Crimes in the Virtual World: A Bibliometric Analysis

Ani Munirah Mohamad*

School of Law, Universiti Utara Malaysia, Sintok, Kedah, Malaysia

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.91100090

Received: 17 November 2025; Accepted: 25 November 2025; Published: 01 December 2025

ABSTRACT

The rapid expansion of digital technologies has transformed crime into new dimensions within virtual environments, making “crimes in the virtual world” a critical subject of scholarly investigation. Despite the growing number of studies, there remains a lack of comprehensive understanding of research patterns, collaboration networks, and thematic developments in this field. To address this gap, this study employs a bibliometric analysis to systematically examine existing literature and uncover knowledge structures. Data were collected using the Scopus database through an advanced search strategy, yielding a total of 1,068 documents relevant to the theme. The dataset was cleaned and harmonised using OpenRefine, followed by statistical and graphical analyses conducted through the Scopus Analyzer. Furthermore, VOSviewer software was employed to generate visualisation maps, including keyword co-occurrence networks, co-authorship collaborations, and thematic clusters. The findings reveal significant publication growth over the past decade, with notable contributions from leading countries such as India, the United States, and the United Kingdom. Keyword co-occurrence analysis highlighted dominant research foci on cybercrime, computer crime, cybersecurity, and digital forensics, while emerging topics such as artificial intelligence, blockchain, and machine learning suggest evolving interdisciplinary approaches. Co-authorship analysis demonstrated that research collaboration is concentrated among a few developed nations, although participation from emerging economies is steadily increasing. These results provide empirical evidence of the dynamic and interdisciplinary nature of virtual world crime research, emphasising both technological and socio-legal perspectives. In conclusion, this study enriches the body of knowledge by offering a structured overview of global research trends, identifying thematic strengths and gaps, and providing valuable insights for future scholarly directions, policymaking, and international collaboration in combating crimes in the virtual world.

Keywords: crimes, cybercrimes, online, virtual

INTRODUCTION

The advent of virtual worlds has revolutionised the way individuals interact, offering unprecedented opportunities for socialisation, entertainment, and commerce. However, alongside these benefits, virtual worlds have also become a breeding ground for various forms of criminal activities. Crimes in the virtual world, ranging from virtual theft and fraud to more severe offenses like virtual rape and murder, pose significant challenges to law enforcement and legal systems worldwide. This paper aims to explore the nature of crimes in virtual worlds, the motivations behind these crimes, and the implications for law enforcement and policy-making.

Virtual worlds, such as Second Life and the metaverse, have become integral parts of many people's lives, providing platforms for social interaction, business, and entertainment. However, these virtual environments are not immune to criminal activities. Crimes in virtual worlds can mirror those in the real world, including theft, fraud, and even more severe offenses like virtual rape, espionage and murder [1], [2], [3], [4]. The anonymity and lack of physical presence in virtual worlds can embolden individuals to engage in behaviors they might avoid in real life, leading to a unique set of challenges for law enforcement and legal systems [5], [6], [7].

One of the primary concerns in virtual worlds is the rise of cybercrime. As more individuals and businesses engage in virtual environments, the potential for cybercrime increases. Cybercrimes in virtual worlds can include virtual theft, fraud, privacy violations, and hacking [8], [9], [10]. These crimes can have real-world implications, as virtual property often holds significant monetary value, and the theft of such property can result in substantial financial losses for victims. Additionally, the lack of clear legal frameworks and regulations in virtual worlds complicates the prosecution and prevention of these crimes [2], [11], [12].

The psychological impact of crimes in virtual worlds is another critical area of concern. Victims of virtual crimes, such as cyberbullying, stalking, and harassment, can experience significant psychological distress, including anxiety, depression, and post-traumatic stress disorder (PTSD) [13], [14], [15]. The immersive nature of virtual worlds can exacerbate these effects, as the experiences can feel very real to the victims [3], [16]. Studies have shown that involvement in cyberbullying, whether as a victim or perpetrator, can lead to greater psychological suffering, highlighting the need for effective prevention and intervention strategies [15].

Law enforcement faces significant challenges in addressing crimes in virtual worlds. Traditional methods of investigation and prosecution may not be effective in these environments, necessitating new approaches and legal frameworks. For example, undercover operations in virtual worlds require adaptations to existing legal procedures to balance the need for effective investigations with the protection of individuals' rights to privacy and fair trial. Additionally, the global nature of virtual worlds complicates jurisdictional issues, as crimes can be committed across international borders, further challenging law enforcement efforts [12], [17].

Accordingly, crimes in virtual worlds present a complex and evolving challenge for law enforcement, legal systems, and society as a whole. The anonymity and lack of physical presence in these environments can lead to a range of criminal activities, from virtual theft and fraud to more severe offenses like virtual rape and murder. The psychological impact on victims can be profound, necessitating effective prevention and intervention strategies. Law enforcement must adapt to the unique challenges of investigating and prosecuting crimes in virtual worlds, including addressing jurisdictional issues and developing new legal frameworks. As virtual worlds continue to grow in popularity and complexity, ongoing research and collaboration between policymakers, law enforcement, and technology developers will be essential to address these challenges and ensure the safety and security of virtual environments.

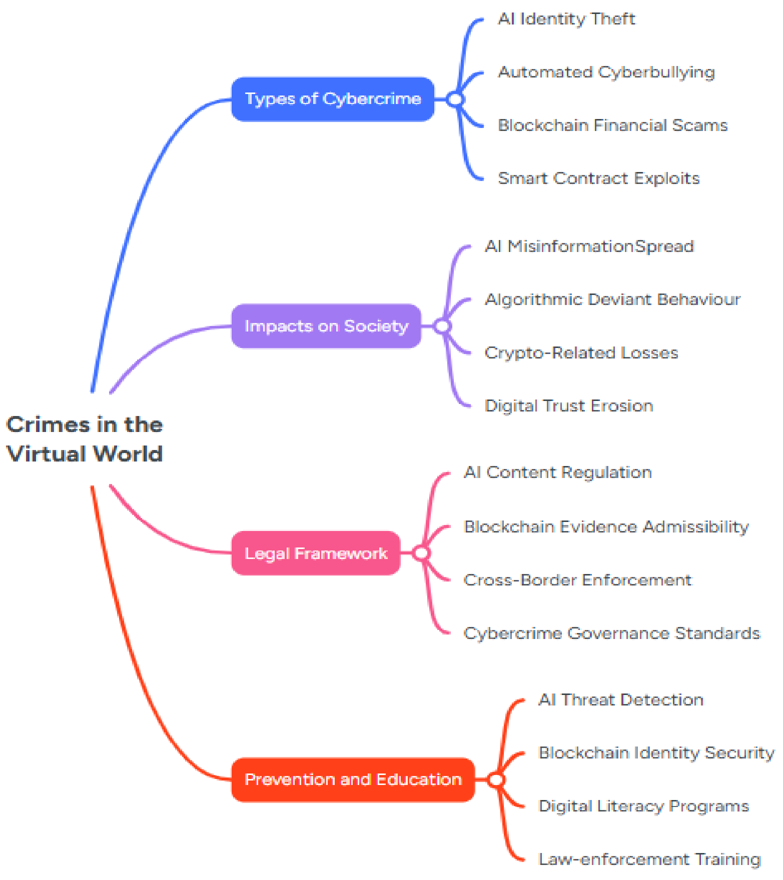

Figure 1. Key concepts generated on crimes in the virtual world

Figure 1 illustrates a concept map that comprises four main themes supported by sixteen condensed concepts, each chosen to capture the essential dynamics of contemporary virtual crimes shaped by artificial intelligence and blockchain technologies. The first theme on types of cybercrime highlights core offence patterns, including AI identity fraud, automated cyberbullying, blockchain financial scams, and smart-contract exploits, reflecting the technological drivers behind modern illicit activity. The second theme focuses on societal impacts, addressing how AI misinformation, algorithmic deviant behaviour, crypto-related losses, and digital trust erosion collectively undermine social stability and economic resilience. The third theme outlines the legal framework, emphasising the necessity of regulating AI content, ensuring blockchain evidence admissibility, strengthening cross-border enforcement mechanisms, and advancing coherent cybercrime governance standards. The final theme concerns prevention and education, underscoring the importance of AI threat detection, blockchain-based identity security, digital literacy programmes, and improved law-enforcement training. Together, these themes and concepts present a structured rationale for understanding the evolving landscape of virtual crimes, demonstrating the interplay between emerging technologies, their misuse, and the corresponding regulatory and preventive responses required.

As can be seen, crimes in the virtual world present multifaceted challenges that require a comprehensive understanding of their nature, impact, and prevention. The integration of virtual spaces into daily life necessitates a multidisciplinary approach to address the legal, regulatory, and technological aspects of virtual crimes. As society continues to embrace virtual environments, it is imperative to develop robust legal frameworks, enhance cybersecurity measures, and implement targeted prevention programs to mitigate the adverse effects of virtual crimes. By doing so, we can ensure that the benefits of virtual worlds are maximised while minimising the risks associated with criminal activities in these spaces.

Research Questions

This study investigates the following five research questions:

RQ1: What are the research trends of crimes in the virtual world according to the year of publication?

RQ2: What are the top 10 cited articles of crimes in the virtual world?

RQ3: Which are the top 10 countries on crimes in the virtual world based on number of publication?

RQ4: What are the popular keywords related to crimes in the virtual world?

RQ5: What are co-authorship by countries' collaboration of crimes in the virtual world?

METHODOLOGY

Bibliometrics constitutes a systematic approach to the collection, organisation, and evaluation of bibliographic data derived from scientific publications [18], [19], [20]. Rather than being confined to descriptive statistics - such as identifying the distribution of journals, temporal trends, and leading authors [21], bibliometric analysis extends to advanced techniques, including document co-citation analysis, which enables the mapping of intellectual structures within a research domain. The execution of a rigorous literature review, therefore, necessitates an iterative and methodical process of keyword selection, literature retrieval, and critical assessment, ultimately yielding a comprehensive bibliography and robust analytical outcomes [22]. Guided by this rationale, the present study concentrated on high-impact publications, recognising their pivotal role in illuminating the theoretical foundations that underpin the field. To ensure reliability and precision, SCOPUS was employed as the principal data source [23], [24], [25]. given its extensive coverage and established credibility in scholarly research. Accordingly, publications indexed in Elsevier's Scopus database from 2010 through 2025 were systematically retrieved and analysed.

Data search strategy

For this study, the Scopus database was selected as the principal source of data collection due to its broad disciplinary coverage, reliable indexing of peer-reviewed materials, and established credibility in bibliometric research. To ensure accuracy and relevance, the advanced search function in Scopus was employed, using the following search string as shown in **Table 1**: TITLE ((crime) AND (technology OR cloud OR virtual OR cyber OR online)) AND PUBYEAR > 2009 AND PUBYEAR < 2026 AND (LIMIT-TO (LANGUAGE , "English")). This query was specifically designed to capture publications focusing on crimes in relation to technological, cyber, virtual, online, and cloud-based contexts, with the initial number of documents to be 1,348. To maintain temporal relevance, the search was restricted to publications appearing between 2010 and 2025, a period that corresponds with the rapid proliferation of cloud technologies, digital platforms, and cyber environments that have redefined both the nature of criminal activity and scholarly inquiry.

In addition, to ensure consistency and accessibility of interpretation, the language criterion was limited to English, while non-English studies were excluded to prevent issues of translation bias and uneven accessibility. This filtering process was guided by explicit inclusion and exclusion criteria as shown in **Table 2**. The inclusion parameters allowed English-language works published within 2010–2025 that addressed crime in technologically mediated contexts, while the exclusion parameters systematically removed publications before 2010 or written in non-English languages. The access date of the search was October 2025, an important step in maintaining transparency and reproducibility since bibliographic databases are continuously updated with newly indexed publications. Following the application of these filters, a total of 1,068 documents were retrieved, forming the final dataset for analysis. This volume of literature demonstrates both the scholarly significance of the topic and the interdisciplinary interest it generates across fields such as criminology, law, computer science, sociology, and information technology. Ultimately, by employing a structured and transparent search strategy, supported by well-defined screening criteria, the study constructed a robust bibliometric dataset that balances breadth with precision.

Table 1. The search string

Source	**Search string**
Scopus	TITLE ((crime) AND (technology OR cloud OR virtual OR cyber OR online)) AND PUBYEAR > 2009 AND PUBYEAR < 2026 AND (LIMIT-TO (LANGUAGE , "English")) Access date: October 2025

Table 2. The selection criterion of searching

Criterion	Inclusion	Exclusion
Language	English	Non-English
Timeline	2010 – 2025	< 2010 > 2025

Data analysis

VOSviewer, developed by Nees Jan van Eck and Ludo Waltman at Leiden University, the Netherlands [26], [27] is a widely recognised bibliometric software designed for the visualisation and analysis of scientific literature. Renowned for its intuitive and interactive interface, the software facilitates the construction of sophisticated network visualisations, clustering analyses, and density maps, thereby enabling scholars to discern structural patterns and intellectual linkages within complex research domains. Its versatility extends to the mapping of co-authorship, co-citation, and keyword co-occurrence networks, offering comprehensive insights into the dynamics of scholarly communication. Continuous updates and methodological refinements further enhance its analytical robustness, ensuring that both novice and advanced researchers can engage effectively with large-scale bibliometric datasets. The software's capacity to compute a wide range of metrics, customise visual outputs, and integrate seamlessly with multiple bibliometric data sources positions VOSviewer as an indispensable tool for advancing knowledge mapping and research evaluation.

A distinctive strength of VOSviewer lies in its ability to transform highly intricate bibliometric datasets into visually interpretable maps and charts, enabling the detection of keyword co-occurrence patterns, thematic clusters, and citation linkages. Unlike traditional bibliometric software, VOSviewer combines methodological rigor with accessibility, thus broadening its applicability across disciplinary boundaries. Its adaptability, combined with a focus on network visualisation and density mapping, ensures that research landscapes are represented with precision and analytical clarity. The sustained development of VOSviewer has secured its position at the forefront of bibliometric analysis, with customisable functionalities that provide scholars with both depth and flexibility in exploring research frontiers.

For the present study, bibliometric datasets comprising publication year, title, author name, journal, citation count, and keywords were retrieved in PlainText format from the Scopus database, covering the period from 2010 through October 2025. These datasets were processed using VOSviewer version 1.6.20, where clustering and mapping techniques were applied to generate comprehensive knowledge maps. Methodologically, VOSviewer provides an alternative to the Multidimensional Scaling (MDS) approach by situating items within low-dimensional spaces such that the proximity of items reflects their degree of relatedness and similarity [26]**.** While sharing conceptual similarities with MDS [28]**.** VOSviewer diverges by adopting a more refined normalisation technique for co-occurrence frequencies, namely the association strength (ASij), which is calculated as [29]**:**

$$AS_{ij} = \frac{C_{ij}}{w_i w_j}$$

where *Cij* denotes the observed co-occurrence of items *i* and *j*, and w_i and w_j represent their respective occurrence frequencies. This metric is proportional to the ratio between the observed and the expected number of co-occurrences under the assumption of statistical independence [29]. Through this methodological innovation, VOSviewer enhances the precision of bibliometric mapping, making it a superior tool for uncovering the latent structures underpinning scholarly domains.

FINDINGS AND DISCUSSION

This section deliberates on each of the five research questions of the study.

Research Question 1: What are the research trends of crimes in the virtual world according to the year of publication?

The publication trend on “crimes in the virtual world” between 2010 and 2025 demonstrates a gradual but fluctuating growth in scholarly attention as shown in **Figure 2**.

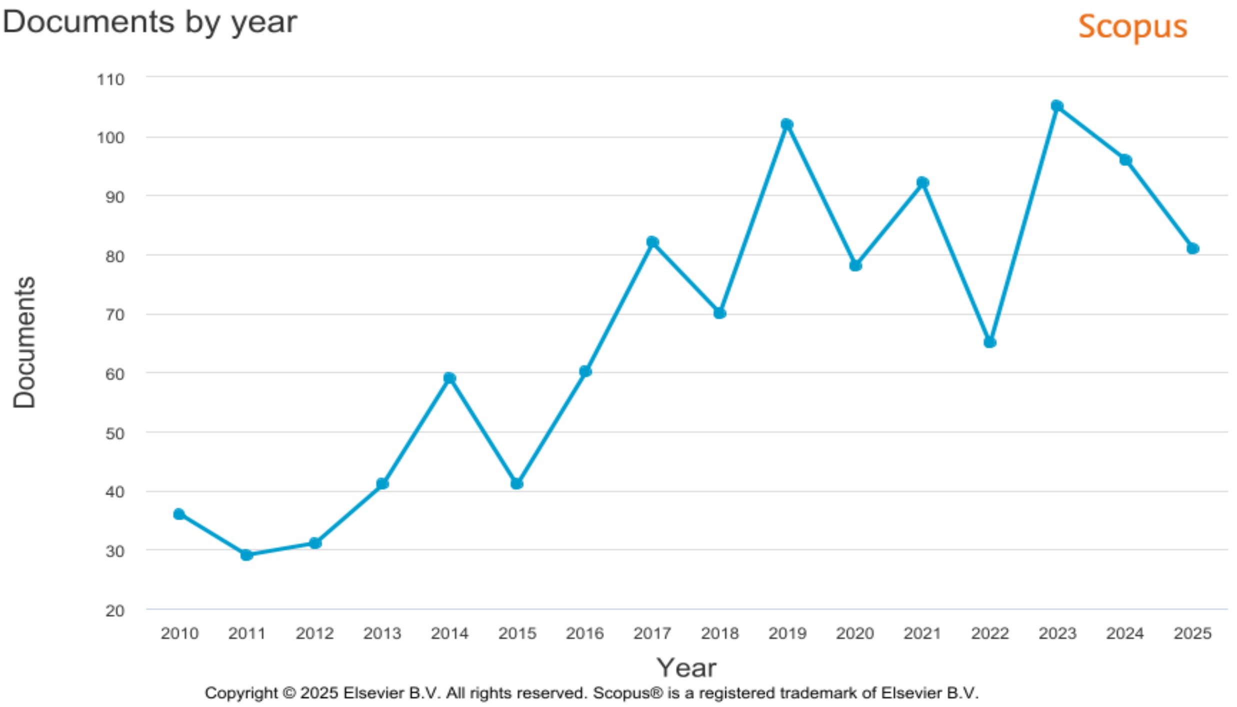

Figure 2. Publication trend by year of publication

In the early years, research output was relatively low, with fewer than 40 documents annually between 2010 and 2012. A slight increase began in 2013 (41 documents), followed by a notable jump in 2014 (59 documents), reflecting the growing recognition of cybercrime as a global issue. However, this momentum temporarily slowed in 2015 (41 documents) before picking up again from 2016 onwards. By 2017, publications had risen to 82, and the output surged further in 2019, reaching 102 documents, this is a clear indication of the field's growing importance. While there were dips in 2018 (70 documents) and 2020 (78 documents), the broader trend reflects consistent academic interest, culminating in the peak of 105 publications in 2023.

The reasons behind this pattern are closely tied to technological and societal developments. The significant rise after 2016 corresponds with increasing global concerns over ransomware, financial cybercrimes, and dark web activities. The peak in 2019 can be linked to worldwide debates on digital privacy and high-profile cyber incidents, which likely spurred scholarly research. Similarly, the COVID-19 pandemic in 2020–2021 heightened digital dependency, encouraging studies on vulnerabilities in online platforms, which explains the sustained high numbers during these years. The sharp increase in 2023 coincides with emerging challenges such as AI-driven cybercrime, cryptocurrency fraud, and the governance of virtual environments like the metaverse. The decline in 2024 (96 documents) and 2025 (81 documents) may suggest a consolidation of research, with scholars focusing on more specialised sub-fields rather than producing broader exploratory studies. Overall, the trend underscores how the evolution of digital technologies continues to shape academic discourse on virtual world crimes.

Research Question 2: What are the top 10 cited articles of crimes in the virtual world?

Produced below in **Table 3** is the list of top 10 cited articles on the topic of crimes in the virtual world.

Table 3: Top 10 cited articles

Authors	Title	Year	Source title	Citation count
H.S., Singh Lallie, Harjinder Singh; L.A., Shepherd, Lynsay A.; J.R., Nurse, Jason R.C.; A., Erola, Arnau; G., Epiphaniou, Gregory; C.R., Maple, Carsten R.; X.A., Bellekens, Xavier A.	Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic	2021	Computers and Security	401
A., Hutchings, Alice; T.J., Holt, Thomas J.	A crime script analysis of the online stolen data market	2015	British Journal of Criminology	175
S., Brayne, Sarah; A., Christin, Angéle	Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts	2021	Social Problems	171
U., Buck, Ursula; S., Naether, Silvio; B., Räss, Beat; C., Jackowski, Christian; M.J., Thali, Michael Josef	Accident or homicide - Virtual crime scene reconstruction using 3D methods	2013	Forensic Science International	156
R.G., Broadhurst, Roderic G.; P.N., Grabosky, Peter N.; M., Alazab, Mamoun; S., Chon, Steve	Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime	2014	International Journal of Cyber Criminology	137
S.P., Roche, Sean Patrick; J.T., Pickett, Justin T.; M.G., Gertz, Marc G.	The Scary World of Online News? Internet News Exposure and Public Attitudes Toward Crime and Justice	2016	Journal of Quantitative Criminology	119
J.C.F., Chan, Jason C.F.; A., Ghose, Anindya; R.C., Seamans, Robert C.	The internet and racial hate crime: Offline spillovers from online access	2016	MIS Quarterly: Management Information Systems	115

I., Awan, Imran; I., Zempi, Irene	The affinity between online and offline anti-Muslim hate crime: Dynamics and impacts	2016	Aggression and Violent Behavior	108
D., Maimon, David; E.R., Louderback, Eric R.	Cyber-Dependent Crimes: An Interdisciplinary Review	2019	Annual Review of Criminology	102
C.S.D., Brown, Cameron S.D.	Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice	2015	International Journal of Cyber Criminology	102

The citation analysis of the top ten most cited papers on crimes in the virtual world highlights several key trends in scholarly attention and impact. The most cited article, Cyber security in the age of COVID-19 by [30], with 401 citations, reflects how the global pandemic significantly accelerated both cybercrime incidents and research interest, making it a foundational reference point for subsequent studies. Other highly cited works, such as [31] and [32], focus on the online stolen data market and algorithmic crime prediction in policing, respectively. Their strong citation counts (175 and 171) suggest the academic and policy relevance of these topics, as they directly address the intersection of technology, law enforcement, and criminal markets. Classic works such as [33] on virtual crime scene reconstruction and [34] on organised cybercrime groups also remain influential, pointing to the importance of both methodological innovation and understanding criminal networks in cyberspace.

The distribution of citations across themes reveals the drivers of scholarly impact in this field. Papers linked to timely global issues, such as COVID-19 cyber-attacks or online hate crimes tend to attract higher citations because of their immediate policy and social relevance. Studies that integrate interdisciplinary perspectives, such as criminology, computer science, and sociology, also achieve higher visibility, as seen in [35] review on cyber-dependent crimes. Furthermore, publications in high-impact journals like Computers and Security, MIS Quarterly, and the British Journal of Criminology provide wider reach and recognition, contributing to greater citation rates. Overall, the results show that scholarly impact in virtual crime research is driven by topical urgency, interdisciplinary framing, and publication in well-established journals that bridge academic, technical, and policy audiences.

Research Question 3: Which are the top 10 countries on crimes in the virtual world based on number of publication?

The following **Figure 3** reveals the top 10 countries based on number of publication in the area of crimes in the virtual world.

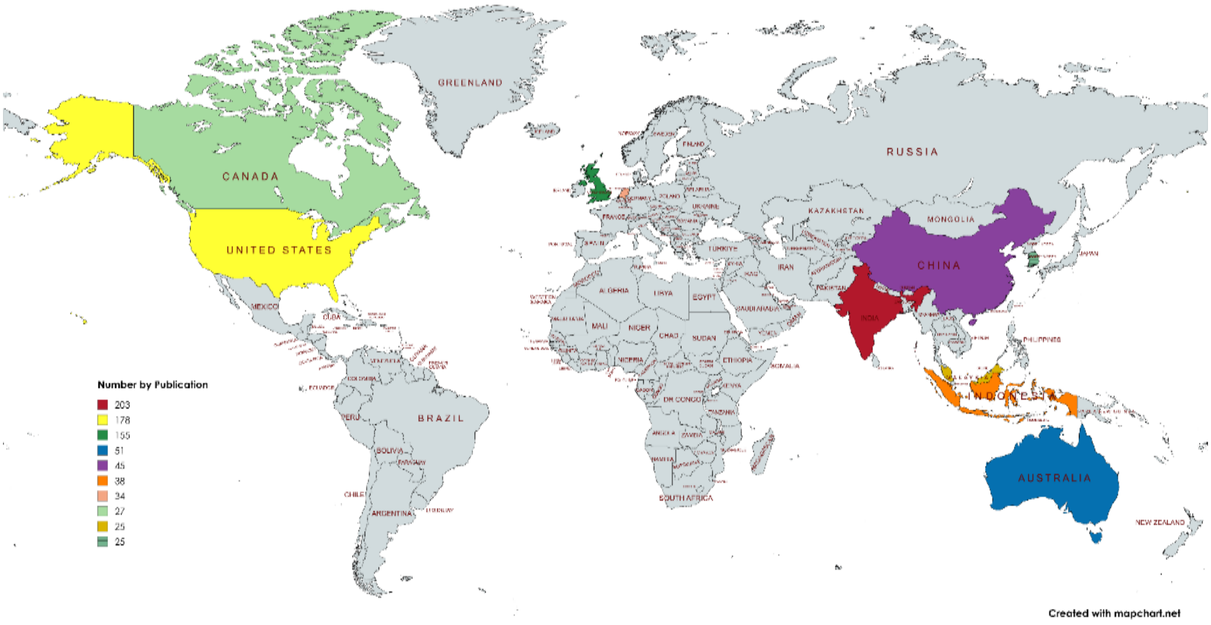

Figure 3. Top 10 countries based on number of publications

The bibliometric data shows that India (203), the United States (178), and the United Kingdom (155) dominate research output on crimes in the virtual world, significantly outpacing other countries. This trend reflects not only the academic capacity and research culture of these nations but also the pressing relevance of cybercrime in their contexts. India's lead can be attributed to its rapidly growing digital economy, high internet penetration, and increasing incidents of cyber fraud and online crime, which drive both government and academic focus on virtual crime research. Similarly, the United States and the United Kingdom are global technology hubs with advanced legal, technological, and cybersecurity frameworks, making cybercrime a priority research area for their universities, policy think tanks, and legal scholars.

The moderate output from Australia (51) and China (45), followed by Indonesia (38), the Netherlands (34), and Canada (27), highlights regional diversity in the research landscape. For countries like China and Indonesia, rapid digitalisation coupled with evolving legal infrastructures has spurred growing academic interest in addressing virtual crimes. Meanwhile, smaller but technologically advanced nations such as the Netherlands and South Korea (25) maintain a specialised focus, often tied to cybersecurity innovation and international collaborations. Malaysia's contribution (25) is also noteworthy, reflecting increasing government and academic initiatives to address cybercrime challenges in Southeast Asia. Overall, the distribution suggests that publication volume is shaped by a combination of factors: the scale of digital adoption, prevalence of cyber threats, research infrastructure, and national policy priorities in combating virtual world crimes.

Research Question 4: What are the popular keywords related to crimes in the virtual world?

The following **Figure 4** highlights the main keywords used by the authors related to the study of crimes in the virtual world.

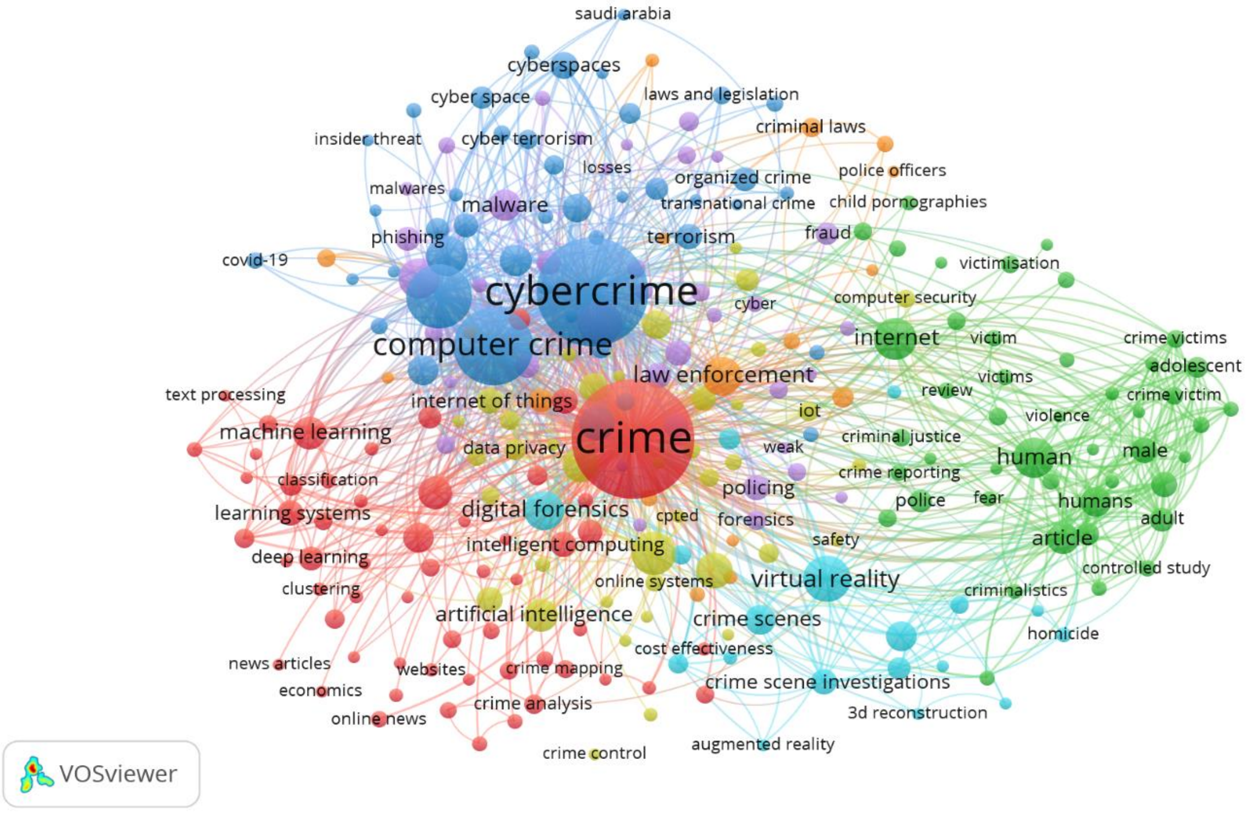

Figure 4: Network visualisation map of keywords' co-occurrence

Co-occurrence analysis of author keywords using VOSviewer is a bibliometric technique that identifies how frequently keywords appear together across publications, thereby revealing thematic structures, trends, and research linkages in a particular field. In this case, the analysis was generated using the full counting method, with a minimum occurrence threshold of 5, which means only keywords that appeared at least five times were included. From the total 3,915 keywords, 259 met the threshold, and with the additional criterion of a minimum cluster size of 5, the software generated 7 clusters. These clusters visually map the intellectual structure of research on crimes in the virtual world, showing central keywords like “crime” (406 occurrences, 2,419 link strength) and “cybercrime” (335 occurrences, 1,596 link strength), alongside interconnected terms such as “cyber security,” “digital forensics,” and “law enforcement.” The clustering reflects thematic concentrations, where closely related concepts are grouped together, highlighting the multidisciplinary intersections of criminology, technology, and law.

The findings contribute to the body of knowledge by offering a structured understanding of how research themes evolve and interact in the digital crime domain. The prominence of keywords like “cybercrime,” “computer crime,” and “cyber security” underscores the centrality of technological dimensions in modern criminology. Meanwhile, emerging terms such as “machine learning,” “artificial intelligence,” “internet of things,” and “blockchain” reveal the growing influence of advanced technologies in both criminal activity and crime prevention strategies. Similarly, the presence of socio-legal terms like “law enforcement,” “crime prevention,” and “legal frameworks” reflects ongoing debates about governance, regulation, and human impact. Overall, this keyword co-occurrence analysis not only maps the landscape of current research but also signals emerging trends and interdisciplinary collaborations, guiding scholars toward gaps in literature and new research opportunities in cybercrime and virtual world studies.

Research Question 5: What are co-authorship by countries’ collaboration of crimes in the virtual world?

Produced below is **Figure 5**, depicting the network visuatisation mapping of the authors’ co-authorship collaboration by country.

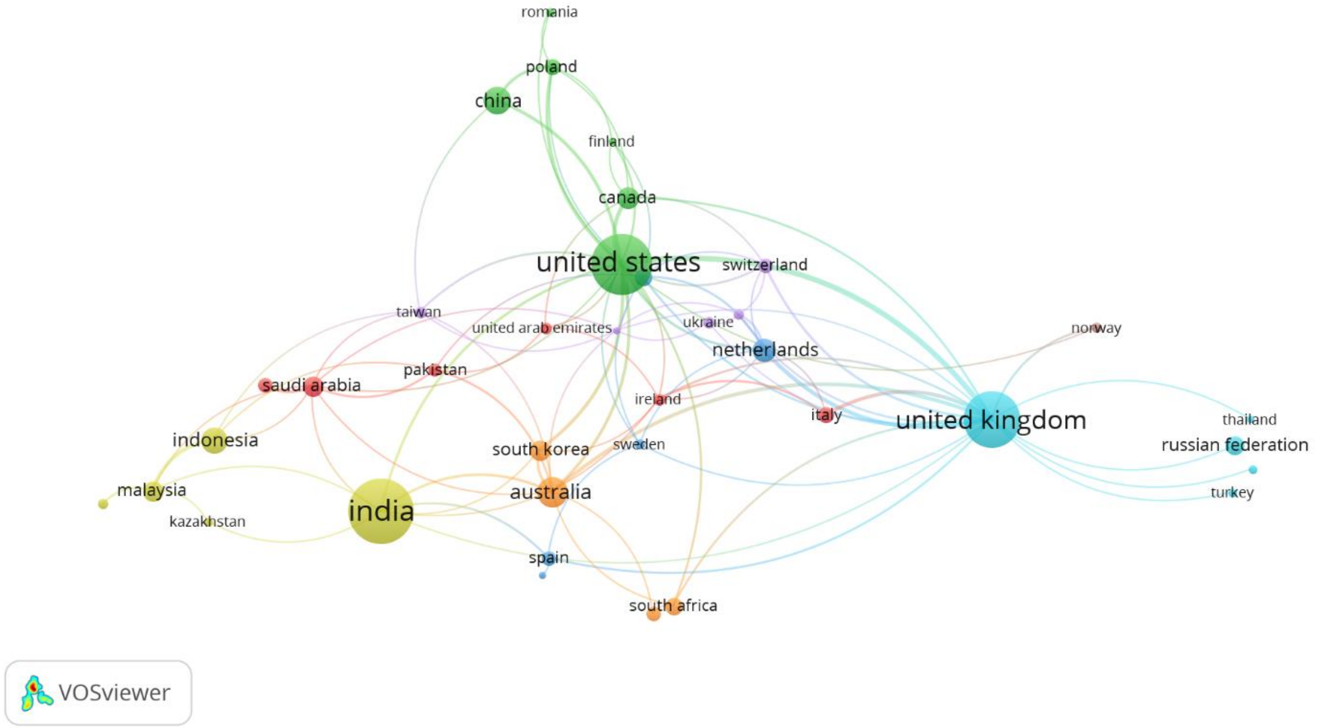

Figure 5. Network visualisation map of authors’ collaboration by country

Co-authorship by country collaboration analysis in VOSviewer is a bibliometric mapping method that identifies research partnerships among countries based on joint publications. It shows which countries are most interconnected in producing scholarly work, with stronger links reflecting more frequent or impactful collaborations. In this case, the analysis used the full counting method, where each co-authorship counts equally, with a minimum threshold of 5 documents per country. Out of 97 countries, 37 met the threshold, and by applying a minimum cluster size of 5, the software grouped them into 8 clusters. These clusters visualise global research collaboration patterns, where countries such as the United States (177 documents, 2,872 citations, link strength 62), the United Kingdom (154 documents, 2,289 citations, link strength 58), and Australia (52 documents, 779 citations, link strength 23) emerge as central players in international scholarly networks, forming hubs of intellectual exchange.

The findings contribute to the body of knowledge by showing how research on crime in the virtual world is shaped by global collaboration rather than isolated efforts. The dominance of Western countries (United States, United Kingdom, Netherlands, Australia) suggests they are leading in resources, funding, and international partnerships, while emerging economies like India (201 documents, 1,100 citations) and Malaysia (25 documents, 133 citations) reflect growing regional contributions, though with relatively lower citation impact and collaboration strength. The clustering also highlights multi-regional connections, such as Asia–Europe linkages (India, China, Malaysia with European partners) and Middle Eastern collaborations (Saudi Arabia, UAE). This visualisation not only underscores existing disparities in global knowledge production but also identifies opportunities for strengthening South–South cooperation. By revealing central hubs and peripheral contributors, the analysis guides policymakers and academics to enhance inclusive international collaboration and balance knowledge exchange in digital crime research.

CONCLUSION

This study set out to examine the scholarly landscape of crimes in the virtual world by conducting a bibliometric analysis of publications indexed between 2010 and 2025. The main purpose was to identify research trends, leading contributions, geographical distribution of scholarship, influential keywords, and patterns of international collaboration. By addressing these questions, the analysis provides a structured overview of how the study of virtual world crimes has evolved and where it is heading.

The results reveal that research on this subject has steadily increased over the past decade, with peak productivity occurring in 2023. Highly cited works largely reflect responses to pressing global developments, including the rise of cybercrime during the COVID-19 pandemic, the growth of online hate speech, and the use of predictive algorithms in law enforcement. In terms of geography, India, the United States, and the United Kingdom emerge as leading contributors, with other regions such as Southeast Asia and China showing growing engagement. Keyword co-occurrence analysis highlights the dominance of themes such as cybercrime, cybersecurity, and digital forensics, while newer concepts like artificial intelligence, blockchain, and the metaverse signal emerging interdisciplinary directions. Collaboration patterns demonstrate strong research hubs in developed countries, with gradual expansion of contributions from developing economies.

This research contributes to the field by offering empirical evidence of both the maturity and gaps in scholarship. It enriches existing literature by mapping knowledge structures, identifying dominant themes, and highlighting underexplored areas, such as socio-psychological impacts of virtual crime and the development of robust legal frameworks. For policymakers and practitioners, these findings underscore the need for cross-border collaboration, enhanced cybersecurity strategies, and regulatory innovations to address evolving threats in digital environments.

Nonetheless, the study is limited by its reliance on a single database, the exclusion of non-English publications, and the inability to capture very recent works beyond the data collection period. Future research could broaden the scope by incorporating multiple databases, examining non-English literature, and integrating qualitative approaches to capture nuanced dimensions of virtual world crimes. Expanding collaboration among regions currently underrepresented in the dataset would also strengthen the global dialogue on this issue.

In closing, this bibliometric study demonstrates the importance of systematic mapping in understanding how academic inquiry adapts to the challenges posed by digital crime. By revealing trends, gaps, and emerging directions, the analysis not only consolidates knowledge but also sets a foundation for future research and practice. The significance of this work lies in showing that crimes in virtual environments cannot be addressed solely within technical or legal silos but must be approached through an interdisciplinary and collaborative lens to ensure resilience in the face of evolving digital threats.

ACKNOWLEDGMENT

The author would like to express gratitude to Dr. Wan Azani Mustafa for providing guidance and insights in completing this paper, and to Universiti Utara Malaysia for the resources necessary in finalising this paper.

REFERENCES

1. T. Gorrindo and J. E. Groves, “Crime and hate in virtual worlds: A new playground for the Id,” Harv. Rev. Psychiatry, vol. 18, no. 2, pp. 113–118, 2010, doi: 10.3109/10673221003683937.
2. A. Guinchard, “Crime in virtual worlds: The limits of criminal law,” Int. Rev. Law, Comput. Technol., vol. 24, no. 2, pp. 175–182, 2010, doi: 10.1080/13600861003748284.
3. E. Haber, “The Criminal Metaverse,” Indiana Law J., vol. 99, no. 3, pp. 843–891, 2024, [Online]. Available:https://www.scopus.com/inward/record.uri?eid=2-s2.0-85197465131&partnerID=40&md5=b5a2fa27e91eaf7f73fbfd95019b89cf
4. W. R. W. Rosli, S. Kamaruddin, A. M. Mohamad, N. N. M. Saufi, and Z. Hamin, “Governing Cyber Espionage Threats via the Integration of the Risk Society-Cyber Securitisation Theory,” in 3rd IEEE International Virtual Conference on Innovations in Power and Advanced Computing Technologies, i-PACT 2021, Universiti Teknologi, MARA, Faculty of Law, Selangor, Malaysia: Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/i-PACT52855.2021.9696812.
5. C. Barbieri, I. Grattagliano, and R. Catanesi, “Crimes without a body: reflections on a case series of online crimes,” Forensic Sci. Res., vol. 8, no. 4, pp. 328–331, 2023, doi: 10.1093/fsr/owad035.
6. M. Boskovic, G. Misev, and N. Putnik, Analyzing New Forms of Social Disorders in Modern Virtual Environments. 2023. doi: 10.4018/978-1-6684-5760-3.
7. S. Lakhani, “Perspectives on Internet-Based Crimes,” in Criminal Psychology and the Criminal Justice System in India and Beyond, 2021, pp. 145–153. doi: 10.1007/978-981-16-4570-9_9.
8. A. Bhardwaj, “Navigating the metaverse: Forecasting cybercrime in the new age of virtual reality,” in Forecasting Cyber Crimes in the Age of the Metaverse, 2023, pp. 33–65. doi: 10.4018/9798369302200.ch003.
9. S. D. Keene, “Emerging threats&colon; financial crime in the virtual world,” J. Money Laund. Control, vol. 15, no. 1, pp. 25–37, 2011, doi: 10.1108/13685201211194718.
10. [10] N. C. Patterson and M. Hobbs, “A multidiscipline approach to governing virtual property theft in virtual worlds,” in IFIP Advances in Information and Communication Technology, 2010, pp. 161–171. doi: 10.1007/978-3-642-15479-9_15.
11. C. Chambers, “Can you ever regulate the virtual world against economic crime?,” J. Int. Commer. Law Technol., vol. 7, no. 4, pp. 339–349, 2012, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84867182025&partnerID=40&md5=e3ead851846a4080b48a6b7d0093427c
12. H. X. Qin, Y. Wang, and P. Hui, “Identity, crimes, and law enforcement in the Metaverse,” Humanit. Soc. Sci. Commun., vol. 12, no. 1, 2025, doi: 10.1057/s41599-024-04266-w.
13. G. C. López, A. D. de la Rosa Gómez, R. D. Figueroa, and X. D. Baca, “Virtual reality exposure for trauma and stress-related disorders for city violence crime victims,” in Technology, Rehabilitation and Empowerment of People with Special Needs, 2015, pp. 61–72. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84958597023&partnerID=40&md5=1ba19251d11b6f710d0af6fd5ec1238a
14. A. Palassis, C. P. Speelman, and J. A. Pooley, “An Exploration of the Psychological Impact of Hacking Victimization,” SAGE Open, vol. 11, no. 4, 2021, doi: 10.1177/21582440211061556.
15. [15] R. V. D. S. Silva, H. S. Dias Moura, P. N. A. Betetti, F. L. D. Santos, and C. M. Fortuna, “Virtual Violence as a Contributing Factor to the Mental Health of Young People: A Scoping Review,” Can. J. Nurs. Res., 2025, doi: 10.1177/08445621251364528.
16. [16] N. K. Singh, R. K. Ray, N. Silayach, D. P. Dash, and A. Singh, “Avatars at risk: Exploring public response to sexual violence in immersive digital spaces,” Comput. Human Behav., vol. 163, 2025, doi: 10.1016/j.chb.2024.108500.
17. [17] R. Rice, “Augmented reality tools for enhanced forensics simulations and crime scene analysis,” in Working Through Synthetic Worlds, 2012, pp. 201–213. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84938073815&partnerID=40&md5=841c4316c34c9b3a5b27c4600ca51ddc
18. [18] J. L. Alves, I. B. Borges, and J. De Nadae, “Sustainability in complex projects of civil construction: Bibliometric and bibliographic review,” Gest. e Prod., vol. 28, no. 4, 2021, doi: 10.1590/1806-9649-2020v28e5389.
19. D. S. Assyakur and E. M. Rosa, “Spiritual Leadership in Healthcare: A Bibliometric Analysis,” J. Aisyah

J. Ilmu Kesehat., vol. 7, no. 2, 2022, doi: 10.30604/jika.v7i2.914.

20. A. Verbeek, K. Debackere, M. Luwel, and E. Zimmermann, “Measuring progress and evolution in science and technology - I: The multiple uses of bibliometric indicators,” Int. J. Manag. Rev., vol. 4, no. 2, pp. 179–211, 2002, doi: 10.1111/1468-2370.00083.
21. Y. C. J. Wu and T. Wu, “A decade of entrepreneurship education in the Asia Pacific for future directions in theory and practice,” 2017. doi: 10.1108/MD-05-2017-0518.
22. B. Fahimnia, J. Sarkis, and H. Davarzani, “Green supply chain management: A review and bibliometric analysis,” 2015. doi: 10.1016/j.ijpe.2015.01.003.
23. A. Al-Khoury et al., “Intellectual Capital History and Trends: A Bibliometric Analysis Using Scopus Database,” Sustain., vol. 14, no. 18, 2022, doi: 10.3390/su141811615.
24. G. di Stefano, M. Peteraf, and G. Veronay, “Dynamic capabilities deconstructed: A bibliographic investigation into the origins, development, and future directions of the research domain,” Ind. Corp. Chang., vol. 19, no. 4, pp. 1187–1204, 2010, doi: 10.1093/icc/dtq027.
25. G. P. Khiste and R. R. Paithankar, “Analysis of Bibliometric term in Scopus,” Int. Res. J., vol. 01, no. 32, pp. 78–83, 2017.
26. N. J. van Eck and L. Waltman, “Software survey: VOSviewer, a computer program for bibliometric mapping,” Scientometrics, vol. 84, no. 2, pp. 523–538, 2010, doi: 10.1007/s11192-009-0146-3.
27. N. J. van Eck and L. Waltman, “Citation-based clustering of publications using CitNetExplorer and VOSviewer,” Scientometrics, vol. 111, no. 2, pp. 1053–1070, 2017, doi: 10.1007/s11192-017-2300-7.
28. F. P. Appio, F. Cesaroni, and A. Di Minin, “Visualizing the structure and bridges of the intellectual property management and strategy literature: a document co-citation analysis,” Scientometrics, vol. 101, no. 1, pp. 623–661, 2014, doi: 10.1007/s11192-014-1329-0.
29. N. J. Van Eck and L. Waltman, “Bibliometric mapping of the computational intelligence field,” in International Journal of Uncertainty, Fuzziness and Knowldege-Based Systems, 2007, pp. 625–645. doi: 10.1142/S0218488507004911.
30.]H. S. Singh Lallie et al., “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,” Comput. Secur., vol. 105, 2021, doi: 10.1016/j.cose.2021.102248.
31. A. Hutchings and T. J. Holt, “A crime script analysis of the online stolen data market,” Br. J. Criminol., vol. 55, no. 3, pp. 596–614, 2015, doi: 10.1093/bjc/azu106.
32. S. Brayne and A. Christin, “Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts,” Soc. Probl., vol. 68, no. 3, pp. 608–624, 2021, doi: 10.1093/socpro/spaa004.
33. U. Buck, S. Naether, B. Räss, C. Jackowski, and M. J. Thali, “Accident or homicide - Virtual crime scene reconstruction using 3D methods,” Forensic Sci. Int., vol. 225, no. 1–3, pp. 75–84, 2013, doi: 10.1016/j.forsciint.2012.05.015.
34. R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, “Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime,” Int. J. Cyber Criminol., vol. 8, no. 1, pp. 1–20, 2014, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84901820106&partnerID=40&md5=b28b5a91fa6e528515e3d480d1eb70df
35. D. Maimon and E. R. Louderback, “Cyber-Dependent Crimes: An Interdisciplinary Review,” Annu. Rev. Criminol., vol. 2, pp. 191–216, 2019, doi: 10.1146/annurev-criminol-032317-092057.