Three Decades of Publications on Hacking and The Law: A Bibliometric Analysis

Ani Munirah Mohamad[1]*, Zaiton Hamin[2], Mohd Bahrin Othman[2]

[1] **School of Law, Universiti Utara Malaysia, Sintok, Kedah, Malaysia**

[2] **Faculty of Law, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia**

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2026.10100127

Received: 02 January 2026; Accepted: 10 January 2026; Published: 24 January 2026

ABSTRACT

This study examines three decades of scholarly output on hacking and the law, addressing the growing need to understand how legal, regulatory and ethical dimensions of hacking have evolved in response to rapid technological change. Despite the proliferation of cybersecurity incidents and corresponding policy developments, there has been limited systematic assessment of the intellectual landscape shaping this field. To address this gap, the study employed a structured bibliometric methodology. Data were collected using Scopus advanced searching, covering publications from 1995 to 2025, yielding an initial dataset of 246 documents that was subsequently refined to 236 through the application of inclusion criteria. Statistical trends and distributional patterns were analysed using the Scopus Analyzer, while OpenRefine was used to clean, standardise and harmonise author names, keywords and source information to ensure data accuracy. VOSviewer was then applied to generate visualisations of co-authorship networks, keyword co occurrence structures and thematic clusters, enabling the identification of dominant research themes and collaborative patterns. The results demonstrate a marked increase in publication activity after 2010, with notable peaks between 2020 and 2025, and reveal substantial thematic concentration around ethical hacking, cybersecurity, penetration testing and legal governance of digital intrusions. Co-authorship mapping further highlights the central roles of the United States, India and the United Kingdom, alongside emerging contributions from Malaysia and selected European countries. The analysis shows that research in this domain is expanding, diversifying and becoming increasingly interdisciplinary. The study concludes that bibliometric insights provide a robust foundation for understanding how legal scholarship is adapting to the complexities of contemporary cyber threats and regulatory transformations, while also identifying future research directions in technology law and governance.

Keywords: hacking, cybercrime, law, legal

INTRODUCTION

The relationship between hacking and the law is a multifaceted and evolving domain that reflects the complexities of our increasingly digital world. Hacking, defined as the manipulation of software, data, computer systems, or networks without the user's knowledge and permission, constitutes a significant criminal offense [1]. However, the legal landscape surrounding hacking is not straightforward, as it involves balancing the need for cybersecurity with the protection of individual rights and freedoms. This study aims to explore the intricate interactions between hacking practices and legal frameworks, highlighting the challenges and proposing potential regulatory approaches.

The problem of hacking is exacerbated by the dual-use nature of many hacking tools, which can be employed for both legitimate and malicious purposes. This duality complicates the legal process of distinguishing between lawful and unlawful use, leading to potential overreach and unintended consequences in legal enforcement [2], [3]. Moreover, the rapid advancement of technology and the increasing availability of sophisticated hacking tools have outpaced the development of corresponding legal measures, creating a gap that cybercriminals can

exploit [4], [5]. This study is necessary to address these gaps and provide a comprehensive understanding of how hacking is regulated and how laws can be adapted to better manage the risks associated with cybercrime.

The literature on hacking and the law reveals several key concepts and themes. One significant area of focus is the ethical and cultural dimensions of hacking. Historically, hacking was associated with a culture of active access to information and a commitment to transparency and democracy [6]. However, as hacking practices have evolved, they have become increasingly dissociated from these founding ethics, leading to a more ambivalent relationship with democratic values [6][7]. This shift underscores the need for legal frameworks that can adapt to the changing nature of hacking while preserving fundamental democratic principles.

Another critical theme is the use of hacking tools by law enforcement agencies. The deployment of such tools for criminal investigations raises significant legal and ethical questions, particularly concerning privacy and human rights [8], [9], [10], [11]. For instance, the use of malware by law enforcement to access and control suspects' devices on the dark web represents a profound disruption of traditional legal norms and poses challenges for international law and cross-border investigations [10], [12]. The legal discourse must address these challenges by establishing clear guidelines and oversight mechanisms to ensure that law enforcement hacking is conducted within the bounds of the law and with respect for individual rights [1], [5].

The ambiguity in the legal definition of hacking further complicates the regulatory landscape. Different countries have varied definitions and penalties for hacking, leading to inconsistencies and legal controversies [4]. For example, the amendments to the Computer Fraud and Abuse Act (CFAA) in the United States, known as Aaron's Law, aim to reduce excessive punishment and legal ambiguity by providing more specific legislation [4]. Comparative studies of national laws can offer valuable insights into how different jurisdictions address hacking and suggest ways to harmonise legal approaches to reduce controversy and enhance legal clarity.

Accordingly, the study of hacking and the law is essential for understanding the socio-technical changes and legal challenges posed by our connected society [13]. By examining the ethical, cultural, and legal dimensions of hacking, this research aims to contribute to the development of more effective and balanced regulatory frameworks. These frameworks should protect cybersecurity while safeguarding individual rights and freedoms, ensuring that the law can keep pace with technological advancements and the evolving nature of cyber threats.

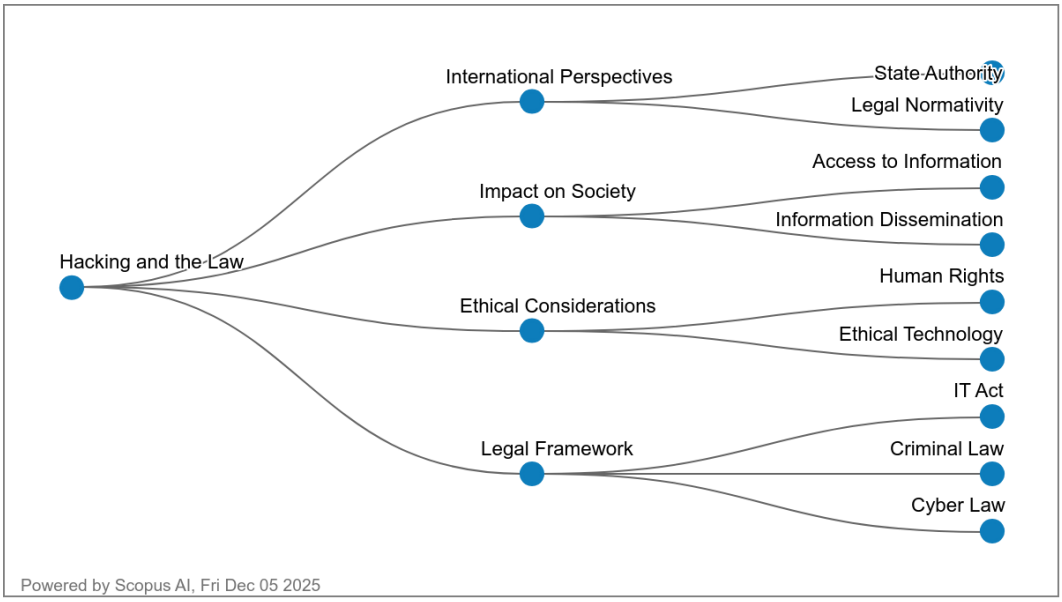

Figure 1. Key concepts generated on hacking and the law

Figure 1 shows the conceptual map on hacking and the law, which comprises four principal thematic branches, each extending into specific conceptual nodes that together illustrate nine distinct but interrelated ideas. The map begins with International Perspectives, which highlights two concepts that frame hacking within broader questions of state authority and legal normativity. The second branch, Impact on Society, contains two concepts that emphasise how hacking influences public access to information and shapes patterns of information

dissemination. The third branch, Ethical Considerations, introduces two concepts that examine the tension between human rights and the pursuit of ethical technology, underscoring the need for normative evaluation of technological conduct. The final branch, Legal Framework, presents three concepts that outline the statutory and regulatory responses to hacking through information technology legislation, criminal law and cyber law. Collectively, the nine concepts reflect a structured progression from global normative concerns to societal impacts, ethical dilemmas and legal mechanisms. The deductive flow demonstrates that understanding hacking requires moving from overarching governance considerations to concrete legal responses, thereby revealing the multi-dimensional nature of regulating technological intrusion.

Research Questions

This study investigates the following five research questions:

RQ1: What are the research trends of hacking and the law according to the year of publication?

RQ2: What are the top 10 cited articles of hacking and the law?

RQ3: Which are the top 10 countries on hacking and the law based on number of publication?

RQ4: What are the popular keywords related to hacking and the law?

RQ5: What are co-authorship by countries' collaboration of hacking and the law?

METHODOLOGY

Bibliometrics entails the systematic collection, organisation and examination of bibliographic data drawn from scientific publications [14], [15], [16]. In addition to fundamental descriptive measures that identify core journals, publication trends and principal authors [17], bibliometric inquiry incorporates advanced analytical techniques such as document co-citation analysis. A rigorous literature review depends on a deliberate and iterative procedure involving the selection of appropriate keywords, structured searching and comprehensive analytical scrutiny. This process enables the construction of a coherent and exhaustive bibliography while supporting methodological reliability [18]. Guided by these considerations, the present study prioritised high-impact publications, recognising their value in elucidating the conceptual foundations and theoretical trajectories of the field. To preserve data integrity, SCOPUS was adopted as the primary data source [19], [20], [21], and only peer-reviewed journal articles were included, with books and lecture notes intentionally omitted to maintain scholarly rigour [22]. Using Elsevier's Scopus, noted for its extensive coverage, publications from 1995 to 2025 were collected for detailed analysis.

Data search strategy

The search strategy for this study was formulated through a precise and replicable approach using the Scopus advanced search function. The search string TITLE (hacking AND (law OR rule OR ruling OR polic* OR legal OR regulat* OR governance OR princip* OR convention OR ethic*)) was constructed to capture publications in which the term hacking appears explicitly in the title together with at least one term associated with legal, regulatory, governance or ethical dimensions. This syntactic structure was chosen to ensure conceptual relevance by filtering for works that directly engage with the normative or institutional aspects of hacking, rather than merely describing technical phenomena. To refine temporal relevance, the parameters PUBYEAR > 1984 AND PUBYEAR < 2026 were applied, aligning the dataset with the modern evolution of hacking discourse from the mid-1980s to the end of 2025, a period in which cyber governance frameworks became increasingly formalised. The search was further restricted to publications in the English language through LIMIT-TO (LANGUAGE , "English"), ensuring interpretability and consistency in analysis. At the initial stage, this search strategy produced 246 documents that met the automated criteria as of the access date in December 2025. The final search string is shown in **Table 1**. This corpus represented the preliminary universe of potentially relevant studies spanning four decades of scholarly engagement with the legal, regulatory and ethical dimensions of hacking.

Following this automated retrieval, a structured screening process using explicit inclusion and exclusion criteria

was undertaken in order to enhance the accuracy and conceptual coherence of the dataset as shown in **Table 2**. The inclusion criteria required that publications be written in English and fall within the defined timeline of 1985 to 2025. Items that met these conditions were retained for further examination. Conversely, the exclusion criteria removed non English items and those outside the designated temporal range. In addition to these basic filters, the screening process incorporated a qualitative assessment to ensure that each publication maintained substantive relevance to hacking within a legal, regulatory, governance or ethical context. This step was necessary because automated searches may retrieve documents whose titles contain the specified search terms but whose content diverges from the intended thematic scope. Through this detailed screening, ten documents were excluded, resulting in a final dataset of 236 papers. This refined corpus provides a more accurate reflection of the scholarly landscape on hacking-related legal and governance issues and forms a robust basis for subsequent bibliometric and thematic analyses. The reduction from 246 to 236 documents illustrates the importance of human-led screening to correct for mechanical retrieval errors and to uphold methodological rigour. The final dataset thus represents a carefully curated body of literature that is both comprehensive and conceptually aligned with the objectives of the study, enabling a deeper exploration of how hacking has been examined, regulated and theorised within academic discourse over the last four decades.

Table 1. The search string

Source	**Search string**
Scopus	TITLE (hacking AND (law OR rule OR ruling OR polic* OR legal OR regulat* OR governance OR princip* OR convention OR ethic*)) AND PUBYEAR > 1984 AND PUBYEAR < 2026 AND (LIMIT-TO (LANGUAGE , "English")) Access date: December 2025

Table 2. The selection criterion of searching

Criterion	Inclusion	Exclusion
Language	English	Non-English
Timeline	1995 – 2025	< 1995 > 2025

Data analysis

VOSviewer, developed by Nees Jan van Eck and Ludo Waltman at Leiden University in the Netherlands [23], [24], has become a widely recognised and methodologically robust software for the visualisation and analysis of scientific literature. Known for its intuitive, interactive interface, it enables researchers to construct advanced network visualisations, clustering analyses and density maps that reveal structural patterns and intellectual relationships within complex scholarly fields. Its functional range includes the mapping of co-authorship, co citation and keyword co-occurrence networks, offering extensive insight into the dynamics of academic communication. Continuous updates and methodological refinements reinforce its analytical reliability, ensuring that both emerging and experienced scholars can work effectively with large scale bibliometric datasets. With capabilities that include the computation of diverse metrics, extensive customisation of visual outputs and compatibility with major bibliometric data sources, VOSviewer has established itself as an indispensable instrument for knowledge mapping and research evaluation.

A key strength of VOSviewer lies in its capacity to convert intricate bibliometric data into accessible visual representations, enabling the identification of thematic clusters, keyword co-occurrence structures and citation linkages. Distinguished from traditional bibliometric tools, VOSviewer integrates methodological rigour with usability, thereby extending its relevance across multiple academic disciplines. Its adaptability and emphasis on

network visualisation ensure that research landscapes are depicted with precision and conceptual clarity. For this study, bibliometric datasets containing publication year, title, author, journal, citation count and keywords were extracted in PlainText format from the Scopus database covering the period from 1995 to 2025. These data were processed using VOSviewer version 1.6.20, where clustering and mapping procedures were applied to generate comprehensive knowledge maps. Methodologically, VOSviewer provides an alternative to Multidimensional Scaling by situating items in low dimensional spaces such that spatial proximity reflects degrees of relatedness [23]. Although it shares conceptual affinities with MDS [25], VOSviewer employs a more refined normalisation method based on association strength, computed as:

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

where Cij represents the observed co occurrence frequency of items i and j, and w_i and w_j denote their respective occurrence frequencies [26]. This proportional measure captures the ratio between observed and expected co occurrences under statistical independence, thereby enhancing the precision and interpretive power of bibliometric mapping and enabling deeper exploration of latent intellectual structures.

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 hacking and the law according to the year of publication?

The publication trend on "hacking and the law" between 1995 and 2025 demonstrates a gradual but fluctuating growth in scholarly attention as shown in **Figure 2**.

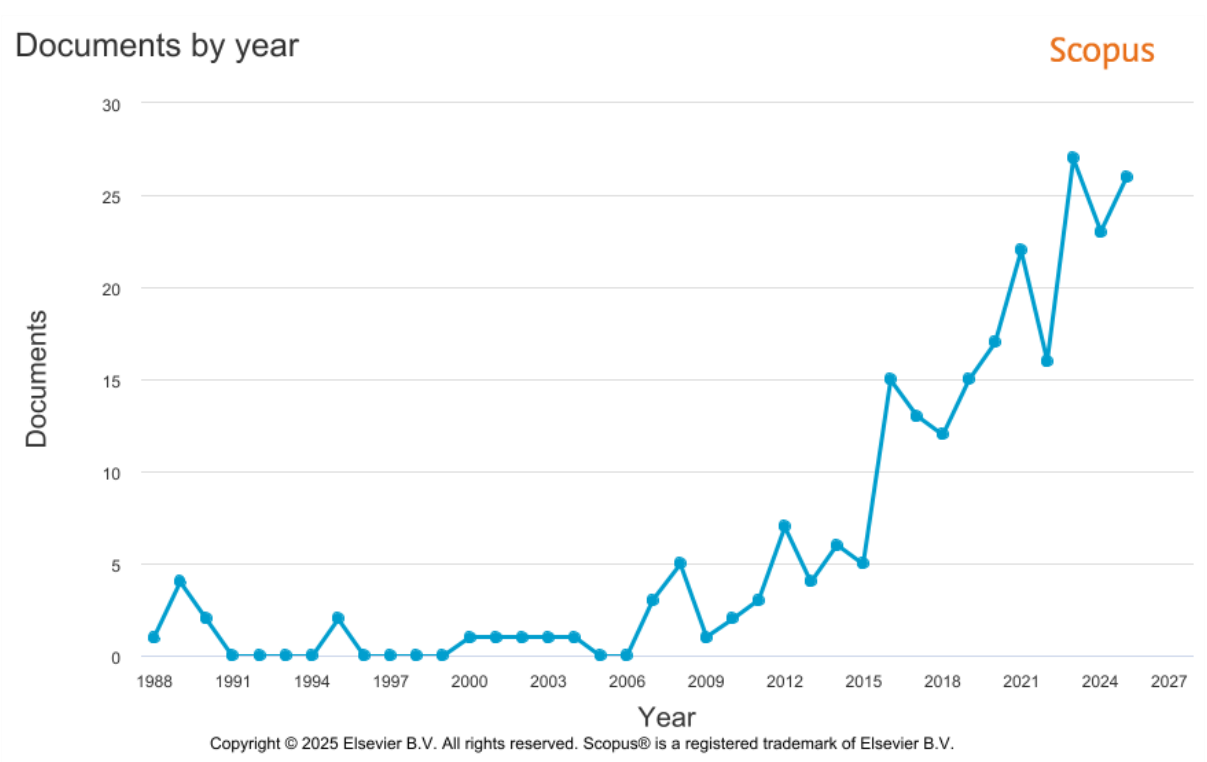

Figure 2. Publication trend by year of publication

The publication trajectory from 1995 to 2025 demonstrates a clear upward progression, with modest activity in the earlier years and pronounced expansion from the mid-2010s onwards. Between 1995 and 2010, annual outputs remained low, fluctuating between one and seven publications. This period reflects the nascent stage of legal scholarship on hacking, when cyber intrusions were still emerging phenomena and regulatory frameworks

were relatively underdeveloped. Early academic attention focused mainly on foundational definitional issues and rudimentary statutory responses, which limited the volume of specialised research. A gradual increase appears from 2011 to 2018, during which annual publications rise from three to twelve. This growth aligns with the global proliferation of digital technologies, the rise of high-profile breaches and the institutionalisation of cyber governance debates. As governments introduced dedicated cyber legislation and international bodies expanded norms on digital conduct, scholarly interest widened, contributing to a steadier flow of publications.

The steepest rise occurs from 2019 onwards, culminating in peaks of 27 publications in 2023 and 26 in 2025. This period corresponds with heightened regulatory and societal pressures shaped by several convergent developments. First, large-scale incidents such as ransomware attacks, supply chain penetrations and state-linked cyber operations increased the salience of legal analysis on hacking. Second, rapid technological advances in artificial intelligence, automation and cryptographic systems generated complex legal and ethical questions, prompting intensified academic engagement. Third, national and regional reforms, including revisions of cybercrime statutes, data protection frameworks and cross-border cooperation instruments, opened new avenues for doctrinal and policy-oriented inquiry. The slight fluctuations between 2020 and 2025 reflect variations in publication cycles rather than substantive decline. Overall, the trend indicates a maturing, increasingly interdisciplinary field shaped by evolving threats, expanding regulatory architectures and growing societal dependence on digital infrastructures.

Research Question 2: What are the top 10 cited articles of hacking and the law?

Produced below in **Table 3** is the list of top 10 cited articles on the topic of hacking and the law.

Table 3: Top 10 cited articles

Authors	**Title**	**Year**	**Source title**	**Citation count**
Coleman, G.E.	Coding freedom: The ethics and aesthetics of hacking	2012	Book	390
Lyócsa, Š.; Molnár, P.; Plíhal, T.; Siranova, M.	Impact of macroeconomic news, regulation and hacking exchange markets on the volatility of bitcoin	2020	Journal of Economic Dynamics and Control	102
Yaacoub, J.-P.A.; Noura, H.N.; Salman, O.; Chehab, A.	Ethical hacking for IoT: Security issues, challenges, solutions and recommendations	2023	Internet of Things and Cyber-Physical Systems	93
Palmer, C.C.	Ethical hacking	2001	IBM Systems Journal	54
Wang, Y.; Yang, J.	Ethical hacking and network defense: Choose your best network vulnerability scanning tool	2017	Proceedings 31st IEEE International Conference on Advanced Information Networking and Applications Workshops Waina	45
Lakshmi, C.; Thenmozhi, K.; Rayappan, J.B.B.; Amirtharajan, R.	Encryption and watermark-treated medical image against hacking disease—An	2018	Computer Methods and Programs in Biomedicine	41

	immune convention in spatial and frequency domains			
Hatfield, J.M.	Virtuous human hacking: The ethics of social engineering in penetration-testing	2019	Computers and Security	30
Sri Devi, R.S.; Kumar, M.M.	Testing for Security Weakness of Web Applications using Ethical Hacking	2020	Proceedings of the 4th International Conference on Trends in Electronics and Informatics Icoei 2020,	28
Patil, S.; Jangra, A.; Bhale, M.; Raina, A.; Kulkarni, P.	Ethical hacking: The need for cyber security	2018	IEEE International Conference on Power Control Signals and Instrumentation Engineering Icpcsi	26
Jaquet-Chiffelle, D.-O.; Loi, M.	Ethical and Unethical Hacking	2020	International Library of Ethics, Law and Technology	21

The citation pattern among the ten most cited works indicates that scholarship on hacking and the law is shaped by a combination of foundational theoretical contributions and contemporary applied studies. The Coding Freedom [27], with 390 citations, dominates the list, reflecting its status as a seminal ethnographic and philosophical analysis of hacker culture that continues to inform discussions on digital rights, autonomy and normative frameworks in computing. Its methodological depth and conceptual breadth likely explain its enduring influence. High citation counts for works such as [28] , which analyse hacking in cryptocurrency markets, demonstrate the prominence of economic and regulatory implications in contemporary debates. Similarly, [29] gain traction by addressing ethical hacking challenges in the Internet of Things, an area experiencing rapid technological expansion and heightened vulnerability. These trends suggest that works become highly cited when they either establish foundational understanding or intersect with fast-growing technological domains that create new regulatory and ethical imperatives.

The remaining papers share a focus on ethical hacking, penetration testing, cybersecurity practices and the moral evaluation of hacking-related activities. Early contributions such as [30] continue to be cited because they laid conceptual and technical groundwork that shaped subsequent professional and academic discourse. Papers addressing practical security methodologies, including [31], [32] and [33], attract attention due to their operational relevance as organisations increasingly depend on ethical hacking for defensive strategies. Studies applying ethical analysis to emerging techniques, such as [34] examination of social engineering and [35] distinction between ethical and unethical hacking, resonate within broader debates on responsible cyber conduct. The cumulative pattern demonstrates that citation impact is driven by conceptual originality, empirical relevance to evolving technological contexts and the growing interdisciplinary demand for legal, ethical and technical guidance in addressing hacking phenomena.

Research Question 3: Which are the top 10 countries on hacking and the law based on number of publication?

The following **Figure 3** reveals the top 10 countries based on number of publication in the area of hacking and the law.

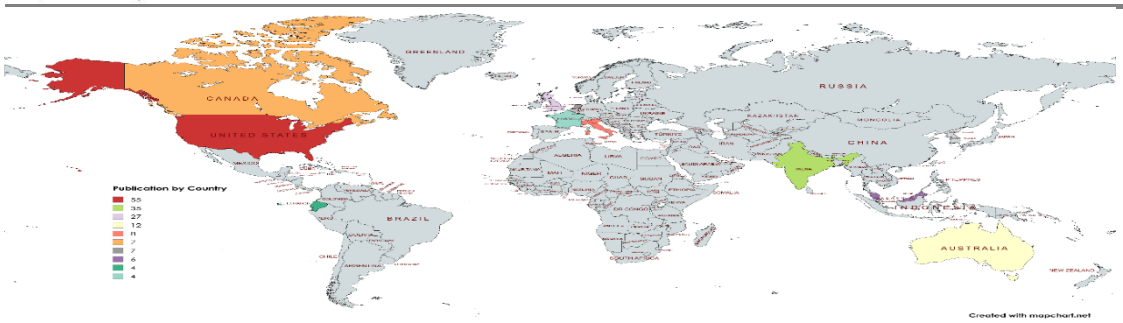

Figure 3. Top 10 countries based on number of publications

The distribution of publications across the top ten countries illustrates the global yet uneven engagement with the legal and regulatory dimensions of hacking. The United States leads with 55 publications, which is consistent with its advanced technological ecosystem, high incidence of cyber incidents and extensive academic infrastructure supporting research on cybersecurity law. India follows with 35 publications, reflecting its expanding digital economy, increasing cybersecurity challenges and strong growth in technical and legal scholarship. The United Kingdom, with 27 publications, demonstrates sustained interest driven by its mature legal system, active regulatory reforms in cyber governance and established research networks in information law. Australia's 12 publications are aligned with national policy attention to cyber threats and its investment in interdisciplinary cyber research centres. Italy, Canada and the Netherlands, with counts between seven and eight, contribute through specialised research clusters and active participation in European cyber governance initiatives, which encourage comparative and doctrinal work on digital regulation.

Malaysia's presence with six publications indicates a developing but growing scholarly engagement with hacking-related legal issues, likely influenced by national legislative reforms, increasing digitalisation and the country's participation in regional cybersecurity dialogues. Ecuador and France, each contributing four publications, illustrate distinct pathways into the discourse: Ecuador's engagement may be driven by growing cybersecurity concerns in emerging digital economies, while France's contribution aligns with its strong academic tradition in technology ethics, data governance and public regulatory law. Overall, the geographical distribution corresponds closely with levels of technological advancement, exposure to cyber risks, availability of research funding and national regulatory priorities. Countries with robust digital infrastructures and active governance reforms tend to generate more sustained academic output on hacking and the law, while emerging economies contribute selectively as digital transformation deepens and legal challenges become more pronounced.

Research Question 4: What are the popular keywords related to hacking and the law?

The following **Figure 4** highlights the main keywords used by the authors related to the study of hacking and the law.

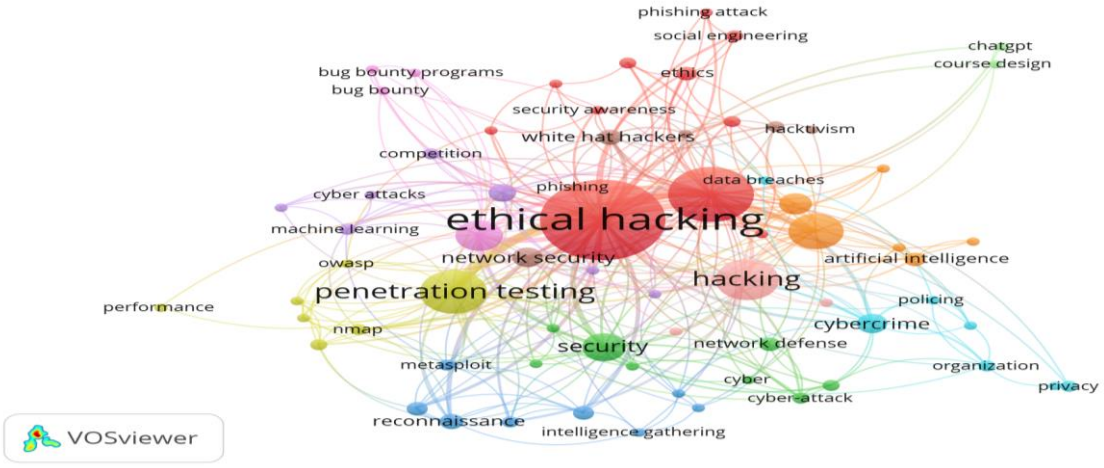

Figure 4: Network visualisation map of keywords' co-occurrence

Co-occurrence analysis of author keywords in VOSviewer identifies how frequently specific terms appear together within the same publications, thereby revealing conceptual linkages and thematic structures within a research field. By mapping these relationships, VOSviewer visualises how ideas cluster around shared intellectual concerns, allowing researchers to detect dominant themes, emerging areas, and the relational intensity between concepts. In this study, the full counting method was applied, meaning each keyword occurrence was counted equally across all documents. A minimum threshold of two occurrences was set, resulting in 70 of the original 473 keywords meeting the inclusion criteria. A minimum cluster size of five was imposed to ensure that only thematically coherent groups were retained, producing eleven clusters. This configuration enabled a balanced representation of both prominent and moderately recurring concepts, ensuring the final map reflected the structural complexity of the field without being diluted by noise from infrequently used terms.

The findings contribute to the existing body of knowledge by delineating the intellectual landscape of research on hacking and the law, highlighting both central and peripheral themes. The most prominent concepts as highlighted in **Figure 4** include ethical hacking (74), cybersecurity (39), penetration testing (26), hacking (24) and information security (19), showing that scholarship in this area is anchored in technical security practices with strong normative implications. Keywords such as vulnerabilities (15), network security (7), cybercrime (7) and white hat hackers (5) indicate sustained attention to risk identification, legal accountability and professional roles. The presence of terms linked to tools and methodologies, such as metasploit (3), kali linux (4), nmap (3) and reconnaissance (5), reflects the technical depth of the field, while emerging themes like machine learning (3), artificial intelligence (4), chatGPT (2) and data protection (2) suggest expanding intersections between law, automation, and regulatory governance. Collectively, the co-occurrence structure demonstrates a research domain that is both maturing and diversifying, where technical, legal and ethical elements converge to shape contemporary understandings of hacking and its regulatory implications.

Research Question 5: What are co-authorship by countries' collaboration of hacking and the law?

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 identifies patterns of international research cooperation by mapping how frequently authors from different countries publish together. This analytical approach visualises the structural relationships that underpin global knowledge production, revealing both strong bilateral collaborations and broader clusters of countries that tend to co publish within shared thematic or disciplinary spaces. Using the full counting method, each co-authored publication contributes equally to the link strength between countries, ensuring that all collaborative ties are represented without weighting. No minimum threshold was applied, allowing all 52 identified countries to be included in the analysis. A minimum cluster size of five was imposed to generate coherent groups of collaborating countries, resulting in six clusters. This configuration ensures that the map reflects meaningful international linkages while avoiding fragmentation caused by isolated or infrequently collaborating states.

The findings provide significant insight into the geopolitical distribution and collaborative intensity of research on hacking and the law. As shown in **Figure 5**, the United States leads in both document count (56) and citation impact (586), indicating its central role in shaping scholarly discourse, although its total link strength of 9 suggests moderate levels of international co-authorship. India (33 documents, link strength 5) and the United Kingdom (27 documents, link strength 4) demonstrate strong domestic research productivity with comparatively limited but targeted international engagement. Malaysia, despite a smaller output of six documents, shows a

relatively high link strength of 6, signalling an active pattern of cross border collaboration that enhances its visibility within the field. Countries such as France (citations 96), the Netherlands (200 citations), Canada (439 citations) and Switzerland (164 citations) contribute substantial intellectual influence despite moderate publication volumes, pointing to their involvement in high impact collaborative work. The presence of diverse countries across six clusters illustrates that research on hacking and the law is becoming increasingly internationalised, with collaborative networks supporting the diffusion of legal, technical and policy expertise. This mapping enriches the body of knowledge by demonstrating how global partnerships contribute to the development of nuanced, context sensitive understandings of cybersecurity governance and legal frameworks.

CONCLUSION

This study set out to examine three decades of scholarly work on hacking and the law, with the aim of mapping publication patterns, influential contributions, thematic developments and collaborative structures within this expanding field. Through bibliometric techniques applied to 236 Scopus-indexed documents published between 1995 and 2025, the analysis addressed key questions concerning temporal research trends, citation prominence, geographical distribution, conceptual emphases and international co-authorship networks.

The findings reveal a clear acceleration of academic interest, particularly from 2010 onwards, culminating in substantial growth between 2020 and 2025. This trend corresponds with the increasing complexity of cyber intrusions, evolving regulatory frameworks and the intensification of public policy debates. The dataset indicates that ethical hacking, cybersecurity governance, penetration testing, vulnerabilities, and information security constitute the most recurrent research themes. The most cited works substantially shaped the conceptual foundations of this domain, while country-level output demonstrates that contributions are led by technologically advanced jurisdictions, although emerging economies have begun to show expanding engagement. Co-authorship mapping further illustrates a progressively internationalised research environment, marked by multi-country collaborations that facilitate the development of shared legal and technical understandings.

The study contributes to the field by offering an empirical overview of how academic discourse on hacking and the law has evolved and diversified across time, geography and disciplinary intersections. Such insights provide a structured basis for understanding how legal scholarship responds to rapid technological change and expanding societal reliance on digital infrastructures. For practice, the patterns identified highlight areas where regulatory and professional development may be strengthened, particularly in the domains of cybersecurity governance, incident response, ethical standards and cross-border legal cooperation.

Several limitations warrant acknowledgment. The exclusive reliance on Scopus may have omitted relevant works indexed elsewhere, and the focus on English-language publications restricts representation from non-English jurisdictions. Bibliometrics also cannot fully capture the qualitative depth of legal reasoning or normative debate. Future research may expand coverage across databases, integrate qualitative content analysis and explore longitudinal shifts in doctrinal interpretations more closely. Further examination of underrepresented regions and emerging technologies would also deepen understanding of global disparities and future regulatory trajectories.

Overall, the study underscores the value of bibliometric analysis as a method for tracing the evolution of scholarship on hacking and the law, identifying dominant and emerging research pathways, and clarifying the intellectual structure of this interdisciplinary field. Such analyses remain essential for guiding future inquiry, supporting evidence-based policy discussions and strengthening conceptual coherence in an area of law that continues to develop in response to persistent technological innovation and new forms of cyber risk.

ACKNOWLEDGMENT

The authors would like to express gratitude to Universiti Utara Malaysia for the resources necessary in finalising this paper.

REFERENCES

1. M. Pisarić, "The Use of Policeware to Hack Electronic Evidence in Germany and the Netherlands," NBP. Nauk. bezbednost, Polic., vol. 28, no. 1, pp. 16–26, 2023, doi: 10.5937/nabepo28-43759.
2. P. Sommer, "Criminalising hacking tools," Digit. Investig., vol. 3, no. 2, pp. 68–72, 2006, doi: 10.1016/j.diin.2006.04.005.
3. Q.-H. Wang, R. Geng, and S. H. Kim, "Chilling Effect of the Enforcement of Computer Misuse Act: Evidence from Publicly Accessible Hack Forums," Inf. Syst. Res., vol. 35, no. 3, pp. 1195–1215, 2024, doi: 10.1287/isre.2019.0346.
4. S. Oh and K. Lee, "The need for specific penalties for hacking in criminal law," Sci. World J., vol. 2014, 2014, doi: 10.1155/2014/736738.
5. S. Hennessey, "Lawful hacking and the case for a strategic approach to going dark," in Brookings Big Ideas for America, 2017, pp. 241–250. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85037867658&partnerID=40&md5=800f2d8548cbf87c87fed35e4e84f45a
6. K. Best, "The Hacker's challenge: Active access to information, visceral democracy and discursive practice," Soc. Semiot., vol. 13, no. 3, pp. 263–282, 2003, doi: 10.1080/1035033032000167015.
7. Z. Hamin and W. R. W. Rosli, "Managing cyber stalking in electronic workplaces," Adv. Sci. Lett., vol. 23, no. 8, pp. 7895–7899, 2017, doi: 10.1166/asl.2017.9603.
8. G. Ziccardi, "The European Parliament study on hacking activities by law enforcement: A legal-informatics analysis (and legislative policy)," Arch. Penal., vol. 69, no. 2, pp. 512–537, 2017, doi: 10.12871/9788674101948.
9. G. Ziccardi, "The hacking tools in the 'Riforma Orlando': Some legal informatics reflections," Arch. Penal., vol. 2018, pp. 497–511, 2018, doi: 10.12871/978883318026725.
10. A. Ghappour, "Searching places unknown: Law enforcement jurisdiction on the dark web," Stanford Law Rev., vol. 69, no. 4, pp. 1197–1236, 2017, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85019227158&partnerID=40&md5=29fe4eee581b427e142667134dba57ec
11. S. D. Brown, "Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice," ERA Forum, vol. 20, no. 3, pp. 423–438, 2020, doi: 10.1007/s12027-019-00571-z.
12. J. Mayer, "Government hacking," Yale Law J., vol. 127, no. 3, pp. 570–662, 2018, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85042114062&partnerID=40&md5=3e99287f45827b1361b5d072585a45a8
13. A. M. Mohamad et al., "Socio-Legal Enquiry into the Motivating Factors of Cyberbullying in Malaysia," Bild Law J., vol. 7, no. 1, pp. 74–84, 2022, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85140069781&partnerID=40&md5=8109b26ab4b08ce86bab80e44abd925f
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.

21. G. P. Khiste and R. R. Paithankar, "Analysis of Bibliometric term in Scopus," Int. Res. J., vol. 01, no. 32, pp. 78–83, 2017.
22. D. Gu, T. Li, X. Wang, X. Yang, and Z. Yu, "Visualizing the intellectual structure and evolution of electronic health and telemedicine research," Int. J. Med. Inform., vol. 130, 2019, doi: 10.1016/j.ijmedinf.2019.08.007.
23. 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.
24. 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.
25. 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.
26. 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.
27. G. E. Coleman, Coding freedom: The ethics and aesthetics of hacking. London: Princeton University Press, 2012. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84870601883&partnerID=40&md5=4017a4f223690180a4fee54d0b36cb89
28. Š. Lyócsa, P. Molnár, T. Plíhal, and M. Siranova, "Impact of macroeconomic news, regulation and hacking exchange markets on the volatility of bitcoin," J. Econ. Dyn. Control, vol. 119, 2020, doi: 10.1016/j.jedc.2020.103980.
29. J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," Internet Things Cyber-Physical Syst., vol. 3, pp. 280–308, 2023, doi: 10.1016/j.iotcps.2023.04.002.
30. C. C. Palmer, "Ethical hacking," IBM Syst. J., vol. 40, no. 3, pp. 769–780, 2001, doi: 10.1147/sj.403.0769.
31. Y. Wang and J. Yang, "Ethical hacking and network defense: Choose your best network vulnerability scanning tool," in Proceedings 31st IEEE International Conference on Advanced Information Networking and Applications Workshops Waina, 2017, pp. 110–113. doi: 10.1109/WAINA.2017.39.
32. R. S. Sri Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," in IEEE International Conference on Power Control Signals and Instrumentation Engineering Icpcsi, 2020, pp. 354–361. doi: 10.1109/ICOEI48184.2020.9143018.
33. S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, "Ethical hacking: The need for cyber security," in IEEE International Conference on Power Control Signals and Instrumentation Engineering Icpcsi, 2018, pp. 1602–1606. doi: 10.1109/ICPCSI.2017.8391982.
34. J. M. Hatfield, "Virtuous human hacking: The ethics of social engineering in penetration-testing," Comput. Secur., vol. 83, pp. 354–366, 2019, doi: 10.1016/j.cose.2019.02.012.
35. D.-O. Jaquet-Chiffelle and M. Loi, "Ethical and Unethical Hacking," in International Library of Ethics, Law and Technology, vol. 21, 2020, pp. 179–204. doi: 10.1007/978-3-030-29053-5_9.