174 publications). Considering the co-authorship links on a country-level (Figure 2), strong links are noted between the most prolific countries for publishing, with the shorter distance between clusters indicating closer citation links.

Figure 2: Network map of co-authorship by country



The most prolific outlets for cybercrime publications provides insight into the leading journals shaping the future direction of the field. The leading journal for cybercrime articles, *IEEE Access* published 77 articles in the designated period, followed closely by the *International Journal of Cyber Criminology* (67 publications), *Computers & Security* (47 publications) and *Deviant Behavior* (29 publications).

Evaluation of impact

Given that metrics of publication alone are not sufficient to determine the impact of research within a field, Table 1 provides an overview of the top ten most cited countries, journals and authors for

cybercrime research during the period. The results suggest that the USA is the most impactful country of publication, achieving 7,119 citations throughout the period, *IEEE Access* is the most impactful journal for cybercrime publications, achieving 1,882 citations during the period, more than double any other journal.

Table 1: Top Ten Most-Cited Countries, Journals and Authors of Cybercrime Research

Ranking	Country	Journal	Author
1	United States of America (7119)	IEEE Access (1882)	Holt, T. (1305)
2	England (3258)	Deviant Behavior (752)	Alazab, M. (1153)
3	Australia (3170)	Computers and Security (724)	Soman, K. (811)
4	India (2050)	Computers in Human Behavior (594)	Poornachandran, P. (795)
5	People's Republic of China (1709)	Journal of Contemporary Criminal Justice (423)	Vinayakumar, R. (795)
6	Canada (1458)	Crime, Law and Social Change (374)	Venkatraman, S. (786)
7	Netherlands (1387)	British Journal of Criminology (349)	Bossler, A. (681)
8	Saudi Arabia (1155)	Cyberpsychology, Behavior and Social Networking (340)	Al-Nemrat, A. (600)
9	South Korea (874)	Digital Investigation (337)	Choo, K. (499)
10	Malaysia (825)	Future Generation Computer Systems (304)	Reyns, B. (396)

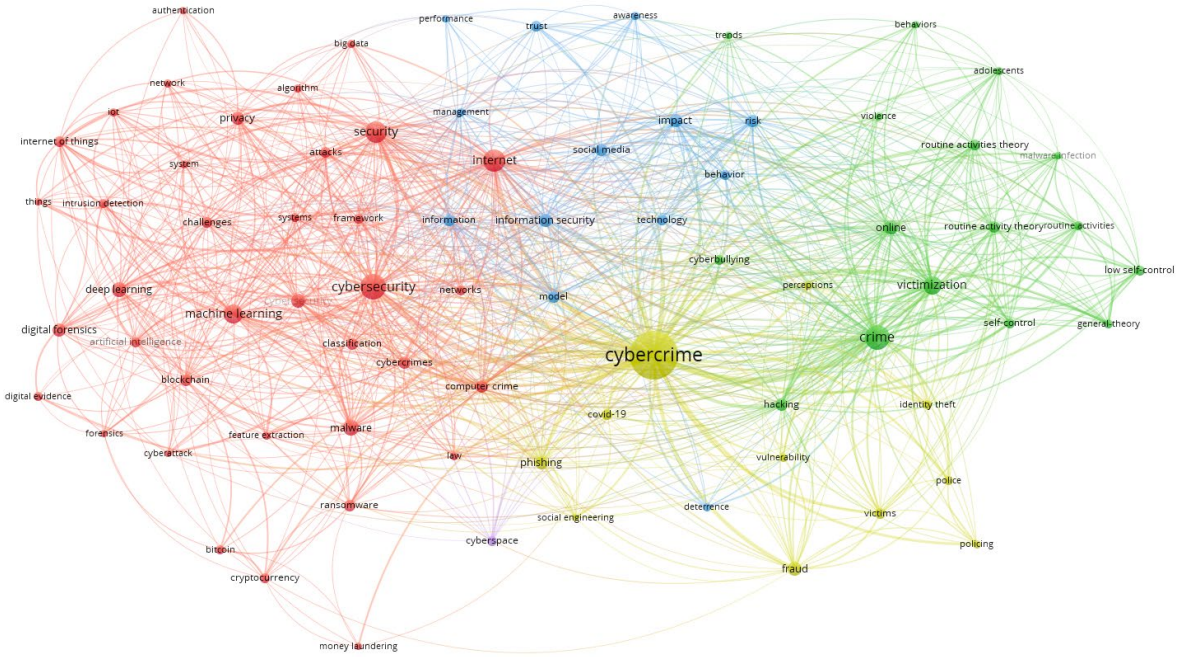
*Note that the number in brackets in the total number of citations during the period under investigation.

Keyword co-occurrence

The keyword co-occurrence network *"focuses on understanding the knowledge components and knowledge structure of a scientific field by examining the links between keywords in the literature"*[10]. The keywords present a summary of the critical themes in each article in the database, which is able to provide insight into the future direction of the field. The most commonly occurring keyword, cybercrime, was identified 837 times in the dataset, followed by cybersecurity (233), crime (224), internet (181) and security (163).

As identified in Figure 3 below, the research identified four distinct clusters, representing trends in the literature, where each keyword occurred at least 20 times. The first cluster (red) focuses on the technical aspects of cybersecurity and new technologies that may impact cybersecurity, with notable inclusions of artificial intelligence, block chain, cryptocurrency and big data. The second cluster (yellow) primarily considers drivers of cybercrime, including phishing, vulnerabilities, identify theft and fraud. The third cluster (green) tends to focus on outcomes and potential effects of cybercrime including cyberbullying, malware, infection and violence. The final cluster (blue) primarily considers factors that could impact one's propensity to be exposed to cybercrime including trust, awareness, behaviors and information security.

Figure 3: Network map of keyword co-occurrence



Most influential articles

Vinayakumar and colleagues achieved the greatest number of WoS citations (595) during the period with a further article placing sixth (173 citations). The top ten most-cited cybercrime articles during the period are presented in Table 2 below.

Table 2: Top Ten Most-Cited Cybercrime-related Articles

No.	Article	Number of WoS citations
1	Vinayakumar et al. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access, 7,* 41525-41550.	595
2	Chen et al. (2004). Crime data mining: A general framework and some examples. *Computer, 37*(4), 50-56.	251
3	Holt & Bossler (2009). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behaviour, 30*(1), 1-25.	237
4	Reyns et al. (2011). Being Pursued Online Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.	228
5	Al-garadr et al. (2016). Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. *Computers in Human Behavior, 63*, 433-443.	187
6	Vinayakumar et al. (2019). Robust Intelligent Malware Detection Using Deep Learning. *IEEE Access, 7*, 46717-46738.	173

7	Leukfeldt & Yar (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263-280.	170
8	Osanaiye et al. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking, 130.*	169
9	Yaqoob et al. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems – The International Journal of eScience, 92*, 265-275.	146
10	Martin (2014). Lost on the *Silk Road*: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice, 14*(3), 351-367.	138

Discussion

Given the recent spike in cybercrime related research, this research sought to develop a more nuanced understanding of the current state of cybercrime literature through a bibliographic analysis. The analysis aimed to better understand key issues in order to further advance the research in the field. The research identified the most prolific and impactful authors, journals and countries of cybercrime related research, evaluated keyword co-occurrence to determine the future direction of the field and considered the most influential research during the period under review.

The results suggest that the growth of attention in cybercrime-related research is far-reaching, with interest stemming from multiple academic fields including the social science domain. The recent interest in the field has seen the number of publications grow substantially since 2020, with a continued upward trajectory noted each year. This aligns with the increasing prevalence of cybercriminal activities that organizations are working to protect themselves against stemming from the rapid shift to online behavior during and post-pandemic. Research conducted by PwC in 2022 identified cybercrime as the single biggest threat to small, medium and large organizations following a considerable increase in hacking – with 46% of organizations experiencing some kind of cybercrime within the previous two-year period[11]. The continued formalization of organized crime groups in the digital space has resulted in enhanced collaboration, resulting in more frequent and more sophisticated cybercriminal activity[12]. The recent growth in cybercrime-related scholarly literature is indicative of the scale and the threat posed by these criminal activities.

The research further suggests that there is evidence of cross-country collaboration in cybercrime-related literature, suggesting the global importance of the phenomenon. The leading journal for cybercrime articles, *IEEE Access,* is a multidisciplinary journal, with a number of other top publishing and cited journals being in the field of criminology. Despite the technological nature of cybercrime research, there is a noted absence of the top information systems (IS) journals as publishers of cybercrime research in the dataset. This may be due to the rapid expansion of interest in the field as it impacts a host of other disciplines which appear to be dominating the discourse. However, in many cases the technology of a discipline is able to change and redefine a discipline and the rapid pace of technological change that has resulted in the growth of cybercriminal activities warrants further investigation from IS scholars and publication outlets. It is likely that this will change in the future as we start to see topics such as artificial intelligence, blockchain and

the internet of things (IoT) appearing in the cybercrime literature. This already appears to some extent as a research cluster in Figure 3 - however we are likely to see further research examining the cybersecurity impacts of new technologies as they come to the fore. The keyword co-occurrence analysis identified three further trends in the research considering the drivers of cybercrime, the outcomes and potential effects of cybercrime and finally, factors that may impact exposure to cybercrime. These trends represent critical knowledge areas for CISOs seeking to safeguard an organization's digital assets. Expanding on these trends, we predict that future research will also consider the organizational impact and importance of the CISO together with considerations of their role within the executive structure.

Conclusion

In sum, this research sought to explore the knowledge structure of cybercrime research through a bibliographic analysis. The results offer insight into the most prolific and impactful authors, journals and countries of cybercrime research, the most influential articles and key trends in the research that represent critical knowledge areas for the CISO. The source of publications further indicates that there is widespread interest in cybercrime across diverse disciplines and geographies – which is indicative of the scope of the phenomenon globally. The limitations of this research primarily relate to the use of a single database and the restrictions placed on research outputs to be included in the dataset, as this may have excluded cybercrime related research published via other avenues, such as industry reports or book chapters. Given the rapid pace of technological change, it would be beneficial for future researchers to revisit the bibliographic analysis within a year to identify the further development of the field, to examine the continued growth and/or change of the four noted trends in the literature, and to expand the dataset to potentially incorporate practitioner-oriented publications.

References

1. Morgan, S. (2020). "Cybercrime To cost the world $10.5 trillion annually by 2025", https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Accessed 2024 February 25).
2. Moschetta, G., Beato, F., and Joshi, A. (2023). "Cybersecurity in this era of polycrisis. World Economic Forum", https://www.weforum.org/agenda/2023/02/cybersecurity-in-an-era-of-polycrisis/ (Accessed 2024 February 25).
3. Das, S., and Nayak, T. (2013). "Impact of cybercrime: issues and challenges," *International Journal of Engineering Sciences & Emerging Technologies,* vol. 6 no. 2, pp. 142-153.
4. Wall, D. (2005). The internet as a conduit for criminal activity. In: Pattavina, A. (Ed.), *Information Technology and the Criminal Justice System.* Sage Publications: USA.
5. Jahankhani, H., Al-Nemrat, A., and Hosseinian-Far, A. (2014). In: Akhgar, B., Staniforth, A., & Bosco, F. (Eds.) *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Elsevier.
6. Zandt, F. (2023). "The most prevalent forms of cybercrime", https://www.statista.com/chart/30870/share-of-worldwide-cyber-attacks-by-type/ (Accessed 2024 February 25).
7. Wainwright, R. (2019). "The ascent of the CISO", https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-the-ascent-of-the-ciso.pdf (Accessed 2024 February 25).
8. Ferreira, C. and Robertson, J. (2020), "Examining the boundaries of entrepreneurial marketing: a bibliographic analysis", *Journal of Research in Marketing and Entrepreneurship,* vol. 22 no. 2*,* pp. 161-180.
9. Van Eck, N. and Waltman, L. (2010), "Software survey: VOSViewer, a computer program for bibliometric mapping", *Scientometrics*, vol. 84 no. 2, pp. 523-538.
10. Radhakrishnan, S., Erbis, E., Isaacs, J. and Kamarthi, S. (2017), "Novel keyword co-occurrence network based methods to foster systematic reviews of scientific literature", *PLoS One*, vol. 12 no. 3, pp. 172778.
11. PwC. (2022), "Cybercrime poses biggest threat to businesses – as the impact of hackers becomes more destructive", PwC. https://www.pwc.com/bm/en/press-releases/pwcs-global-economic-crime-and-fraud-survey-2022.html#:~:text=In%20this%20year's%20survey%20results,only%2034%25%20experienced%20customer%20fraud (Accessed 2024 February 25).
12. Ellerbeck, S. (2022), "Nearly half of businesses are being hit by economic crime, with cybercrime the gravest threat. What can they do about it?" World Economic Forum. https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/ (Accessed 2024 February 24).