Based on Citespace — Taking WOS Data as an Example (2016-2026)

Jinghan Chen*

Hongyi Honor College, Wuhan University, Wuhan, Hubei Province, 430072, China

*2024300003166@whu.edu.cn

Abstract. As the core of the digital society governance system, Cyber Law has a profound impact on cyberspace security, digital economy regulation, and the protection of citizens' rights. Existing research often focuses on specific areas or cases, lacking a systematic overview of global research trends, knowledge structures, and cutting-edge hotspots, making it difficult to grasp the overall state of the discipline. Therefore, this study will systematically explore the global research dynamics in the field of Cyber Law from 2016 to 2026, aiming to identify core themes, analyze the evolution of hotspots, and reveal knowledge structures and development frontiers to contribute to theoretical deepening, policy optimization, and practical innovation. This study employs bibliometrics and visualization analysis, using the Web of Science Core Collection as the data source. CiteSpace 6.4 R1 is used to conduct collaborative network analysis, co-occurrence analysis, cluster analysis, and emergence detection on relevant literature, thereby objectively and quantitatively presenting the core research and evolutionary trajectory of this field. Analysis reveals that Cyber Law research between 2016 and 2026 exhibits an evolutionary pattern from topic differentiation to focus convergence. Research topics are gradually focusing on cutting-edge issues such as Digital Sovereignty, Platform Responsibility, Digital Trade, and Geopolitical Competition, reflecting a progressive logic from normative construction to institutional practice and then to conflict governance.

Keywords: Cyber Law, research hotspots and trend analysis, CiteSpace, WOS

1 Introduction

Cyber law, a comprehensive legal field that emerged alongside the development of the internet, was shaped by both academia and practice. In his 1990s book *Code*, American scholar Lawrence Lessig systematically expounded the multi-faceted governance logic of cyberspace, making a crucial contribution to laying the theoretical foundation of cyber law. With the explosive development of internet technology and the deep integration of emerging technologies such as artificial intelligence, cyberspace governance faces increasingly complex security, economic, and ethical challenges. In recent years, legislative practices such as the EU's General Data Protection Regulation (GDPR) and China's Cybersecurity Law, as well as ongoing discussions within the UN

J. Rak et al. (eds.), *Proceedings of the 2026 11th International Conference on Social Sciences and Economic Development (ICSSED 2026)*, Advances in Economics, Business and Management Research 391,
https://doi.org/10.2991/978-94-6239-701-9_97

framework regarding international rules for cyberspace, have highlighted the global strategic significance of cyber law.

In academia, different scholars have systematically discussed and analyzed Cyber Law. For example, Schmitt (2017) systematically elaborated on the rules of international law applicable to cyber warfare in his edited Tallinn Manual 2.0, defined the legal threshold of cyberattacks from the perspective of international humanitarian law, and emphasized the expansionary interpretation of the concept of "attack", laying the foundation for normative analysis framework for subsequent research [1]. Macák (2017) critically pointed out that the absence of states in cyberspace legislation has led to non-state actors dominating the formulation of norms, forming a "normative crisis", and advocated that states should regain the leading role in cyberspace governance [2]. Haataja (2022) started from the relationship between international law and the norms of responsible state behavior, revealing the legal application dilemma of norms for the protection of critical infrastructure, and pointed out the superposition effect of subjective concepts and legal uncertainty [3]. Gisel et al. (2020) based on the practice of the International Committee of the Red Cross, systematically demonstrated the inevitability of cyber warfare being bound by international humanitarian law, but acknowledged that there are still interpretation differences on emerging issues such as the protection of "civilian data" [4]. Wheatley (2023) used deductive reasoning to criticize the overexpansion of "cyber sovereignty rules" and advocated for a strict distinction between the logical boundaries of constitutive rules and regulatory rules [5]. Ohlin (2017) questioned the regulatory effectiveness of the traditional international law framework for low-intensity cyber actions based on coercion theory in response to the cyber interference incident in the 2016 US election [6].

Analysis of existing research reveals a significant fragmentation in current Cyber Law studies. First, there is severe interdisciplinary overlap, with international public law, international humanitarian law, criminal law, and domestic law norms intertwined, lacking a unified analytical paradigm. Second, the normative hierarchy is confused, with the boundaries between soft and hard law blurred, from the Tallinn Manual to the UN GGE report. Third, empirical research is scarce, with most studies remaining at the level of normative interpretation, lacking a systematic examination of judicial practice and law enforcement effectiveness. Fourth, the contradiction between technological iteration and legal lag is prominent, with emerging topics such as AI weapons and metaverse governance yet to form a stable research agenda. Against this backdrop, this study aims to systematically review international research dynamics in Cyber Law from 2016 to 2026 using bibliometrics and knowledge graph methods, accurately identifying core issues, evolutionary paths, and cutting-edge trends, thereby providing empirical evidence and directional references for strengthening the discipline's theoretical system.

2 Analysis Method and Data Sources

2.1 Research Method

This study employs a combination of quantitative and qualitative research methods to conduct a comprehensive and in-depth analysis of the hot topics and trends in Cyber Law research from both macro and micro perspectives.

Quantitative Analysis. This study utilized the scientific knowledge graph tool CiteSpace 6.4 R1 to perform bibliometric analysis and visualization of selected literature data. CiteSpace, developed by Professor Chen Chaomei, is a bibliometric software whose core function is to reveal the knowledge base, research hotspots, evolutionary paths.

Qualitative Analysis. This study also employs a case study methodology to conduct in-depth analysis of specific cyber legal events or institutional practices. This approach selects several representative or landmark international and domestic cases, analyzing their background, core controversies, applicable laws, and subsequent impacts through thorough normative and comparative research.

2.2 Data Sources and Data Collection

The data for this study comes from the internationally recognized authoritative citation database—the Web of Science (WOS) Core Collection. To ensure the relevance, representativeness, and quality of the literature data, the specific retrieval and collection process is as follows: First, search restrictions were set in the WOS database. A core concept search was conducted using the keyword "Cyber Law" to comprehensively cover literature in this field. Simultaneously, the time range was limited to January 1, 2016 to December 31, 2026, to focus on the latest research developments over the past decade. The document type was limited to "Article" and "Review" to obtain the most representative peer-reviewed research results. The database scope was limited to the "Web of Science Core Collection." Language restrictions were not initially imposed to include research in English and other major languages worldwide. After conducting the above search, relevant literature entries were initially obtained. Subsequently, all search results were screened a second time by manually reading the titles and abstracts, removing obviously irrelevant, duplicate, and non-academic entries. Ultimately, 452 valid documents matching the research topic and criteria were obtained. After screening, the complete records of all documents (including titles, authors, abstracts, keywords, and references) were exported in plain text format as the data foundation for subsequent import into CiteSpace software for knowledge graph analysis.

3 Trend Analysis of Cyber Law

This study comprehensively utilizes bibliometrics and employs CiteSpace 6.4 R1 to conduct knowledge graph visualization analysis of Cyber Law research, identifying

core authors, key node documents, and evolutionary paths, clarifying the structural characteristics of the discipline's development. The specific analysis is as follows.

3.1 Keyword Cluster Analysis of Cyber Law

According to the clustering network generated by CiteSpace, based on a dataset of 452 valid documents (time span: 2016-2026) that meet the research topic and criteria, the knowledge graph of this research field is divided into 12 main clusters. The overall structure of this clustering network exhibits significant clustering effects, with a modularity (Q) value as high as 0.845. Generally, a Q value greater than 0.3 indicates a significant network structure; the Q value of this network suggests tight internal connections within clusters, clear cluster boundaries, and a high degree of differentiation in research topics. (Fig 1)

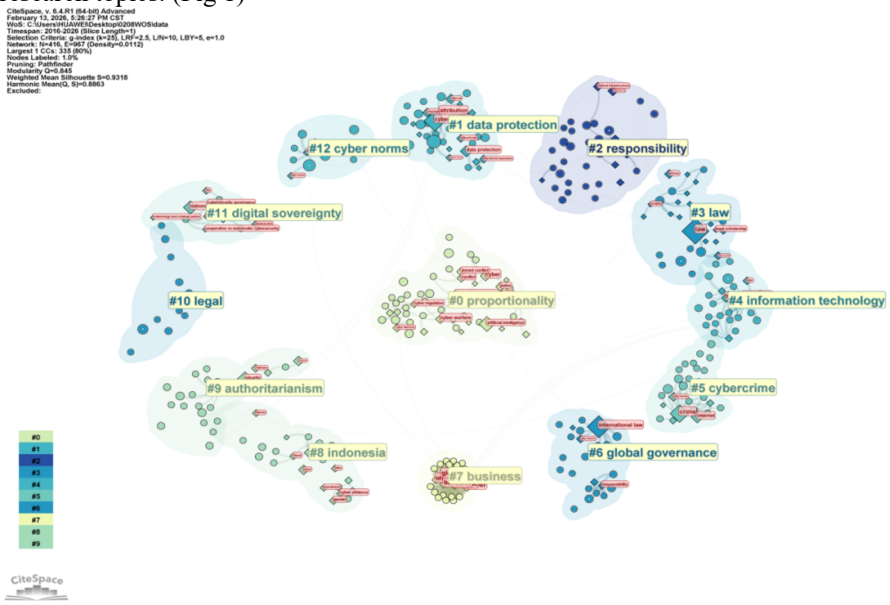

Fig. 1. Clustering (co-occurrence) analysis of Cyber Law keywords (2016-2026)

Specifically, the study selected 10 core research areas for detailed analysis. The #0 Proportionality cluster includes keywords such as Proportionality Principle, Reasonableness Review, Fundamental Rights, Intensity of Intervention, And Balancing of Interests. The above research primarily focuses on the need for a moderate and balanced proportional relationship between means and ends when public power intervenes in citizens' fundamental rights. The research typically revolves around three dimensions: appropriateness, necessity, and narrow proportionality, exploring its judicial application in specific cases. This cluster is relatively large, mainly influenced by policy orientation, the international environment, and technological development. In terms of policy, global data regulation emphasizes risk-based approaches, forcing compliance review mechanisms to re-examine the application of the proportionality

principle. Internationally, the case law system of transnational human rights conventions continuously standardizes the application of the proportionality principle. Technologically, the risks of abuse of technologies such as facial recognition and artificial intelligence algorithm decision-making have prompted academia to re-examine the boundaries between technological intervention and civil liberties.

The #1 Data Protection cluster includes Keywords Such as Data Protection, Privacy and Security, and Informed Consent. The above research primarily focuses on the legal and technological protections of personal information during collection, storage, and processing, with a core focus on users' control over their personal data and the compliance obligations of data processors. Research interest in this area continues to rise, mainly driven by policy, such as the EU GDPPR and the enactment and implementation of China's Personal Information Protection Law. Simultaneously, technological advancements have made cross-border data flows commonplace, exacerbated the risk of data breaches and led to a surge in research demand at the intersection of law and technology.

The #2 Responsibility cluster includes keywords such as legal responsibility, duty of care, joint liability, and fault determination. The above research primarily explores the civil or criminal liability that entities such as network service providers and algorithm designers should bear when tortious acts occur in the digital age. The research focuses on the evolution of attribution principles and the boundaries of liability allocation. With the development of information technology and digital intelligence technology, the definition of tortfeasors has become more difficult, challenging the traditional fault-based liability principle and sparking widespread academic discussion on the boundaries of liability.

The #3 Law cluster includes keywords such as Comparative Law, Legal Transplantation, Legal System, Jurisdiction, And Conflict of Laws. The above research is relatively macro-level, focusing on the adaptation and transformation of law as a social norm in the face of the borderless nature of the internet. The research often involves different regulatory paths for the same technological issues in different jurisdictions and their comparisons. An international perspective is the main driving factor; the global nature of data flow has led to increasingly apparent conflicts of legal jurisdiction. At the policy level, countries are attempting to vie for rule-making power through the extraterritorial application of domestic laws, making comparative law and private international law research hotspots.

The #4 cluster, Information Technology, includes keywords such as blockchain, cloud computing, the Internet of Things, encryption technology, and data security. The above research focuses on the underlying technological architecture of the information society and the legal governance issues it raises. It not only focuses on the iteration of the technology itself but also on how technological applications reshape existing legal relationships. The expansion of this field stems directly from technological development itself; the iterative updates of emerging technologies constantly impact the existing regulatory system, forcing regulators to strike a balance between encouraging innovation and preventing risks, thus spurring a large amount of research on technological neutrality and technology regulation.

The #5 Cybercrime cluster includes keywords such as Cyber Fraud, Hacking, Data Theft, Dark Web, and Digital Forensics. The above research focuses on crimes committed using computers or networks as tools or targets, covering topics such as the evolution of criminal methods, rules of electronic evidence in criminal investigations, and judicial cooperation mechanisms for transnational cybercrime. The development of modern technologies, such as AI face-swapping and deepfakes, has made cybercrime more covert and deceptive; simultaneously, the commodification of technological tools has significantly lowered the barrier to entry for crime, leading to a trend of younger and less professional perpetrators, posing new challenges to traditional criminal investigation methods and technologies.

3.2 Research Trends in Cyber Law

The timeline overview, as shown in Fig 2, illustrates the evolution of Cyber Law research (2016-2026). Specifically, research in the field of Cyber Law from 2016 to 2026 can be divided into two main phases: the early foundational exploration phase (2016-2020) and the phase of in-depth discussion and expansion (2021-2026). The following section elaborates on this in conjunction with cluster numbers and research content.

From 2016 to 2020, the main research topics were clusters #0 to #6, as detailed below. For the #0 Proportionality cluster, research evolved from the introduction of legal principles to the application of technological governance. Initially, the focus was on balancing the principle of proportionality between national security and civil liberties; later, the focus shifted to proportionality review in technological measures such as internet surveillance and data interception. This shift stemmed from the increasing concern among countries regarding the conflict between security and rights during the expansion of cyberspace, particularly the global reflection following the Snowden revelations. For the #1 Data Protection cluster, the evolution was from privacy protection to the regulation of data sovereignty and cross-border flows. Early research focused on interpreting legislative texts such as the EU GDPR; later, the focus shifted to overcoming practical bottlenecks such as data localization and cross-border law enforcement evidence collection. This shift reflects the new challenges to data governance posed by the global digital economy, as well as the differentiation and competition between European and American data governance models. For the #2 Responsibility cluster, research expanded from national responsibility to platform responsibility. Early research focused on the accountability of public entities like the state in cyberattacks, citing state responsibility clauses in international law. Later research delved into the legal responsibilities of private entities such as social media and cloud service providers in content management and algorithm accountability. This evolution reflects the diversification of cyberspace governance entities and the impact of rising private power on traditional legal frameworks. (Fig 2)

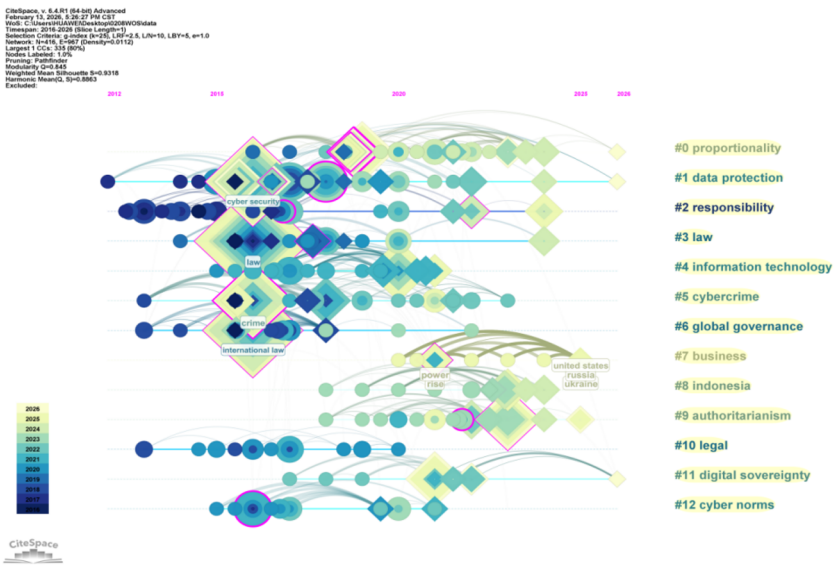

Fig. 2. Research Trend Analysis of Cyber Law Keywords

Note: Author information (box); Keyword information (circle)

For the #3 "law" cluster, the research evolved from the application of domestic law to the restructuring of the international legal system. Early research primarily explored the application of traditional legal rules in cyberspace, while later research focused on whether a completely new international convention for cyberspace was needed. This shift stemmed from the adaptive challenges posed to the existing international legal system by emerging threats such as cyber militarization and cyber espionage. For the #4 "Information Technology" cluster, research evolved from technological neutrality to legal responses to technological regulation. Early research emphasized that the law should maintain technological neutrality, while later research focused on legal issues arising from specific technologies such as artificial intelligence and blockchain, such as algorithmic discrimination and the validity of smart contracts. This shift reflects the ever-increasing demands of technological updates on legal regulatory capabilities. For the #5 "Cybercrime" cluster, the research evolved from transnational crime enforcement cooperation to the regulation of new forms of cybercrime. Early research focused on cross-border evidence collection and extradition mechanisms within the framework of the Budapest Convention, while later research shifted its focus to legal responses to emerging forms of crime such as ransomware, dark web transactions, and cryptocurrency money laundering. This evolution stems from the rapid iteration and industrialization of cybercrime technologies. Regarding the #6 global governance cluster, research has gradually shifted from a multi-stakeholder model to great power competition. Early research championed the multi-stakeholder governance model represented by ICANN, while later research focused on the differences and competition between China, the US, and Europe regarding cyber governance rules, as well as the revival of

intergovernmental negotiations within the UN framework. This shift reflects the profound impact of geopolitical factors on cyber governance mechanisms.

From 2020 to 2026, clusters #7 to #12 will be the main research topics, analyzed in detail below. For cluster #7, Business, research has evolved from corporate compliance to exploring the formulation of digital trade rules. Early research focused on the data compliance costs and privacy protection investments of multinational corporations, while later research focused on international trade law issues such as digital taxes, barriers to cross-border data flows, and tariff exemptions for electronic transmissions. This evolution reflects the deep intersection of cyber law and economic law, and the reality that digital trade has become a new frontier in great power competition. For cluster #8, Indonesia, as a representative of regional studies, research has evolved from analyzing the country's legal system to exploring South-South cooperation and critiquing digital colonialism. Early research focused on Indonesian domestic legislation such as the Personal Information Protection Act and the Electronic Transaction Act, while later research placed Indonesia and other Southeast Asian countries within the global digital geopolitical landscape, exploring their stance choices and development paths in the US-China technological competition. This shift has promoted the decentralization of global cyber law research, challenging the previously Western-dominated global governance model. For cluster #9, Authoritarianism, research has evolved from clarifying the concept of internet authoritarianism to digital authoritarianism. Early discussions primarily focused on the internet control models and theoretical implications of countries like China and Russia. Later, the focus shifted to the export and transplantation of tools such as digital surveillance technologies and social credit systems to other countries. This evolution reflects the increasing attention paid to technological progress from a political science perspective, while the competition among governance models has gradually become more theoretical. For the #10 Legal cluster, research has evolved from legislative comparison to judicial precedents and the evaluation of the effects of legal transplantation. Early research focused on textual comparisons and institutional borrowing from national internet legislation, while later research delved into the practical impact of typical judicial precedents and the localization of legal transplantation in different jurisdictions. This shift reflects an empirical turn in research paradigms. For the #11 Digital Sovereignty cluster, research has evolved from conceptual construction to institutional practice and geopolitical competition. Early research primarily explored the theoretical implications and legitimacy of digital sovereignty, while later research focused on specific institutional practices such as the EU's Gaia-X and sovereign cloud, as well as the clashes and interactions between China, the US, and the EU on the concept of digital sovereignty. This evolution marks the transition of digital sovereignty from academic discourse to policy practice. For the #12 Cyber Norms cluster, research has evolved from norm advocacy to norm implementation. In its early stages, the focus was primarily on advocating for responsible state behavior norms within frameworks such as the UN Group of Governmental Experts (UNGGE). Later, the emphasis shifted to concrete implementation pathways, compliance assessment mechanisms, and responses to violations. This shift reflects the international community's progress from rule-making to rule-implementation.

4 Case Analysis

To overcome the limitations of bibliometric analysis in revealing institutional practices and judicial logic, this study selects five significant international and Chinese cases from recent years (Table 1) and conducts in - depth analysis using normative analysis methods. The selection of cases follows three criteria: first, a high degree of relevance to the core issues of the aforementioned cluster analysis; second, demonstrating the application dilemmas of legal rules in technological scenarios; and third, a demonstrative effect of institutional innovation. Based on the above analysis, this study attempts to construct a multi-dimensional evaluation framework for norm formulation, institutional constraints, and compliance effectiveness, providing methodological support for the systematic integration and policy transformation of Cyber Law research, and promoting the paradigm shift in this field from crisis response to prevention and governance.

Table 1. Comparative Analysis of Internet Law Cases

Number	Case	Background	Methods / Technologies	Association Clustering	Innovation
1	TikTok Ireland's € 530 million fine	Chinese employees remotely accessed European user data; the DPC determined this constituted "remote access equals transmission, "and imposed a fine of € 530 million.	Transboundary Transmission Impact Assessment (TIA) and Substantial Equivalence Protection Standards	#1, #11	For the first time, temporary copies are explicitly defined as constituting data export, bringing internal operations and maintenance under regulatory scrutiny.
2	German Federal Court case concerning the data breach on a music platform (VI ZR 396/24)	User data was leaked on the dark web; the plaintiff claimed damages for emotional distress. The court ruled that "loss of control constitutes harm."	Expansive interpretation of non-material damages and presumption of causation	#0, #2	Establishing a dual harm assessment standard based on data loss of control and the fear of future misuse significantly lowers the threshold for individual claims.
3	The Ministry of Public Security of the People's Republic of China's "Cybersecurity Protection 2025 "case involving	The system attack resulted in losses of over 4 million yuan for the public, and the operator, contractor, and maintenance company were administratively punished.	Supply chain security review and compliance assessment	#2, #4	For the first time, the joint liability of multiple parties in the supply chain is clearly defined, and the failure to retain logs will be used as a separate basis for penalties.

	the Guizhou government service system.				
4	A Shanghai-based multinational company was found to have violated regulations by exporting data across borders.	User information was illegally transmitted to the overseas headquarters without passing a security assessment or obtaining separate consent.	Data security assessment, individual consent rules	#1, #7	Enforcement authorities have clarified that even visits to headquarters require exit procedures, rejecting the industry practice of granting exemptions within groups.
5	EU sanctions against "copycats "for disinformation (Doppelganger)	The EU imposes sanctions on Russia-led digital disinformation campaign for the first time targeting hybrid threats.	Hybrid threat identification and critical infrastructure protection	#6, #12	Defining information manipulation as a sanctionable malicious cyber behavior expands the scope of cyber sanctions.

The 5 typical cases mentioned above reflect three development trends in the evolution of Cyber Law. First, the trend of interconnected dissemination of responsibility among stakeholders. The "Cybersecurity 2025" case demonstrates that legal responsibility has extended from direct infringers to system builders, operators, and even overseas parent companies, making supply chain security a new focus of legal regulation [7]. Second, the trend of subjective damage assessment. The German Federal Court's VI ZR 396/24 judgment established the standard of loss of control as damage, incorporating the psychological fear of future abuse into the scope of non-material damages. The legal basis of data protection not only focuses on property logic but also on the protection of personality rights. Third, the trend of diversified regulatory methods. The EU's "imitator" sanctions case included the manipulation of false information within the scope of sanctions, marking the expansion of Cyber Law's governance tools from single legal norms to a composite system combining law with diplomacy, cybersecurity, and other areas, increasingly becoming an institutional vehicle for geopolitical competition [8]. In response to the aforementioned trends, Cyber Law research and practical application need to seek a delicate balance : technically, it should drive security capabilities inward and embed compliance requirements into the system lifecycle ; legally, it should explore tiered responsibility allocation to avoid excessive concentration of compliance burdens ; and internationally, it should resolve data sovereignty conflicts through multilateral negotiations to provide a predictable legal environment for digital trade.

5 Findings and Conclusion

This study, through keyword clustering and time trend analysis, reveals that Cyber Law research from 2016 to 2026 exhibits an evolutionary trend from topic differentiation to

focus convergence. The core research clusters cover ten major topics, including #0 Proportionality, #1 Data Protection, #2 Responsibility, and #5 Cybercrime. Research themes have expanded from early basic theoretical discussions to in-depth explorations, gradually focusing on cutting-edge issues such as Digital Sovereignty, Platform Responsibility, Digital Trade, and Geopolitical Competition, reflecting a progressive logic from normative construction to institutional practice and then to conflict governance. Furthermore, case analysis further corroborates and supplements the bibliometric findings. Five typical cases reveal a three-fold evolutionary trend in Cyber Law at the institutional practice level: a trend of interconnected dissemination of responsibility among responsible parties, a trend towards subjectivity in damage assessment, and a trend towards the diversification of regulatory means.

As artificial intelligence becomes deeply embedded in cyberspace, Cyber Law research should proactively address the following issues : At the trend development level, attention should be paid to the impact of emerging scenarios such as AI-generated content, deepfakes, and algorithmic discrimination on the existing legal framework ; after the introduction of AI, greater attention needs to be paid to the ethical aspects, exploring the balance between technological empowerment and rights protection, and preventing the distortion of tools such as digital surveillance and social credit ; at the risk avoidance level, promoting the internalization of data compliance, embedding legal requirements into the entire process of AI system design, and exploring institutional pathways for algorithm auditing, tiered liability, and cross-border regulatory cooperation. The data sources for this study are limited to the Web of Science Core Collection, spanning from 2016 to 2026. While this provides a good reflection of international academic research dynamics, it may omit non-English literature, policy reports, and cutting-edge explorations from the practical field. Furthermore, the bibliometric method focuses on the structured presentation of existing results and cannot fully capture the deep-seated connections between technological iteration and legal change. Future research can expand to multi-source data, combining policy text analysis and interview surveys to further deepen the dynamic observation of the evolution of the Cyber Law system.

References

1. Schmitt, M.N.: Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, Cambridge (2017).
2. Macák, K.: From cyber norms to cyber rules: Re-engaging states as law-makers. Leiden Journal of International Law 30(4), 877–899 (2017).
3. Haataja, S.: Cyber operations against critical infrastructure under norms of responsible state behavior and international law. International Journal of Law and Information Technology 30(4), 423–443 (2022).
4. Gisel, L., Rodenhäuser, T., Dörmann, K.: Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. International Review of the Red Cross 102(913), 287–334 (2020).
5. Wheatley, S.: Election hacking, the rule of sovereignty, and deductive reasoning in customary international law. Leiden Journal of International Law 36(3), 675–698 (2023).

6. Ohlin, J.D.: Did Russian cyber interference in the 2016 election violate international law? Texas Law Review 95(7), 1579–1598 (2017).
7. Gomathy, D.C.K., Geetha, D.V., Shyam, D.: Cyber law and cyber crime. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT 8(9), 1–5 (2024).
8. Setyoningsih, A.D.A., Farid, A.M.: Prophetic cyber law enforcement: a holistic paradigm of cyber law enforcement in Indonesia. In: Advances in Social Science, Education and Humanities Research, pp. 756–769. (2025).