Research Article

Cheng Chen* and Bin Dong

Digital forensics analysis based on cybercrime and the study of the rule of law in space governance

https://doi.org/10.1515/comp-2022-0266
received September 20, 2022; accepted January 20, 2023

Abstract: With the rapid development of social informatization, the Internet has become an important channel for global information dissemination. The wireless network space and the real space are intertwined and have a significant impact on the political, economic, and cultural aspects of international society. For example, it can effectively solve the problem of information exchange between cities, regions, and countries. Wireless network crime and wireless network space security issues involve the development of information technology in various countries and, more importantly, involve all aspects of national security. In the age of science and technology, the current situation of cybercrime can be expressed by data as follows: the online crime rate is high. According to relevant statistics, nearly 5 million Internet users are involved in various cases every year due to the use of the Internet. This article starts with the digital forensics of wireless network crime and wireless network security management systems and discusses the composition, characteristics, existing problems, and future development directions of the current wireless network security management system. By comparing the wireless network security laws of China and the United States, using the latent Dirichlet allocation (LDA)-Gibbs model and the k-means algorithm to analyze the data, this article provides guidance for future research on wireless network space governance. The combination of digital forensics analysis based on cybercrime and space governance can improve the level of public security work. At present, the world has made some progress in cyberspace, but it still faces severe challenges. In the face of new situations and new measures, it is necessary to strengthen legislation, improve relevant systems, and strengthen supervision capacity. At the same time, it is necessary to establish perfect technical means and safeguards to ensure that this goal can be achieved.

Keywords: global cultural time domain, wireless network crime, space security governance, network security, legal comparison

1 Introduction

Driven by the information technology revolution, the Internet has penetrated every aspect of real social life. While human society has benefited from the rapid progress of the Internet age, a series of potential threats in cyberspace have become increasingly apparent and are increasingly affecting the stability of the real world [1]. The digital forensics of wireless network crime and the governance of wireless network space have begun to receive attention. The international community has made a series of attempts at the governance of cyberspace [2]. The various actors in cyberspace actively participated in the innovation and established such worlds as the Information Society World Summit, Internet Governance Forum, World Telecommunication Conference, Internet Name, and Number Address [3]. The fundamental reason is that it has mastery of key Internet resources, but its close relationship with the United States has also made internet corporation for assigned names and numbers (ICANN) lack global governance. As the world's largest international organization, the United Nations has an unshirkable responsibility for the international responsibility of cyberspace governance. The developing countries are also full of expectations for the United Nations to break through the monopoly of developed countries in the field of cyberspace governance. After the US officially handed over oversight of ICANN, how the United Nations can enhance its influence in cyberspace governance is worthy of attention. This article studies the

* **Corresponding author: Cheng Chen,** Office of Research on Law and Policy, Hangzhou People's Procuratorate, Hangzhou 310000, Zhejiang, China, e-mail: cc1123172624@126.com
Bin Dong: Criminal Prosecution Department, Hangzhou People's Procuratorate, Hangzhou 310000, Zhejiang, China, e-mail: 1123172624@qq.com

effectiveness of the United Nations cyberspace governance mechanism. The mechanism complexity theory is used to analyze the current difficulties and reasons for the United Nations network governance mechanism, trying to provide theoretical reference for promoting the effectiveness of the United Nations network governance mechanism.

Research on cyberspace governance is an emerging research area [4]. Affected by the differences in the informatization process, the research on cyberspace governance in developed countries in Europe and America started earlier and was deeper. For the study of the United Nations cyberspace governance mechanism, scholars from other countries focus on the construction of the principles and norms of the mechanism itself. In contrast, Chinese scholars have more regard for the construction of the United Nations cyberspace governance mechanism as a way for developing countries, including China, to gain access to global cyberspace governance. Among them, the digital forensics of wireless network crimes in the global cultural time domain and wireless network space security issues are important breakthroughs, most of which are Chinese.

Yang pointed out that cyber weapons are malicious software entities deployed to cause damage to adversary's computer networks and systems. It threatens the integrity and functionality of the digital systems that support global communication and exchange, and has significant potential impact on social, economic and political order [5]. Drawing on the classic concept of security dilemma, the paper also advocated distinguishing between national cybersecurity and social cybersecurity. The main structural features of governance issues in cybersecurity and Internet governance were similar. The joint production of Internet services and cybersecurity made them heavily interdependent. This means that cybersecurity governance and Internet governance models need to be compatible, and the approach they adopt affects how they approach the other side. The financial services industry has been the victim of complex cyberattacks that exploit vulnerabilities caused by employee misconduct. Terlizzi et al. by analyzing bank reports and their policies [6] determined the following five main control and governance mechanisms that FSI implements to protect data: (a) National standards and technologies have studied the framework in combination with its network security governance model. (b) The policies for managing the use of information assets have been formulated. (c) The code of conduct for employees has been formulated. (d) The enterprise security culture has been developed. (e) The enterprise security has been maintained. Stadnik explored two mainstream debates about the possibility of establishing an international cybersecurity regime [7]. On the one hand, he developed the idea of different governance models based on sovereignty and, on the other hand, developed multi-stakeholderism. In addition, he also pointed out the applicability of the constructivist framework in understanding the security threats of wireless cybercrime under wireless networks and formulating international norms applicable to wireless cyberspace. The article concluded that the multi-stakeholder method of formulating norms may be a feasible way to solve the problem of establishing an international wireless network security system and analyzing how to digital forensics of wireless network crimes.

As more criminal investigations involve an increasing number and complexity of digital traces, the quality of digital forensics results is declining, as is the understanding of cybercrime [8]. The challenges of cybercrime investigation and digital forensics involve the transformation of crime pattern, the Internet of Things, and the significant complexity of the investigation. After moving toward the era of the Internet of Everything, there are a variety of forensics means based on the Internet of Things, including multi-party forensics, such as sensor equipment, communication equipment, refrigerators, cars, and drones, and the relationship between intelligent clusters and intelligent buildings [9]. Standard operating procedures are necessary for computer forensics to obtain digital evidence so that the data are not contaminated or modified during the analysis. The application of digital forensics is conducive to the normal progress of legal procedures [10]. The Internet and computer systems are often plagued by cybercrime. In this context, it is of the utmost importance to have educated and trained personnel carry out comprehensive and objective investigations into cybercrime. Education and training in digital forensic investigations and cybercrime prosecutions are therefore proposed [11]. Today's massive data, heterogeneous information and communication technologies, and borderless cyber infrastructure have created new challenges for security experts and law enforcement agencies investigating cybercrimes, and the digital forensics of the future can effectively protect modern society and hunt down cybercriminals [12].

This article started with the governance mechanism of wireless cyberspace and analyzed the governance problems faced by wireless cyberspace and how to conduct digital forensics for wireless cybercrime. The existing governance mechanisms in this field have been sorted out, and the role and existing problems of these governance mechanisms have been analyzed. A method for managing wireless network space security can be found through sorting, research, and analysis. This article compared the US's wireless network security governance philosophy with China's governance philosophy in developing

countries and analyzed the background and reasons, the differences in specific concepts, and the impact on the governance process in order to better reflect Europe and the United States as a supranational behavior specialty. The concept of governance has the uniqueness of the subject. The latent Dirichlet allocation (LDA)-Gibbs model and *k*-means algorithm were used to process and analyze the data.

2 Comparison of basic theories of wireless network security legislation

2.1 Different concepts of wireless networks

To study network security legislation, the concept of cyberspace must be understood. In order to clarify the concept of cyberspace, the connotation and extension of the network must be defined first. In fact, when the United States defines cyber, rather than cyberspace, it is sometimes simply defined as a wireless network facility itself, that is, only its technical system part, with the aim of focusing on infrastructure. Over time, the definition of networks and cyberspace is constantly changing. As a new type of criminal activity, cybercrime has attracted people's attention gradually [13]. The characteristics of a wireless network are a supplement and specific explanation of the definition of the wireless network. The research can be better only by clarifying the basic concepts of a wireless network.

2.1.1 Definition of a wireless network

At present, there is no uniform legal requirement for the definition of a wireless network. Many scholars have discussed this. For example, a wireless network is "an area that uses electronic and electromagnetic waves to store, modify, and exchange information through network systems and physical infrastructure." However, these definitions of wireless networks are more emphasized. However, from the general definition of a wireless network, a wireless network is composed of nodes and connected edges and is used to represent multiple objects and their interconnected systems. The use of wireless networks is becoming increasingly common, mainly in some large enterprises and institutions, which has become the mainstream way of network construction. Wireless networks are widely used to solve optimization problems in the fields of engineering technology and scientific production management. The international component for unicode defines a network as a physical or non-physical domain created or formed by all or part of an element. The elements mainly refer to the system of the computer and the computer itself, the data content of the computer, and the running user. However, to be clear, this network refers to the information network, which differs from the Internet of Things in the general sense or the social network based on interpersonal communication. In fact, in simple terms, a wireless network has four elements: a subject, an object, a platform, and an activity. Wireless LAN operates mainly through radio waves to achieve communication, its types include Wi-Fi, Bluetooth, Zig Bee, etc.

2.1.2 Characteristics of a wireless network

Reality is the most important feature of the Internet. After recognizing this feature, the difference between reality and virtual reality must be clarified first. Reality refers to the real existence of things and emphasizes the objective existence of things. Virtuality is something that does not necessarily conform to the characteristics of things. It is imagined by people. However, the wireless network in the global cultural time domain is obviously physical, but it is invisible but realistic. However, a wireless network is obviously physical, but it is invisible but realistic. However, in many books on Internet research, the discussion of virtuality is often regarded as a key feature of the Internet. However, if a wireless network can be legally protected and regulated, the wireless network cannot be virtual. It is not appropriate to infer that information is dematerialized and that the wireless network is virtual. First, electronic information on the wireless network exists objectively. A wireless network can be used as a carrier to present electronic information, without completely relying on the imaginary virtual existence. Second, this definition does not distinguish between the two concepts of virtual and intangible. The absence of an entity does not mean that it is virtual or that the activity itself does not conform to the facts or does not exist. Virtuality refers to something that does not exist. It is a fantasy or just a model that does not exist in reality. What does not exist, whether physically or legally, is unlikely to have any legal consequences, and it is even less likely to be included in the scope of legal adjustment. On the other hand, today's networks have become an increasingly important vehicle for human activities and have a daily impact on the world outside the wireless network. Therefore, virtualization cannot be considered a feature of a wireless network.

2.2 Different standards for network security definition

A state that is not threatened, harmed, lost, or dangerous can be called security. Harmony between man and nature is a kind of security. The state of operation of the system is controllable and does not cause damage to the surrounding environment, human life, and property. This can also be called security. A detailed explanation of network security is shown in Figure 1.

Network security is an important issue in network and network space exploration, and it must be clearly defined in network security legislation. However, the main core of cyberspace security is to ensure security, confidentiality, integrity, availability, etc., in the operation of a wireless network. Therefore, it can be understood that network security refers to the data content involved in a wireless network and the security of the computer system itself during network operation. In this process, the wireless network may be prone to virus invasion, network failure, hacker attack, information disclosure, system vulnerability, and malicious damage risk. In view of the above-mentioned possible risks, it is necessary to adopt comprehensive methods such as law, management, technology, and self-discipline to deal with, to ensure the confidentiality, integrity, and controllability of the information and communication technology system and its data [14].

2.3 Different positions of network sovereignty and security

Cyber sovereignty has received much attention, and there are many explanations for network and cyberspace sovereignty. The future research direction of cybercrime has gradually shifted from "technology" to the exploration of the real world [15,16]. However, basically, it is all about judging the ownership of wireless networks. People have many disputes about "network sovereignty" and "cyberspace sovereignty." It has also been suggested that cyber sovereignty is actually aimed at Internet sovereignty. However, the general view is that "network sovereignty" actually refers to "cyberspace sovereignty" rather than simple Internet sovereignty. In the practice of international legislation, the existence of cyber sovereignty is controversial, and many countries in Europe and the United States do not recognize the existence of cyber sovereignty. However, China clearly recognizes the existence of cyber sovereignty

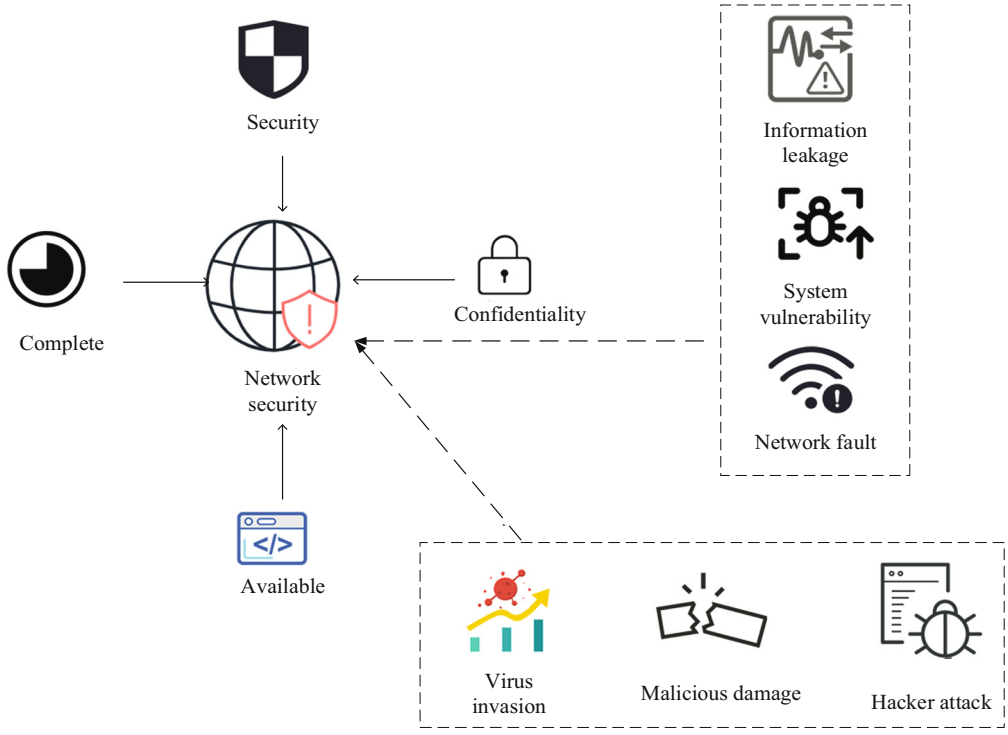

Figure 1: Network security definition standards.

and is reflected in national legislation. For example, Article 72 of the Constitution stipulates that "citizens of the People's Republic of China enjoy the right to communicate the Internet and related information and data"; Article 75 stipulates, "Information networks and their application systems are managed according to law to protect their security and legitimate rights and interests."

2.3.1 The source of the rule of law of network sovereignty

Before the founding of the United Nations in 1945, the doctrine of sovereignty came mainly from Europe. Before the arrival of the wave of independence in the modern nation-state, the early theory of sovereignty focused on the concept of national sovereignty, that is, the state's internal management and control. After that, the concept of sovereignty continued to evolve. The main characteristics of sovereignty are as follows: one is indivisibility, and the other is the highest rule within. Later, with the nation-state independence, the theory of state sovereignty continued to develop, and it was also the independence of the outside world. From the development of the sovereignty of the above countries, it can be known that with the development of navigation technology after the seventeenth century, the maritime countries continued to be strong, and the control of the ocean began to control the national sovereignty to the jurisdiction of the ocean. The development of aviation technology in the early twentieth century, for the continuous exploration of the space field, has extended national sovereignty to space. At the end of the twentieth century, the development of science and technology brought about the development of wireless networks. Information dissemination and exchange rely on Internet technology to become a reality. Human activities are closely linked to the Internet, and the extension of national sovereignty to cyberspace has become an inevitable trend. Throughout the continuous development of the scope and connotation of national sovereignty, it can be seen that the existence of new things cannot be denied. There is a space for human activities to exist, and there must be national control. On this basis, cyber sovereignty is also logical.

2.3.2 Against the existence of cyber sovereignty

Cyber sovereignty has not been widely recognized in countries worldwide, and both supporters and opponents have taken a certain weight. Most scholars who have a negative attitude toward sovereignty theory are basically Western scholars. They mainly start from regional or local cases, and the concept of sovereignty is said to be dying through imputation or comparison, because some areas cannot be solved by sovereignty. In some traditional areas of sovereignty, sovereignty is currently available. The space is not big. Some scholars believe that extending internal attributes to external attributes is the beginning of the death of sovereign theory. There is a constant debate about wireless networks and their impact on sovereignty. The main content of this debate is that one party believes that network development undermines national sovereignty, and the other believes that cyber sovereignty strengthens the management of the state's people against freedom and democracy, which strengthens national sovereignty. The particularity of cyberspace determines that it can have autonomy itself; that is, it can create its legal institutions and legal systems and manage itself autonomously, with a set of logic systems that run and exist on its own. At the national legislative and policy level, the United States represents the developed countries in Europe and the United States and strongly opposes cyber sovereignty. The more important norm of US space governance is the international cyberspace strategy, which states how commercial transactions are conducted, how governments operate, and the changes in defense spending. These activities now rely on the Internet of information technology infrastructure networks, namely cyberspace. The Safe Cyberspace Strategy provides a framework for protecting this infrastructure that is critical to our economy, security, and lifestyle. In general, the private sector is the most capable structure to respond to changing cyber threats. The government assists and responds at the appropriate time. It can be seen that in the face of problems arising from cyberspace, the US government advocates that the private sector is the main body of solution and management, reducing government intervention, and advocating the principle of cyber freedom.

2.3.3 Support the existence of cyber sovereignty

Facts have proved that if there is no national sovereign access to cyberspace, then the use of the Internet for personal crimes, group crimes, terrorist organizations, and "hackers" continues to breed. Cyber warfare is on the verge of exploding. Without the intervention of national sovereignty, once this cyber war is opened, the blow to humanity is also devastating. Finally, from the current

status of network development, countries are highly dependent on wireless networks, and the basic information infrastructure of various countries is constantly being built. Countries have strong supervision and protection claims for their network information infrastructure. It is impossible to regard cyberspace as a no. A wireless network has now become a key infrastructure for China's economic development and people's dependence on life. Wireless network also has borders. Wireless networks within China should be subject to the sovereignty of China. According to the principle of international exchanges between countries, it should be given to China. Network sovereignty is respected and maintained.

2.4 Measurement of the legal value of network security governance

Cybersecurity legislation has a game of "power and rights." The maintenance of wireless network order inevitably strengthens the supervision of public power. However, in the process of supervision, it is bound to limit the private rights of citizens. In order to balance the relationship between the interests of citizens and the interests of the state, the privacy in the network environment must be protected by law. The cyber security legislation should embody two values: the maintenance of wireless network order and the protection of civil rights. These two are a non-zero-sum game. The balance of the relationship between the two can achieve win–win cooperation so that it can be considered as one. These two values in cybersecurity legislation are both opposite and combined. On the one hand, from the perspective of safeguarding national security, social stability and the personal rights of citizens, the online world should be "legitimate." On the other hand, from the perspective of protecting the constitutional rights of citizens, boundaries should be delineated. The government manages the "boundary" of wireless networks and conducts digital evidence collection of wireless network crimes, preventing the abuse of public power and avoiding excessive restrictions on citizens' freedom of speech. At the same time, the important principles in the process of wireless network security legislation are the principle of balance of interests and the principle of simultaneous recommendation. In this context, blockchain-based Internet of Things digital forensics can effectively solve the legal problems faced by traditional evidence and has a wide and far-reaching application prospect in judicial practice [17].

3 Definition of global governance and related concepts in cyberspace

3.1 Network space definition and attributes

Cyberspace is also known by scholars as information technology space or information space. The concept of cyberspace is based on the social and international political significance of cyberspace. It is also believed that cyberspace is a space built by technological facilities that can provide social activities for human beings. However, there are also limitations in cyberspace, which can only be communicated and disseminated through the Internet. At the same time, it is also affected by cybercrimes, hackers, and other factors. When cyberspace is created, it begins to partially incorporate and recombine the space that human beings have opened up, and to carry out international power. If there is no state sovereignty to enter cyberspace, the whole cyberspace becomes unstable and uncontrollable and even ceases to function, becoming an isolated and closed entity. Structural reorganization, the boundaries of the original resources, and international power are redefined in the digital space. This extends the technical level of network technology research to the social level and analyzes cyberspace resources and power from the perspective of international political economy. Some scholars have combed and analyzed the definition of cyberspace from the perspective of cyber warfare and network surveillance. They believe that cyberspace has no boundaries but sovereignty. Although it is a virtual space, the connection with reality cannot be ignored. There is no absolute freedom in cyberspace, and regulation is indispensable. From a technical perspective, cyberspace is defined as a global domain in the information environment. Its uniqueness lies in using electronics and electronic spectra, through interdependent and interconnected networks. Information technology is the support to generate, store, correct, exchange, and benefit information. Attributes refer to the unique attributes of cyberspace, the difference between a wireless network and real society. The meaning is the subversion of the way of thinking, organization, and production of human society after the interaction between cyberspace and real space.

3.2 Global governance theory and cyberspace global governance

The theoretical system of global governance has had a tremendous impact on the theoretical construction and

development of global governance of cyberspace. Its practice and mechanism construction also enrich and improve the connotation of global governance theory. The development of global governance theory is accompanied by a shift from a state-centered system to a multi-dimensional, multi-level system. In this process, it is necessary to build and improve the corresponding security protection system, upgrade the existing system, and establish a new network security platform based on the combination of firewall, intrusion detection and defense, vulnerability scanning, and other technologies [18,19]. The main topics of international relations are not only concentrated in traditional areas such as security, economy, and politics but also include broader and deeper issues such as the environment. Issues such as outer space, infectious diseases, polar regions, oceans, and networks have begun to enter the core areas of international relations. The theory of global governance has a broad connotation and extension. At some point, it is more appropriate to be called a trend of thought and philosophy. In the theory of global governance, various types of international institutions have evolved into a core component that underpins global governance theory and practice. The concept and theory of global governance provide an important theoretical basis and source for the construction of cyberspace global governance theory. At the same time, the controversy over the concept of global governance and the theory itself continues into the theory and practice of global governance of cyberspace. This may also be seen as a factor in the global governance of cyberspace. However, the theoretical connotation and framework of global governance theory and governance system provide a very useful analytical perspective for explaining the global governance of cyberspace.

3.3 Comparing Internet governance and cyberspace global governance

Internet governance and cyberspace global governance are two related governance issues that are indeed two different areas of governance. In the initial creation and final development of the Internet, non-governmental actors played an important role. The pioneers who designed the Internet transformed the theory of governance into multiple hierarchical governance rules that constitute the Internet's architecture, network protocols, code, and operational rules. This way, the Internet's openness, interconnectivity, transparency, and operability were established. As the Internet technology continues to break through and the application deepens, a network space for establishing virtual reality begins to appear, and governance has accordingly entered the global governance stage of cyberspace. Global governance of cyberspace is built on a broader, far-reaching, and more complex governance system and is a period of a complex interaction between the government and the Internet community. The multi-stakeholder governance model has gradually become the consensus in the global governance of cyberspace, and its connotation has also evolved into the governance of cyberspace by governments, enterprises, and civil society.

3.4 The process of cyberspace global governance

The complexity, dynamics, and development of cyberspace have increased the difficulty of international social governance, and cybercrime has become an important factor affecting network security and stable development [20]. The participants in cyberspace global governance lack a unified and clear understanding of the dual game of cyberspace and complexity, which once caused the governance process to be in trouble. This article believes that it is necessary to first understand the complex global cyberspace governance situation under the dual-layer game from the aspects of Internet governance and cyberspace global governance and analyze the positions and relationships in the composite double-layer game. With the advancement of the global governance of cyberspace, all parties have gradually reached a consensus on the attributes of cyberspace, thereby narrowing the differences in governance ethods and paths. Especially at the cognitive level, countries' views on cyberspace are based on different political, economic, and cultural backgrounds, emphasizing their uniqueness and shifting to objective attributes and laws based on cyberspace and emphasizing the integration of different perspectives. The mutual joint sharing attribute of cyberspace determines that the zero-sum game does not apply to cyberspace. The security, development, and freedom of cyberspace are the common goals pursued by the government, the private sector, and civil society. At the same time, the mutual constraints of the three issues of security, development, and freedom make it impossible for either party to ignore the interests of other actors and pursue their absolute interests.

4 Results and discussion

4.1 LDA-Gibbs model

4.1.1 Text acquisition and preprocessing

This article took the relevant laws of China and the United States as the research object and discussed the theme of the national-level cybersecurity legislative text. The Chinese cyber security legislative text data were obtained from the central judicial interpretation library and local regulations and regulations. After screening and removing the invalid records, 138 records were obtained, and the Chinese text was processed by natural language processing & information retrieval for word segmentation. After deduplication and screening, 2,695 attributes were obtained. Finally, this article used the information gain method to extract features and selected 159 attributes from 2,695 attributes for Chinese text representation. The text of the US cybersecurity legislation text included 231 articles related to information security from the US federal and state networks. Natural language toolkit was used to split words and stems and delete stop words. A total of 4,269 attributes were selected by filtering, and information gain was used to select features. Finally, 465 attributes were selected for the English text representation.

4.1.2 LDA-Gibbs theme model

After the text processing, a text-feature vocabulary was obtained. Using the LDA-Gibbs model, a priori parameters α and β in the model were selected as k/1,000 and 0.01, respectively, and k represents the number of topics. According to the manual classification results, after many tests, the number of domestic data topics was set to 6, and the number of American data subjects was set to 8. After 10,000 iterations, the topic of the Chinese network information security legislative text terms and the contribution of each term to the corresponding topic are shown in Table 1. The relevant US topic-word distribution is shown in Table 2.

As shown in Table 1, Topic 1 focuses on user data privacy protection and risk control for each information service platform. Topic 2 is about information system security, and Topic 3 is about financial data security. Topic 4 is about the confidentiality of technical information documents and the provisions of confidential equipment. Topic 5 is about the confidentiality of national unified examinations or government work. As shown in

Table 1: Theme of LDA-Gibbs model based on Chinese legislative text – word distribution and word contribution

Topic 1		Topic 2		Topic 3	
Network	0.2895	Information	0.2689	Virus	0.1235
Information	0.2314	Website	0.1562	Bank	0.1169
Service	0.1123	Protection	0.1269	Project	0.0989
User	0.0512	Public security	0.0895	Detection	0.0895
Platform	0.0312	Country	0.0785	Financial	0.0795
Data	0.0289	Domain	0.0374	Information	0.0706
Protection	0.0265	Blow	0.0312	Features	0.0615
Mode	0.0212	Network	0.0283	Sales	0.0526
run	0.0198	Ministry of Public Security	0.0455	Dedicated	0.0485
risk	0.0192	Personnel	0.0215	Public security	0.0399
Topic 4		**Topic 5**		**Topic 6**	
Technology	0.2155	Country	0.2874	Country	0.2165
Science and Technology	0.2019	Personnel	0.0989	Data	0.1206
Project	0.1228	Review	0.0765	Secret level	0.0769
Result	0.0698	Information	0.0698	Matter	0.0732
Exchange	0.0349	Examination	0.0605	Personnel	0.0524
Review	0.0315	Matter	0.0546	Approve	0.0398
National Science and Technology Commission	0.0256	Involved	0.0425	Foreign	0.0258
Data	0.0226	Secret level	0.0362	Involved	0.0214
Protocol	0.0196	Approve	0.0258	Conservative	0.0936
Foreign	0.0169	Leak	0.0198	Deadline	0.0125

Table 2: LDA-Gibbs model theme based on US legislative text – word distribution and word contribution

Topic 1		Topic 2		Topic 3		Topic 4	
Trademark	0.2435	Federal	0.1859	Service	0.18690.	Administrate	0.1536
Mark	0.1695	Office	0.1425	E-commerce	0.1032	Secretary	0.1433
Service	0.0698	Public	0.1003	Telecommunicate	0.0875	Assist	0.1029
Confusion	0.0512	Service	0.0897	User	0.0664	Develop	0.0813
Domain	0.0456	Administrate	0.0513	Network	0.0524	Serve	0.712
Infringe	0.0312	Defendant	0.0339	Store	0.0428	Federal	0.0389
Advertise	0.0296	Deny	0.0298	Advertise	0.0368	Office	0.0324
Commerce	0.0238	Personnel	0.0221	Technic	0.0285	Plan	0.0305
Public	0.0186	Rights	0.0121	Commerce	0.0225	Public	0.0291
E-commerce	0.0125	Substantial	0.0189	Intercept	0.0185	Technic	0.0257
Topic 5		**Topic 6**		**Topic 7**		**Topic 8**	
Patent	0.3657	Copyright	0.2009	Compete	0.1887	Infringe	0.5883
Art	0.1024	Service	0.0689	Software	0.0668	Own	0.0577
Technique	0.0815	Distribute	0.0664	Corp	0.0516	Hold	0.0490
Corp	0.0412	Public	0.0641	Federal	0.0511	Defendant	0.0564
Deny	0.0344	Phone-record	0.0631	Own	0.0477	Serve	0.0491
Network	0.0302	Rights	0.0627	Defendant	0.0439	User	0.0334
Invalid	0.0235	Royalty	0.0548	Plaintiff	0.0412	Manufacture	0.0309
Affirmed	0.0215	Exclusive	0.0454	Manufacture	0.0385	Profit	0.0291
Software	0.0198	Preempted	0.0301	Deny	0.0305	Sell	0.0211
Accused	0.0169	Re-transmit	0.0251	Advertise	0.0259	Distribute	0.0186

Table 2, it can be seen that Topic 1 is mainly about consumer personal data protection, Topic 2 is about patent data protection, including design requirements for patent applications. Topic 3 is about information security of commercial websites, and Topic 4 is about public health data protection. Topic 5 is about information security in network authentication and authentication, and Topic 6 is about protecting user communication data. Topic 7 is about copyright and copyright issues of web content, and Topic 8 is about government organizations' supervision of public personal information processing.

4.2 Analysis of results

(1) According to the document-topic distribution, texts can be clustered, and text clustering involves text similarity problems. In the topic model, the similarity between texts can be measured by calculating the subject probability distribution. The *k*-means algorithm is fast, simple, and suitable for processing large-scale data sets. The distance measurement method has an important influence on the quality of *k*-means clustering results. Based on the distribution of subject topics, this article used the Euclidean distance to measure text similarity and used the *k*-means method for clustering. Comparing the clustering result with the manual classification result, the clustering accuracy rate P and the recall rate R can be calculated. Figure 2 shows the P and R values of the clustering results of domestic network information security legislation texts. Figure 3 shows the P and L values of the clustering results of the legal text of the US network information security.

As shown in Figure 3, clustering results based on the LDA-Gibbs model are generally satisfactory. In the Chinese text, the accuracy and recall rate of Topic 1, Topic 3, Topic 5, and Topic 6 were both above 70%. The average accuracy and average recall rate were 80.68 and 81.99%, respectively. As shown in Figure 3, there were five topics in the English text with an accuracy rate of above 80% and a recall rate of more than 70% for all topics. Analysis of clustering results found that domestic legislation on network information security was more about defining the security of hardware and important documents. The United States is more concerned about the information generated by the public in production activities and the protection of inherent personal information.

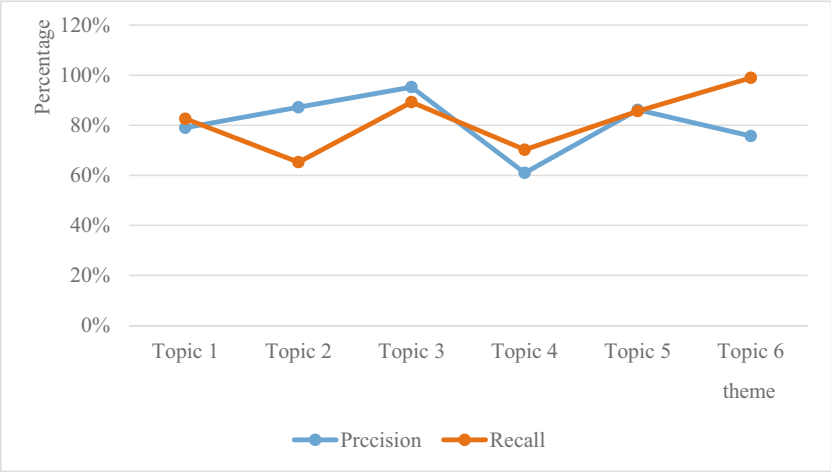

Figure 2: LDA-Gibbs model based on Chinese legislative text clustering accuracy and recall rate.

In the relevant domestic legislative texts, Topic 1 is the only topic related to public data privacy. Compared with the US network information security legislation theme, it can be seen that the United States pays more attention to public privacy protection in terms of network information security, among which Topic 1 deals with consumer data protection. Topic 3's information security issues on commercial websites include not only the website security of the commercial website itself, but also the definition of illegal and criminal behavior caused by user information. Topic 4 is about protecting public health data. Topic 5 is information security issues in network authentication. Topic 6 is information security about user communications. Topic 7 mainly deals with copyright and copyright issues for online content. Topic 8 is concerned with government organizations' oversight of public information and private information processing.

4.3 Analysis of the status quo of the construction of laws and regulations related to network information security in China

From the "Internet +" concept first proposed in November 2012, and then to the first "Internet +" action plan that appeared in the March 2015 government work report, in July 2015, the State Council issued guidance on Advancing the "Internet +" action; the concept of "Internet +" is gradually

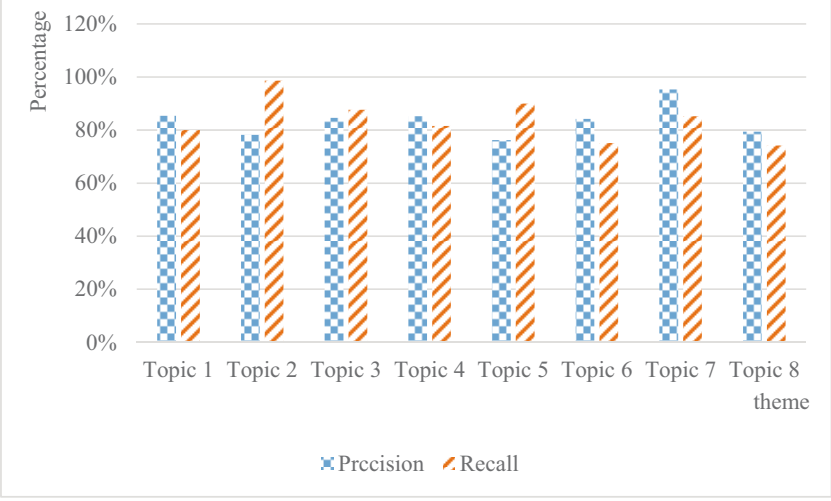

Figure 3: LDA-Gibbs model text clustering accuracy and recall rate based on US legislative texts.

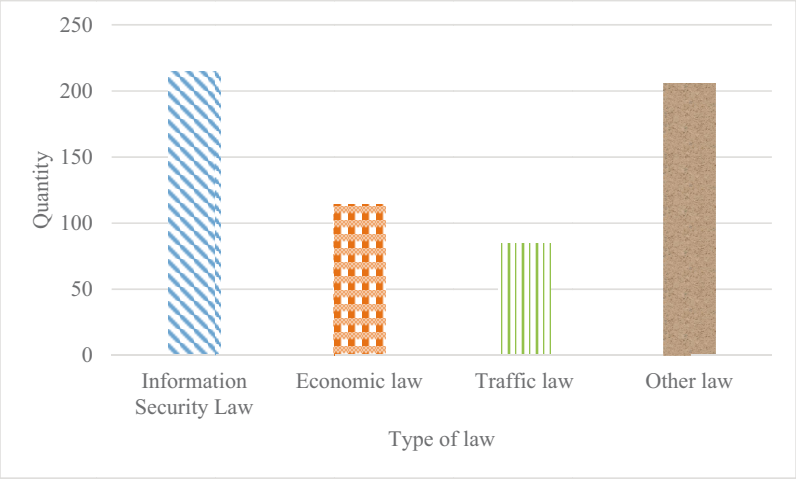

Figure 4: The number of various domestic legislation after the concept of "Internet +" is proposed.

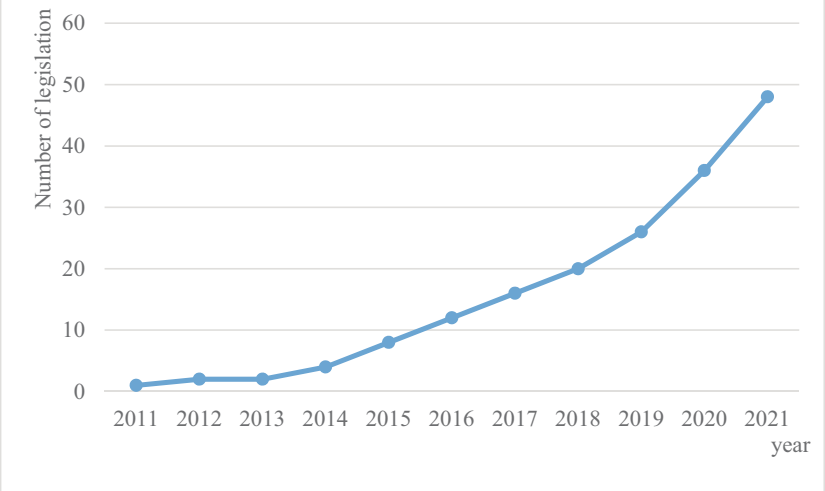

Figure 5: The development of various domestic network information security laws and regulations after the concept of "Internet +" is proposed.

accepted by various fields. At the same time, it also rose to the national strategic level. Figure 4 shows the number of domestic legislation after the concept of "Internet +." Figure 5 presents the growth of various laws and regulations related to network information security in China after the concept of "Internet +."

From the perspective of local laws and regulations, many provincial administrative regions have formulated relevant network information security laws and regulations. The scope covers third-party platforms for online ordering, electronic information platforms issued by customs, non-operating Internet access service units, government websites, and public safety video image information systems. The content includes provisions for information authenticity, information storage security, information collection requirements, and network device stability.

5 Conclusion

The birth of the Internet in the twentieth century and the development of the twenty-first century impacted the integration of the world and the integration of human destiny. The governance process of the US cybersecurity issue also reflects, to a certain extent, the continuous deepening of coordination and cooperation between European

and American countries and the continuous improvement of cyber security defense capabilities. First, the top-level design and organizational coordination at the supranational level are the backbone of US cybersecurity governance. The United States is currently facing a complex and ever-changing cybersecurity situation. The differences in network technology and popularity between countries and the differences in positions have increased the difficulty of unified governance. Although the US cybersecurity governance has achieved certain results, the internal contradictions in the US governance system and the externally complex cyberspace international landscape make the prospects for governance uncertain. Through a comparative study on the security governance of wireless networks in the United States, it is hoped that China can inspire digital forensics of wireless network crimes, and then think about wireless network security governance.

Funding information: No funding was used to support this study.

Author contributions: All authors contributed equally to this study.

Conflict of interest: There are no potential competing interests in our study. All authors have reviewed the manuscript and approved to submit to this journal. We confirm that the content of the manuscript has not been published or submitted for publication elsewhere.

Ethical approval: The article does not cover human or animal research. This article abides by ethical standards.

Data availability statement: This article does not cover data research. No data were used to support this study.

References

[1] G. Spruiell, *Psychoanalysis, identity, and the internet: Explorations into cyberspace*, A. Marzi, Ed., vol. 268, London, Karnac Books, 2018, pp. 392–397.
[2] V. A. Almeida, D. Doneda, and J. de Souza Abreu, "Cyberwarfare and digital governance," *IEEE Internet Comput*, vol. 21, no. 2, pp. 68–71, 2017.
[3] E. Y. Huan, G. H. Wen, S. J. Zhang, D. Y. Li, Y. Hu, T. Y. Chang, et al., "Deep convolutional neural networks for classifying body constitution based on face image," *Comput. Math. Methods Med.*, vol. 2, pp. 1–9, 2017.
[4] T. Stevens, "Cyberweapons: Power and the governance of the invisible," *Int. Politics*, vol. 55, pp. 482–502, 2018.
[5] J. Yang, "Guiding global governance in new frontiers guided with idea of community of shared destiny for mankind," *Contemp. World*, vol. 3, pp. 47–50, 2017.
[6] M. A. Terlizzi, F. D. S. Meirelles, and V. C. D. C. M. Alexandra, "Behavior of Brazilian banks employees on Facebook and the cybersecurity governance," *J. Appl. Secur. Res.*, vol. 12, no. 2, pp. 224–252, 2017.
[7] I. Stadnik, "What is an International Cybersecurity Regime and how we can Achieve it?" *Masaryk. Univ. J. Law Technol.*, vol. 11, no. 1, pp. 129–154, 2017.
[8] E. Casey, "The chequered past and risky future of digital forensics," *Australian J. Forensic Sci.*, vol. 51, no. 6, pp. 649–664, 2019.
[9] T. Baker, P. Buck, F. Iqbal, and Q. Shi, "The Internet of Things: Challenges and considerations for cybercrime investigations and digital forensics," *Int. J. Digital Crime. Forensics* (*IJDCF*), vol. 12, no. 1, pp. 1–13, 2020.
[10] S. Ramadhani, Y. M. Saragih, R. Rahim, and A. P. U. Siahaan, "Post-genesis digital forensics investigation," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 164–166, 2017.
[11] I. Cunha, J. Cavalcante, and A. Patel, "A proposal for curriculum development of educating and training Brazilian police officers in digital forensics investigation and cybercrime prosecution," *Int. J. Electron. Security Digital Forensics*, vol. 9, no. 3, pp. 209–238, 2017.
[12] L. Caviglione, S. Wendzel, and W. Mazurczyk, "The future of digital forensics: Challenges and the road ahead," *IEEE Secur. Priv.*, vol. 15, no. 6, pp. 12–17, 2017.
[13] K. H. Mohammed, Y. D. Mohammed, and A. A. Solanke, "Cybercrime and digital forensics: Bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria," *Int. J. Cybersecur. Intell. Cybercrime*, vol. 2, no. 1, pp. 56–63, 2019.
[14] S. Kumar, S. Pathak, and J. Singh, "An enhanced digital forensic investigation framework for XSS attack," *J. Discret. Math. Sci. Cryptogr.*, vol. 25, no. 4, pp. 1009–1018, 2022.
[15] C. Horan and H. Saiedian, "Cyber crime investigation: Landscape, challenges, and future research directions," *J. Cybersecur. Priv.*, vol. 1, no. 4, pp. 580–596, 2021.
[16] S. O. Baror, H. S. Venter, and R. Adeyemi, "A natural human language framework for digital forensic readiness in the public cloud," *Australian J. Forensic Sci.*, vol. 53, no. 5, pp. 566–591, 2021.
[17] J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park, "A blockchain-based decentralized efficient investigation framework for IoT digital forensics," *J. Supercomput.*, vol. 75, no. 8, pp. 4372–4387, 2019.
[18] Z. Huang, "Towards the international rule of law in cyberspace: Contrasting Chinese and western approaches," *Chin. J. Int. Law*, vol. 16, no. 2, pp. 271–310, 2017.
[19] F. Delerue, "Reinterpretation or contestation of international law in cyberspace?" *Isr. Law Rev.*, vol. 52, no. 3, pp. 295–326, 2019.
[20] I. Koto, "Cyber crime according to the ITE law." *Int. J. Reglem. Soc.* (*IJRS*), vol. 2, no. 2, pp. 103–110, 2021.