The Governance Mechanism and Legal System of European Union Cyberspace Security

Zhi Li [1], Yuemeng Ge[2], Jieying Guo[1]，Mengyao Chen[1]，Junwei Wang [1*]

[1] School of Media and Law, NingboTech University, Ningbo, China;

[2] School of Business, Zhejiang Fashion Institute of Technology, Ningbo, China

* Corresponding author: Junwei Wang, E-mail: lijiamin@nit.zju.edu.cn

Abstract: The whole world is making unremitting efforts to ensure the security of global cyberspace. The European Union (EU) has always regarded cyberspace security as the core competitiveness of regional integration and is committed to improving the cyberspace security legal system's construction. Now it has been at the forefront of the world. Through the analysis of the EU cyberspace security governance mechanism and legal framework, this study concludes that the construction of cyberspace security is a complex project that requires long-term exploration and development. Besides, a sound cyberspace-security governance mechanism and a perfect legal system of cyberspace security should have a clear hierarchy, and specific effectiveness and system, updating the laws and regulations.

Keywords: European Union, Cyberspace, Governance Mechanism, Legal System

Tob Regul Sci.™ 2021;7(5-1): 3698-3709

DOI: doi.org/10.18001/TRS.7.5.1.146

1. Introduction

Cyberspace is another essential living space for human beings in the Internet era. With the development of Internet technology, the form of cyberspace is extended and differentiated from social space. The new meaning of cyberspace is based on communication technology infrastructure, network data information, and human activities in applying information and communication technology. It supports the construction of a highly integrated and interactive artificial space with other spaces, reflecting cyberspace governance's uniqueness and the social value of cyberspace[1].

Of course, there are very prominent security issues in cyberspace, and these issues have even become one of the hot topics in the world. In the traditional concept, information security is the ability obtained by implementing a set of appropriate controls, which can be policies, conventions, procedures, organizational structures, and application functions[2]. These controls are established to ensure that unauthorized persons do not control the users' information and information system, so that information and operation can be identified. Meanwhile, the information and system are controllable, and their services can be provided to authorized persons at any time; thus, the users' specific security goals are met [3]. Therefore, cyberspace security is the key to studying information security issues in information acquisition, storage, transmission, and processing. Computer, electronics, communication, mathematics, physics, transmission, management, laws, and education are integrated to form cyberspace security, which has its own connotation, theory, technology and application, and serves cyberspace.

The security governance of global cyberspace is related to the overall situation of each country's security, economic and social

development, national interests, and the people's fundamental interests. It is the primary task of cyberspace governance. At present, countries all over the world are actively formulating the corresponding network security legal systems. The reason is that they have gradually realized that the network security laws are in a critical position in the global cyberspace governance system and the reform of the national governance system. They can guarantee national cyberspace security and safeguard national cyberspace's sovereignty, security, and development interests.

2. Challenges Faced by the EU in Global Cyberspace

With the rapid development of global network technology, human activities in cyberspace have become increasingly prosperous. Cybercrimes have filled cyberspace, such as cyber terrorism, cyber hackers, cyber viruses, spam, data leakage, and knowledge infringement. Simultaneously, with the vigorous development of network industries, such as cloud computing, big data, Internet of Things, and 5G networks, new forms of cybercrimes and security risks are also continually emerging, creating new challenges to the relevant corporate governance of the EU.

First of all, the network security risks of individual users have increased dramatically. According to the survey, there were 974 cases of network information and data leakage incidents in the first half of 2016 worldwide, and the total number of leaked records reached 554 million, an increase of 15% over 2015 [4]. In recent years, personal data leakage incidents in EU member states has increased sharply, and individual users' network security problems have become increasingly prominent. In Germany, for example, hackers hacked into the parliamentary network and stole 16G of confidential data in 2015. Moreover, in 2019, hundreds of German politicians' personal information was "exposed" on social networks, including bank card information and mobile phone numbers [5].

New types of cybercrimes have emerged. More and more organized cybercrimes begin to use the network sharing economy to disguise themselves as virtual services to defraud. The use of the "dark web" for illegal transactions and smuggling has become more secretive, and the payment methods for underground economic and criminal transactions have become virtual currencies, such as bitcoin.

Cyber terrorism uses the network to spread. Terrorist organizations train hackers to attack the target country's network infrastructure to conduct network smuggling and fraud for money and publish terrorist statements and claims by the network. For example, in June 2016, World-Check, the world's largest anti-terrorism database, was attacked. The personal information of about 2.2 million terrorists and suspects of criminal organizations was made public and sold on the dark web with marked prices. Terrorist organizations have become more skillful and professional in their publicity through website forums and social networks [6].

Finally, the EU faces the threat of cyber warfare. Member states, facing the increasingly difficult situation of cybersecurity, have accelerated the process of cyberspace militarization. France has also increased its cyber defense force and cutting-edge cybersecurity researchers. The conflict between Russia and Ukraine has spread to cyberspace, and the parties fight fiercely on the cyber front, which brings tremendous pressure to the EU countries.

Different scholars have different opinions on cyberspace's legal system, mainly based on network security laws, and formed by multi-level norms such as laws, administrative regulations, and departmental rules to guarantee network security [7]. As Liu Ran (2019) believed, cybersecurity legislation collects various laws and regulations formulated by different legislatures and legal norms regulating different network security issues[8]. Cybersecurity legislation is a dynamic legislative process, a

static legal document obtained from dynamic legislation, and a unity of the two.

Generally, the core cybersecurity legal system is divided into two categories. One is the amendment to the traditional information security system, such as monitoring and early warning, emergency response, and security management system. The other is the legislation on newly derived network issues, such as protecting critical information infrastructure and cross-border data flow. The focus of the cybersecurity legal system covers several systems, such as the maintenance of cyber sovereignty, protection of critical cyber infrastructure, cyber operation security, cyber monitoring, early warning, emergency response, cybersecurity review, cyber information security, and protection of all actors' rights and interests in cyberspace[9]. For this reason, countries have been exploring the useful modes of cybersecurity legal governance for global cyberspace.

3. Construction of the EU Cyberspace Security Governance Mechanism

With the advancement of European integration and the Internet era, the EU has constructed a more systematic cyberspace security governance framework, including governance mechanisms and regulations. The governance mechanisms are mainly responsible for policy formulation, personnel resource allocation, specific implementation, and effect evaluation. Policies and regulations are responsible for regulating the direction, principles, means, and security governance goals. The two complement each other and jointly build the EU's cyberspace security governance framework.

Before and after the Cybersecurity Strategy for the European Union was issued by the EU, member states have established cybersecurity management departments and gradually strengthened their cyber defense capabilities. Especially after the "Prism Event" in 2013, the cooperation between emergency response centers among members has become closer, and the EU's cybersecurity system has become increasingly complete. However, global cybersecurity governance requires government departments' leadership and the active participation of multiple stakeholders such as civil society and private sectors.

In global cyberspace, the EU's governmental departments responsible for building relevant governance mechanisms include the European Council, the European Parliament, and the European External Action Services (EEAS). They are responsible for formulating the overall policies. Among them, the departments responsible for situation research and policy formulation in the telecommunications and networks field include the Commission's Directorate-General for Communications Networks, Content and Technology (DG CNECT), the Transport, Telecommunications, and Energy Council (TTE) of the Council of the European Union, and the Industry, Research, and Energy Committee (ITRE) of the European Parliament. The Directorate-General of Internal Affairs is responsible for the jurisdiction of the EU's network data security. The General Information and Intelligence Department is responsible for the monitoring of cyber espionage. Although it is not a department in charge of cybersecurity, it must coordinate and cooperate with other departments regarding cyberspace affairs. As the EU's common diplomatic agency, the EEAS is responsible for the EU's cyber diplomacy.

In global cyberspace, the relevant governance mechanisms constructed by the EU mainly include the Public-Private Partnership (PPP), the Trust in Digital Life (TDL), the European Data Protection Supervisor (EDPS), the Cyber Security Incident Response Team (CSIRT), and the European Dialogue on Internet Governance (EuroDIG).

PPP refers to a model in which the government and the private sector reach a partnership on a project to jointly provide public products and services. In 2011, the EU launched the Future Internet Public-Private Partnership (FI-PPP) [10], which lays a good foundation for

the establishment of the Digital Single Market (DSM). The document indicated that, firstly, relevant departments should cooperate with more cybersecurity stakeholders to coordinate the relevant strategies, policies, regulations, rules, actions, and regulatory frameworks of the EU and member states' network governance departments. All parties' advantageous resources are integrated to promote the EU's data infrastructure's construction and deployment. Application of the EU's network technology is developed to improve various industries' digitization. Furthermore, efficiency and benefits are increased to accelerate the transformation and upgrading of the EU's digital economy.

The Trust in Digital Life Public-Private Partnership (TDL-PPP) is an organization proposed by the EU's Directive on security of network and information systems in 2009. This organization is a public-private partnership and funded by the EU's 7th Framework Programme. It aims to formulate a strategic network technology research and development agenda in line with European values to strengthen the public's awareness of personal data protection on the Internet [11].

EDPS is a supervisory organization established by the European Data Protection Authority to prevent personal data and privacy from being illegally used. This organization has set up an electronic data processing system, responsible for guiding this system and data protection departments. Besides, the organization is also responsible for supervising the process of using personal privacy and data by the EU's agencies within the EU's legal framework, as well as providing advice on the EU's legal framework of privacy and data protection.

The European Commission and member states have established corresponding cyber emergency response mechanisms. In order to deal with cyber threats, attacks, and vulnerabilities, and to enhance the capabilities of global-cyber situation awareness and incident response, the private sectors have also joined the ranks of cybersecurity mechanism construction, such as the Task Force on Computer Security Incident Response Teams (TF-CSIRT), the Trans-European Research and Education Networking Association (TERENA), the Forum of Incident Response and Security Teams (FIRST), and the European Government CERTs (EGC) Group. The EGC Group is mainly composed of the UK Computer Security Incident Response Team and the German Internet Emergency Response Team.

EuroDIG is an open cyberspace governance dialogue platform belonging to civil society. It was established by government representatives, network public policy organizations, and relevant scholars in 2008. The purposes of EuroDIG are to promote the multi-party participation and dialogue of European network governance, share professional knowledge and practical experience of various departments, and find the cooperative foundation for shared governance. It is co-funded by the European Council, the European Commission, the European Regional At-Large Organization (EURALO), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Society (ISOC), and other institutions.

4. Characteristics of the EU's Cyberspace Security Legal System

Since the popularization of the Internet in Europe, the EU has formulated a series of laws to guide and regulate the Internet's development in technology and management. With the advancement of European integration, the EU has continuously abolished the old and out-of-date regulations, formulated new laws, and gradually constructed and improved the legal system framework, ensuring the EU's cyberspace's order and security. The EU's Internet legal system is divided into three types: the macro strategy of network development, the specific Internet management system, and the technical specifications and standards. Table 1 shows the EU's cybersecurity regulatory system, taking typical regulations promulgated by the EU as

examples.

Table 1. List of the EU's Cyberspace Security Laws and Regulations

No.	Date of establishment	Name of laws and regulations
1	1992	Council Decision of 31 March 1992 in the Field of Security of Information Systems
2	1995	Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications; Data Protection Directive
3	1998	Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations
4	1999	1999/364/JHA: Common Position of 27 May 1999 Adopted by the Council on the Basis of Article 34 of the Treaty on European Union, on Negotiations Relating to the Draft Convention on Cyber Crime Held in the Council of Europe; Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks; Electronic Signatures Directive
5	2000	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce)
6	2001	Cyber-crime Convention; 2002/16/EC: Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, Under Directive 95/46/EC

7	2002	Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Area of Network and Information Security; Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on Access to, and Interconnection of Electronic Communications Networks and Associated Facilities; Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the Authorisation of Electronic Communications Networks and Services; Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services; Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector; Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 Concerning the Distance Marketing of Consumer Financial Services and Amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC; Council Framework Decision on Attacks Against Information Systems
8	2003	Opinion of the Economic and Social Committee on the "Proposal for a Decision of the European Parliament and the Council Amending Decision No 276/1999/EC Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks"; Council Resolution on a European Approach Towards a Culture of Network and Information Security; Council Resolution of 18 February 2003 on the Implementation of the Europe 2005 Action Plan; Decision No 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 Adopting a Multiannual Programme (2003-2005) for the Monitoring of the Europe 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security
9	2004	Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency

10	2005	Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems; Decision No 854/2005/EC of the European Parliament and the Council of 11 May 2005 Establishing a Multiannual Community Programme on Promoting Safer Use of the Internet and New Online Technologies
11	2006	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or Public Communications Networks and Amending Directive 2002/58/EC; Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection; Guidelines on Information and Data Supervision
12	2007	Decision 2007/124 - 2007/124/EC, Euratom: Council Decision of 12 February 2007 Establishing for the Period 2007 to 2013, as Part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention, Preparedness and Consequence Management of Terrorism and Other Security-Related Risks; Commission Decision of 21 February 2007 on Allowing the Use of the Radio Spectrum for Equipment Using Ultra-wideband Technology in a Harmonised Manner in the Community; Council Resolution on a Strategy for a Secure Information Society in Europe
13	2009	Communication from the Commission to the European Parliament, the Council, the European Economic, and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience"; Directive on Data Storage in Local Terminals of European Users
14	2010	Digital Europe Programme
15	2011	Security Protocol of Electronic Tags and Personal Information Protection
16	2012	Communication from the Commission to the European Parliament, the Council, the European Economic, and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century

17	2013	EU Cybersecurity Strategy: an Open, Safe and Secure Cyberspace; Directive Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union; Directive on Attacks Against Information Systems; Digital Single Market Strategy; General Data Protection Regulation; EU Net Neutrality Laws
18	2015	Digital Single Market Strategy; EU Net Neutrality Laws
19	2016	Directive on Security of Network and Information Systems
20	2017	General Data Protection Regulation
21	2018	General Data Protection Regulation
22	2019	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Therefore, the EU's cyberspace security legal framework is not achieved overnight. With the European Council's joint efforts, the European Parliament, and other official missions and member states, it has been continuously adjusted and improved for more than ten years according to the progress of Internet technology and economic and social development. The legal framework of the EU's cyberspace security is a multi-level legal system constructed by the EU's integrated legislation, member states' national legislation, comprehensive legislation, and special legislation. The system aims at ensuring the EU's cyberspace security and has distinct features such as structure, content, and implementation measures.

Firstly, the EU's cyberspace security legal framework goes beyond countries and member states. Because of its prominent status, the EU has the right to enact the laws applying to all EU member states. Generally, the European Commission proposes a legislative bill, then submits it to the European Council for review and decision-making, and finally submits it to the European Parliament for voting. Once the bill is passed, its legal force covers all EU member states. However, as independent sovereign states, member states have the right to enact relevant national cybersecurity laws without violating the EU's cyberspace security legal framework. For example, in 1997, Germany promulgated the Information and Communication Services Act, Italy passed the Digital Signature Act, and in 2002, the UK issued the Electronic Commerce (EC Directive) Regulations. From the perspective of legal force, the laws directly enacted by the EU are in the priority position and have the force of priority and direct application. The relationship between the EU's laws and member states' laws is different from that between international laws and domestic laws and between federal statutes and US member states' statutes. Although the EU's laws' two principles of direct application and priority are not explicitly stipulated, the European Court of Justice has recognized them in the judicial process. For instance, the Directive on Electronic Commerce in 2000 and the Council Resolution on a European Approach Towards a Culture of Network and Information Security in 2003 are above the legal force of member states in corresponding fields.

Secondly, the EU's cyberspace security legal framework includes the mandatory provisions and the guiding "soft laws." Due to the different origins of the EU's laws, the legal forces have some differences. The legal framework mainly includes regulations, directives, decisions, recommendations, and proposals. Among them, regulations have supreme legal authority, general applicability, and comprehensiveness, such as the

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (ENlSA). Directives are used most frequently and have significant impacts. They usually only come into force for individual member states and are necessary means of coordinating member states. Decisions, recommendations, and proposals are merely constructive comments of the EU to member states on specific issues. They are not legally binding on member states and belong to the "soft laws."

Thirdly, the EU's cyberspace security legal framework embodies the combination of general and special provisions. The EU's legal framework has macroscopic and general provisions for network and information security and special provisions for specific issues from the legal norms' content. The EU has an extensive legislation system for network and information security and will revise existing laws and regulations according to changing circumstances to adapt to the new developments. For example, the Council Decision of 31 March 1992 in the Field of Security of Information Systems clearly emphasizes that information security is essential for promoting the harmonious development of the whole economy, improving the people's living standard, stabilizing the society, and uniting the member states. It also points out that the cooperation between the EU and member states, between member states, and between other relevant stakeholders should be valued in action. The decision also reflects the "appropriate protection" principle of information security and requires the law to coordinate the relationship between public and private interests. In general, this is a milestone decision opening a new chapter in constructing the EU's information security legal framework. Although new technologies make some of the provisions in this decision outdated, it is still frequently cited today. The key is that many concepts in this decision have instructive value.

Finally, the EU's cyberspace security legal framework focuses on new security threats to update the legal norms in time. While fighting against security threats such as malicious code, phishing, spam, and illegal websites, the EU is also constantly suffering from new security risks, so its legal norms will be considered updating timely. For example, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse was formally established in 2007. Due to the rapid popularization of the Internet, some criminals use the Internet to produce and spread child pornography and sexually exploit and abuse children, seriously endangering children's growth. Therefore, this convention came into being in this new situation. Besides, the EU also revises the existing legal norms to solve new problems. A typical example is a Decision No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 Amending Decision No 276/1999/EC Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks. EU's lawmakers firmly grasp the concept of "old laws are difficult to solve new problems" and continuously promote the updating of laws and regulations on the road of technological development to respond to the new situations fully.

Consequently, the EU's legal framework of global cyberspace security has its characteristics, distinct levels and features, and detailed regulations on specific issues. In terms of legal force, the EU pays attention to the combination of mandatory legal norms and guiding legal norms, respects each country's specific national conditions, and allows member states to use legal norms according to their national conditions under the general guidelines.

5. Lessons from the EU's Cyberspace Security Legal System

5.1 Advantages of the EU's Global Cyberspace Security Legal System

The EU has constructed a global cyberspace

security legal system in a leading position globally and has established a comprehensive and balanced cyberspace security strategy. The supporting cyberspace security system established by the EU covers all member states so that the legislation of cyberspace security among member states can be relatively balanced under the EU's coordination. Moreover, establishing a unified jurisdiction system related to cybercrime is conducive to the combat and punishment of cybercrime.

For example, in terms of the critical infrastructure protection policies, the Cybersecurity Strategy for the European Union takes the construction and protection of cyberinfrastructure as its strategic priorities, so the member states attach great importance to the construction and protection of cyberinfrastructure. The member states achieve balanced and high-speed network coverage by strengthening the network popularizing rate and networking broadband and other infrastructures in each country. Meanwhile, the relevant legal and policy documents clarify the cyberinfrastructure as a provision, laying a foundation for cybersecurity's fundamental development.

The EU also pays attention to developing core cybersecurity technologies and the popularization of basic network skills. The EU's cyberspace security legal system focuses on the protection of independently developed core cybersecurity technologies. It focuses on the construction of research and defense systems of core cybersecurity technologies and the education of netizens and the network industry's development policy, playing a role in the skill training and knowledge popularization of network users.

Besides, the EU focuses on combating cybercrime. Under the joint action of Europol and the ENISA, the EU has launched a comprehensive crackdown on various cybercrimes. The traditional forms of crime, such as cyber economic crimes, cyber smuggling, and cyber fraud, have been controlled to a certain extent. The EU also focuses on researching and combating new types of cybercrimes to prevent and punish crimes.

Finally, international cooperation is useful for the EU's cybersecurity governance. Through strengthening the cooperation within the EU's member states and with global strategic partners, and involving stakeholders such as non-governmental organizations, private enterprises, and scientific research institutions, the EU's cybersecurity governance becomes more comprehensive and efficient.

4.2 Inadequacy of the EU's Cyberspace Security Legal System

First, whether viewed from the perspective of digital illiteracy or digital technology's popularity, the degree of social citizens' free access to the Internet is still restricted. Moreover, although it is theoretically possible to combine crime rates in different countries, crime statistics are affected by differences in national legislation and can not summarize the reliable data of the EU's overall cybercrime rate. Except for some significant cybercrime cases reported publicly, there is little data available for quantitative assessment. Therefore, it hinders the countries from fighting against cybercrime jointly.

Multi-stakeholders play essential roles in the cyberspace governance model. Co-governance with multi-stakeholders can achieve democracy and efficiency. However, the disadvantage is that the EU only focuses on constructing critical information infrastructure and combating cybercrime, without considering the overall situation. Related policies are lacking in defense. The Cybersecurity Strategy for the European Union, for example, due to many members and the complexity of the organization, the network organization structure is cumbersome. There are overlaps between institutions, the rights and responsibilities are unclear, and the empowerment is repeated. Meanwhile, the countries have different legal concepts, network development levels, and network infrastructures, resulting in different vital points of the

cyberspace security legal system construction and different degree of the cybersecurity legal system construction. Once a network security incident occurs, internal coordination and communication are required, reducing the incident processing efficiency.

4.3 Inspirations for the Cooperation between China and the EU in Cybersecurity

China and the EU have maintained long-term cooperation in the field of global cyberspace. By analyzing the logic and policies of the two sides' external actions, this study can provide some strategic suggestions for China to carry out cyber diplomacy and cybersecurity cooperation with Europe.

First, to achieve the top-level design and strategic docking. The Belt and Road Initiative of China has the goal of connecting and integrating Eurasia. The "Thirteenth Five-Year Plan" of China has proposed to list the "Online Silk Road" as a priority for future development to open up the information channels from Russia to Central and Eastern Europe. Efforts should be made to narrow the digital divide among countries along the Silk Road and achieve interoperability so that people from countries can share the convenience and benefits of network development. In July 2015, the China-EU Digital Cooperation Roundtable was held in Brussels. The two parties signed the Letter of Intent for Cooperation to build the digital Silk Road, aligning the Belt and Road Initiative of China and the EU's Juncker Plan. In the future, China and the EU will carry out all-round and multi-stakeholder cooperation in big data, cloud computing, e-commerce, and the Internet industry. Therefore, the two sides decided to establish the China-EU Internet Forum and the Center for China-EU Internet Policy and Strategic Studies to promote cooperation. In the meantime, China should strengthen cooperation with the network emerging countries and safeguard the developing countries' cyber sovereignty and interests. When hosting the World Internet Conference Wuzhen Summit, the EU's official and non-governmental organizations should be actively invited to build consensus and seek cooperation.

Besides, China should cooperate with the EU based on safeguarding cyber sovereignty. The EU and the United States have repeatedly advocated the open and free network concept on international multilateral cooperation platforms and attempted to use their Internet dominance to erode the cyber sovereignty of developing countries, arousing countries' vigilance. Therefore, when conducting cyber diplomacy with the EU, China should carry out practical cooperation based on the principle of mutual respect for sovereignty and be wary of European countries using "cyber human rights," freedom of speech, and intellectual property rights as excuses to engage in economic blackmail. The overseas enterprises' legal operations in cyberspace should be regulated, and the dissemination of illegal information should be controlled. China can learn from the EU's advanced cybersecurity legislation to improve the national cyber governance legal framework. China and the EU should manage disputes based on seeking common ground while reserving differences and increasing the scope and depth of bilateral cooperation on cybersecurity.

Finally, the business community should be encouraged to carry out "Track II Dialogue" with the EU. China can appropriately learn from the PPP model and encourage enterprises, universities, and non-governmental organizations to participate in cybersecurity governance with enthusiasm and creativity. Relevant departments shall provide support for fund procurement, technology research and development, and public opinion supervision.

6. Conclusions

By analyzing the EU's cyberspace security governance mechanism and legal system, it is concluded that the construction of cyberspace security requires long-term exploration and development. A sound cyberspace-security governance mechanism and a complete cyberspace security legal system should have

clear hierarchies, specific effective grades, and systematic content, updating laws and regulations.

EU's cybersecurity governance mechanism has apparent uniqueness. The subject of cyberspace governance has a supranational and multi-level structure, where the EU, member states, and multi-stakeholders all participate in the governance process. Cyberspace governance is complex and changeable and has its special distribution with cybersecurity threats in other parts of the world. The EU's cyberspace governance pays attention to legislation and institutional construction instead of attack and hard power, with distinctive EU characteristics.

However, the EU's cybersecurity governance legal system shows that the EU still has many problems and faces a series of challenges in terms of laws and regulations. The rapid development of new technologies leads to the endless emergence of cybersecurity vulnerabilities and new attack methods. Although the supranational system can fully coordinate the member states' interests and maintain common security, under the current situation of domestic turmoil and foreign aggression, it is difficult for the EU to do something due to insufficient legitimacy and dominant right. In terms of international cooperation, the lack of autonomy and excessive advocacy of values also make the EU lack authority and speaking right. Therefore, it is difficult for the EU's governing philosophy to gain wide recognition.

Of course, the EU cyberspace security legal system is not a single code of conduct for cyberspace, but a cyberspace security strategic plan integrating the EU's interests. It serves the strategic needs of the EU in political, economic, social, and security aspects. Although the EU faces many difficulties in cyberspace security governance, its cybersecurity strategy has reference significance for the joint response to cyberspace security issues and the construction of international cybersecurity cooperation. When China participates in cyberspace security governance, it is worth learning.

Acknowledgments

This work was supported by the National Social Science Fund of China of the Youth Project “A Comparative Study on the Laws of Global Cyberspace Security Governance and Its Enlightenment to China” (Grant No. 19CXW039).

Reference

1. Li Zhi. (2020), The Concept Prototype, Deduction and New Meaning of Cyberspace. China Media Report, 19(2): 12.
2. Fang Binxing. (2008), Yin Lihua. Research on the Definition of Information Security. Netinfo Security, (1): 8-10.
3. Shen Changxiang, Zhang Huanguo, Feng Dengguo, et al. (2007), Overview of Cybersecurity. Scientia Sinica (Technologica), (02): 129-150.
4. Wang Ling. (2017), 2016 Data Leakage Incident Report: 974 Cases Have Been Exposed in the First Half of the Yea. Guangming Online, 10(01).
5. Yang Xiaoxi.(2019), Personal Information of Hundreds of Politicians in Germany Leaked[N]. Chnia Minutes,7(01).
6. United States Homeland Security Advisory Council. (2007), Report of the Future of Terrorism.
7. Nicolas Huppenbauer, Li Lei, Yang Le. (2019), Cybersecurity Principles and Topics in the EU and China: a Comparison of Laws and Strategie. Information Security and Communications Privacy, (09): 58-69.
8. Cheng Lin. (2017), Comparative Study on Cyber Security Legislation between China and the United States. Beijing: People's Public Security University of China Press, 87.
9. Li Yuxiao, Wu Hequan, Xie Yongjiang, et al. (2016), A Study on the Improvement of the Cybersecurity Legal System in China[J]. Strategic Study of CAE, 18(06): 28-33.
10. Sluijs, Jasper P, P. Larouche, et al. (2011), Cloud Computing in the EU Policy Sphere. Social Science Electronic Publishing, 36(1): 12-32.
11. Wilikilagi V. (2009), What is Network Governance and its Implications for Public Policy Formulation? Social Science Electronic Publishing.