Doctoral (PhD) Dissertation Abstract

ISSUES ON CYBERCRIME IN CHINA: THEORY AND PRACTICE

Song Dawei

Supervisor: Dr. Madai Sándor, PhD

University of Debrecen

Marton Géza Doctoral School of Legal Studies

Debrecen, 2022

I. Research Background and Objectives

Nowadays, it's easy to think how inconvenient living in a time and space without the Internet would be. From the necessities of People's daily life to the social and economic development, and then to the high-tech competition between countries, all aspects of human society are accompanied by the shadow of the Internet. No one could have imagined at the time that the Advanced Research Projects Agency Network (ARPANET), funded by the U.S. Department of Defense to secure military communications during the Cold War, would evolve over decades into an Internet that would connect people around the world and have such a profound impact on the world as a whole.[1] From the popularity of the Internet for commercial and civil use in the mid-1990s to today[2], after more than 20 years of social changes and technological progress, people's demand for the Internet has developed from access to the Internet to open the door to a new world to more diversified experiences such as innovation and cybersecurity. Technological development is also actively responding to people's needs at more levels, mainly reflected in the popularity of a series of information network technology concepts in recent years, such as Meta-universe[3], 5G, Artificial Intelligence, Big Data, Blockchain, Cloud Computing and so on. However, the progress of information network technology cannot solve the fundamental malpractice of the Internet --- cybercrime.

Cybercrime has been around since the dawn of the Internet. Before the formal commercial and civilian adoption of the Internet, especially in the United States, it mainly existed in local area networks (LANs) and was used primarily between national security systems, high-tech information systems, and universities.[4] The birth and initial development of computers make a group of college students interested in it. However, due to the scarcity and high cost of computers and the closed nature of information networks at the initial stage, these college students with strong interest and enthusiasm in computers and networks cannot get corresponding opportunities to get close to and understand computers and networks. Therefore, sneaking into these closed computer systems seemed the only chance for students

---

[1] BARRY M. LEINER, VINTON G. CERF, DAVID D. CLARK, ROBERT E. KAHN, LEONARD KLEINROCK, DANIEL C. LYNCH, JON POSTEL, LARRY G. ROBERTS AND STEPHEN WOLFF: *Brief History of the Internet*. Internet Society, 11 November 2021. https://www.internetsociety.org/internet/history-internet/brief-history-internet/

[2] MAJID YAR: *Cybercrime and Society*. Sage, 2013. 2nd Edition, p. 20.

[3] DAN MILMO: *Enter the Metaverse: The Digital Future Mark Zuckerberg is Steering us Toward*. The Guardian, 11 November 2021. https://www.theguardian.com/technology/2021/oct/28/facebook-mark-zuckerberg-meta-metaverse

[4] SUSAN W. BRENNER: *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston, Northeast University Press, 2012. Chapter 1.

who have no direct access to computers to learn about computer networks. It is also the embryonic form of hacking of cybercrime.[5] With the iterative innovation of technology and the popularization and development of the Internet, cybercrime itself is constantly "evolving." As a result of this evolution, cybercrime, which was initially a by-product of information networks, can now directly affect the development of information networks. In other words, people's anxiety about cybercrime has directly affected their acceptance and tolerance of the Internet.

Every year, governmental agencies of many countries, international organizations, cybersecurity enterprises, academic groups have made reports on the specific indicators of harm caused by cybercrime, such as economic losses, distribution of cybercrime victims, and the number of cybercrimes. For example, from a global perspective, the *2020 Internet Crime Report* published by the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation in the United States noted that: Over the last five years (2016-2020), the IC3 had received 2,211,396 complaints across the globe in total. These cybercrime complaints amounted to a total economic loss of 13.3 billion dollars.[6] In terms of Cybercrime in China, at the 4th Session of the 13th National People's Congress in 2021, the Work Report of the Supreme People's Court showed that China's courts had trialed 33,000 cybercrime cases in 2020.[7] According to the Work Report of the Supreme People's Procuratorate, China's procuratorial system prosecuted 142,000 people for cybercrime in 2020, up 47.9 percent year-on-year amid a decline in the total number of criminal cases.[8]

Taken as a whole, the release of these reports indicates a high level of social concern about cybercrime. On the one hand, such increasing attention shows that the rising harm degree of cybercrime has to attract society's attention. On the other hand, it also indicates the consensus reached by governments worldwide, different international organizations, and social organizations: cybercrime urgently demands governance.

Generally speaking, cybercrime governance means that the country uses a series of legal means, such as legal policies, legislation, law enforcement, judicial, and non-legal means,

---

[5] STEVEN LEVY: *Hackers: Heroes of the Computer Revolution*. New York, Anchor Press/Doubleday, 1984. pp. 18-69.
[6] INTERNET CRIME COMPLAINT CENTER (IC3): *2020 Internet Crime Report*. Federal Bureau of Investigation, 11 November 2021. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[7] QIANG ZHOU: *Work Report of the Supreme People's Court of 2021*. The Supreme People's Court of The People's Republic of China, 21 November 2021, http://www.court.gov.cn/zixun-xiangqing-290831.html
[8] JUN ZHANG: *Work Report of the Supreme People's Procuratorate of 2021*. The Supreme People's Procuratorate of The People's Republic of China, 21 November 2021, https://www.spp.gov.cn/spp/gzbg/202103/t20210315_512731.shtml

such as social policies, to reduce and deal with the occurrence of cybercrime, remedy the infringement caused by cybercrime, and finally achieve the effect of cybercrime control. In recent years, cybercrime governance has become an essential part of the world's crime governance. On the one hand, countries worldwide strengthen cybercrime control by constantly improving policies, management, and cyber legislation, such as the *Cybersecurity Enhancement Act of 2014*, *Cybersecurity Information Sharing Act of 2015*, *Federal Exchange Data Breach Notification Act of 2015*, and *National Cybersecurity Protection Advancement Act of 2015* in the United States. On the other hand, in response to cybercrime globalization, international and regional organizations and treaties are also constantly improving the legal network of cybercrime control. For example, on 14 April 2016, European Union adopted the *General Data Protection Regulation*.

Of course, the global governance of cybercrime based on the guiding ideology of building a community of human cyberspace is inseparable from China's practice and lessons. Since the *Reform and Opening-up Policy* was adopted in the late 1970s, China has made significant economic and social development progress. As the largest developing country in the world, according to the statistics of the World Bank in 2020, China's WORLD GDP Ranks only next to the United States and the European Union, making China the third-largest economy in the world.[9] In recent years, the Chinese government has advocated the transformation of economic development mode and begun to attach importance to the positive role of the Internet in economic and social construction. The concept of "Internet Plus" was first proposed by Chinese Premier Li Keqiang in the *Government Work Report of 2015*. Specifically, the "Internet plus" action plan is formulated to promote the combination of mobile Internet, cloud computing, big data, and Internet of Things (IoT) with modern manufacturing, promote the healthy development of e-commerce, industries, and finance, and guide Internet enterprises to expand the international market.[10] In the *Government Work Report of 2020*, Premier Li Keqiang reiterated and stressed the importance of "Internet Plus" in an all-around way to create new advantages of the digital economy.[11] Under the government's advocacy of the Internet, China's social economy is increasingly showing the characteristics of Internet integration. It has created representative "business cards" with

[9] THE WORLD BANK: *GDP Ranking: Gross Domestic Product Ranking Table*. The World Bank, 12 November 2021. https://datacatalog.worldbank.org/search/dataset/0038130/GDP-ranking
[10] LI KEQIANG: *Government Work Report of 2015*. The State Council of People's Republic of China, 11 November 2021. http://www.gov.cn/guowuyuan/2015-03/16/content_2835101.htm
[11] LI KEQIANG: *Government Work Report of 2020*. The State Council of People's Republic of China, 11 November 2021. http://www.gov.cn/guowuyuan/2020zfgzbg.htm

Chinese features, such as sharing economy, mobile payment, 5G technology, Tik Tok. The high affinity of the Chinese economy and society to the Internet, on the one hand, promotes the vigorous development of Internet technology in China; on the other hand, it also brings risks and challenges -- an increasingly high incidence of cybercrime.

To cope with the risks and challenges brought by cybercrime and protect the development of China's Internet economy, China is constantly taking a litany of measures to achieve cybercrime governance. In particular, over the past decade, Chinese leaders have repeatedly issued statements in the international community on combating cybercrime and safeguarding cybersecurity. At the same time, China is constantly revising existing laws and formulating new laws, regulations, and policies to improve the governance capacity of cybercrimes. China's cybercrime governance practice has achieved remarkable results. According to the Law-and-Order Index of Gallup, China ranks the third safest country globally. [12] The ranking can be interpreted as saying that China is one of the safest countries in the world (including cybersecurity recognition).[13] It is worth mentioning that China is the most populous country in the world. Chinese people's high evaluation of China's security experience based on law and order also reflects the achievements of China's cybercrime governance practice from one side. Therefore, it is of positive learning significance to discuss China's cybercrime governance practice and experience in the context of global cybercrime governance. Furthermore, nothing in the world is perfect, nor is China's practice of cybercrime control. It is also of reference significance to fully understand cybercrime governance through discussions of the shortcomings in the praxis of China's cybercrime governance.

To sum up, this dissertation takes the issues of cybercrime in China as the theme. By sorting out, analyzing, and discussing the practice of cybercrime governance in China and summarizing the issues in China's practice, the following research objectives can be achieved:

(1) Develop a criminological definition of cybercrime and a holistic understanding of cybercrime.

(2) Summarize and assess China's domestic and regional international legal mechanisms for governing cyberspace and cybercrime.

---

[12] JULIE RAY: *Most of the World Remains Confident in Police, Feels Safe*. Gallup Inc., 12 November 2021. https://news.gallup.com/poll/322565/world-remains-confident-police.aspx

[13] CCTV NEWS: *China is "one of the most secure countries in the world" The national public security index in 2020 is 98.4%*. CCTV. COM, 12 November 2021. https://news.cctv.com/2021/04/15/ARTIAuqN0sAjdiQh6rGWd15y210415.shtml

(3) Analyze and summarize China's conviction practice and experience with cybercrime governance.

(4) Conduct research and analysis on the practice and current state of sentencing in China's cybercrime governance.

II. Research Status in China

Based on collecting, analyzing, and researching the results of the bibliometric analysis and classification analysis of 530 sampled literature, this dissertation holds that Chinese scholars' research on cybercrime in the past decade (2011-2020) presents the following characteristics:

First, more emphasis is placed on the response to cybercrime, and less attention is paid to the explanation of cybercrime (the use of criminological theory to explain cybercrime research). Chinese scholars' research on the response to cybercrime was relatively concentrated in the study of cybercriminal law science. There was a significant correlation between the study of cybercriminal law science and the response to cybercrime (χ^2=51.519, p=.001, α=.05). Meanwhile, there was a significant correlation between the response to cybercrime and the form of criminal justice (χ^2=13.247, p=.001, α=.05). It indicates that the research on criminal justice of cybercrime is usually inclined to discuss the response to cybercrime. In other words, Chinese scholars generally study the criminal justice issues of cybercrime to realize the governance of cybercrime.

Second, from a comprehensive perspective of the basic criminal law theory and the involvement of crimes in China's Criminal Code, the research form of criminal law dogmatics occupies a relatively dominant position. There was a significant correlation between the research form of criminal law dogmatics and offenses in China's Criminal Code (χ^2=130.188, p=.001, α=.05). It can be interpreted as that the research object of Chinese scholars' criminal law dogmatics of cybercrime is usually the offenses stipulated in the current Chinese Criminal Legislation or usually involves the provisions of the specific Criminal Code. At the same time, there was a significant correlation between the research form of criminal law dogmatics and the basic criminal law theory (χ^2=189.522, p=.001, α=.05). It could be understood that Chinese scholars focused not only on specific offenses in Criminal Code but also on the study and interpretation of cybercrimes from the perspective of basic criminal law theories, such as the theory of accomplice.

Third, it focused on international governance of cybercrime and non-Chinese practices and lessons. Chinese scholars' research on the internationalization of cybercrime was significantly correlated with cyberspace governance practice (λ=.364, p=.001, α=.05), but not with cybercrime governance and the cybercriminal policy (λ=.052, p=.542, α=.05). It indicated that the internationalization studies of Chinese scholars usually focus on cyberspace governance practice internationally or abroad and less on the governance and criminal policies of cybercrime.

Fourth, Chinese scholars have recognized the impact of the uniqueness of cyberspace on the real world. It is manifested as both the influence on traditional crime and rights and the salience of minority groups. And studying this effect requires a different approach. There is a significant correlation between the study of juvenile or minority groups and the response to crime (χ^2=4.641, p=.031, α=.05). It indicates that Chinese scholars' research on cybercrime for minors and minority groups usually focuses on the response to cybercrime of such notable groups, manifested explicitly in particular groups' crime prevention and regulation.

Finally, it is relatively insufficient that only 16 studies concerned cyber policy, cyber law, and cybercriminal law together, accounting for 3.01% of the total sample. It is also an essential embodiment of the research significance of this doctoral thesis.

III. Methodologies Applied in this Dissertation

In general, the research methods of this dissertation include normative analysis and empirical analysis. Specifically:

Chapter II mainly adopts literature analysis, comparative analysis, and legal doctrines in the overview of cybercrime. By sorting out the different definitions of cybercrime in various studies and combining them with comparative discussions, this chapter redefines cybercrime from the perspective of criminology. This chapter sorts out different theories on the morphological classification of cybercrime and discusses the morphology of cybercrime in China in combination with the specific provisions and legal doctrines of China's criminal law. Finally, Chapter II compares and evaluates the advantages and disadvantages of different criminological frameworks in understanding and explaining cybercrime by sorting out various criminology theories and their applications in cybercrime.

Chapter III mainly adopts literature analysis, historical analysis, descriptive analysis, and institutional analysis in China's legal means of cyberspace and cybercrime governance. Chapter III introduces the basic characteristics of China's legal system through institutional

analysis. Second, through legal search and literature analysis, this chapter collects relevant policy documents and legal texts in China and analyzes and describes the content and characteristics of laws related to cyberspace governance and cybercrime governance. Meanwhile, Chapter III examines the evolution of legislation to protect the same legitimate rights and interests in China's legal system and introduces and comments on the evolution of China's legal system of cybercrime governance in chronological order. Finally, Chapter III mainly presents the current situation of China's participation in regional international cooperation in the governance of cyber affairs through the literature analysis and descriptive analysis of the SCO treaties and declarations. Chapter III does not look at the representations of various laws and policies in isolation but systematically analyzes China's cybercrime governance policies, rules, and regulations to reflect the coherence of policies and legislation.

Chapter IV mainly adopts literature analysis, legal dogmatics, qualitative analysis, functional analysis, and case analysis in the reflection and evaluation of the conviction practice of China's cybercrime governance. In researching cybercrime policy and human rights protection, this section focuses on legal dogmatics and functional analysis and discusses the balance between the Internet real-name system and cybercrime prevention and human rights protection. In researching the extension of the criminal law interpretation of cybercrime, this section emphasizes case analysis and qualitative analysis. It explores the conflict and way out between China's crackdown on online obscene live streaming crimes and the principle of legality in criminal law. In researching the direction of cybercrime legislation and policy, this section mainly uses case analysis, legal dogmatics, and qualitative analysis to explore the culpable possibility of online platform operators and the legislative direction and policy options to protect the Internet sharing economy.

Chapter V mainly adopts theoretical analysis, case analysis, descriptive statistical analysis, correlation analysis, and regression analysis in the research on the sentencing practice of China's cybercrime governance. Chapter V takes the Chinese cybercrime sentencing disparities in judicial practice as the main research object. Chapter V establishes the theoretical framework to guide the research through theoretical analysis and literature analysis first; through case analysis, which establishes the research sample; through descriptive, correlation, and regression analysis, which studies both the legal and extra-legal factors affecting sentencing disparities of cybercrime in China's judicial practice.

IV. Layout and Structure of Dissertation

This dissertation consists of six chapters. Details are as follows:

The first chapter is the introduction. The first chapter mainly introduces the research background, research significance, research method, research layout and writing structure, as well as the new contribution of this research.

The second chapter provides an overview of cybercrime. The second chapter is mainly composed of three parts: the first is to redefine cybercrime from a criminological perspective. The second is to study the morphology of cybercrime. The third is the understanding and interpretation of cybercrime by sociological approaches in criminology.

The third chapter researches the legal means system of China's governance of cyberspace and cybercrime. The third chapter studies China's current legal means for cyberspace and cybercrime governance from domestic and regional international dimensions. Specifically, the third chapter mainly includes five parts: First is the basic characteristics of China's legal system. The second is China's cyber policies on the governance of cyberspace and cybercrime. The third is China's cyber law. Fourth is China's cybercriminal law. The fifth is the status quo of China's participation in regional international cyber affairs governance based on the Shanghai Cooperation Organization.

The fourth chapter researches the conviction practice of China's cybercrime governance. The fourth chapter is mainly based on China's current cybercriminal policy and criminal legislation doctrine. The fourth chapter mainly includes three parts: The first is to study the dynamic balance between cybercrime prevention and human rights protection. This part mainly reflects and evaluates China's Internet real-name system. By analyzing the legislative evolution of the Internet real-name system and its specific application in China, this part discusses its role in preventing cybercrime and its impact on human rights protection. The second is to study the principle of legality in criminal law and the explanation's extension of the current criminal legislation. This part mainly reflects and evaluates China's crackdown on online obscene live streaming crimes. Through the analysis of specific cases and the theoretical analysis of relevant legislation, this part discusses the direction of explanation and extension of current criminal legislation and its relationship with the principle of legality in criminal law. The third is to study the cybercrime governance and culpable possibility of online platform operators under the Internet sharing economy. This part mainly analyzes the case of DiDi in China. By analyzing the culpable possibility of online sharing economy

platform operators, this paper explores the relationship between the future direction of cybercrime governance and ensuring the healthy development of the Internet (economy and technology) in accordance with Chinese criminal law.

The fifth chapter researches the sentencing practice of China's cybercrime governance. Chapter V focuses on empirical evidence regarding the criminal justice practice of the *Crime of illegal utilization of information network technology* [Article 287(I)] and the *Crime of provision of assistance to conduct the cyber-criminal activity* [Article 287(II)] as stipulated in Amendment (IX) of Chinese criminal law. Chapter V summarizes the above two offenses as auxiliary cybercrime. The empirical analysis of criminal justice practice involved in the fifth chapter mainly studies the sentencing disparities of auxiliary cybercrime in China's criminal justice practice. The fifth chapter draws the following conclusions through the statistical analysis of more than 200 cybercrime assisted judgments from 2015 to 2019: the three main factors affecting the disparity in sentencing of cybercrime in China's criminal justice practice include the gender of the offender (an extra-legal factor), the court location (an extra-legal factor) and the seriousness of the cybercrime (a legal factor).

The sixth chapter summarizes the research findings from each chapter, then synthesizes and sublimates them in light of the entire doctoral dissertation's research content, and finally concludes with some experiences and lessons learned about China's cybercrime governance.

V. Conclusions

In Chapter II - Overview of Cybercrime, this dissertation studies three aspects and draws the following conclusions.

(A) In redefining cybercrime, this article clarifies three commonly used terms: *Computer Crime*, *High-Technology Crime*, and *Cybercrime*. This dissertation discovers through a study of terminology that:

(A-a) *Computer Crime* is concerned with the objectification of cybercrime. It began during the early stages of the development of information network technology, that is, during the era of computers as the central component. However, as technology advances and people use the Internet in a variety of ways, using Computer Crime to represent cybercrime no longer accurately reflects cybercrime's current development characteristics.

(A-b) At first glance, *High-technology Crime* resembles a description of cybercrime's characteristics. However, the term "High-technology Crime" encompasses a broader range of crimes. High technology does not always imply the use of information networks. As a result,

using this term to refer to cybercrime requires further explanation and clarification. At the same time, advanced technology does not necessarily correspond to the characteristics of cybercrime in the modern era: criminals do not require sophisticated knowledge or technology to commit cybercrime.

(A-c) *Cybercrime* is defined as a crime committed in cyberspace. With the advancement of information network technology, it can be said that the distinction between physical and virtual space has always been difficult. With this in mind, cybercrime fairly accurately describes the current state of cybercrime, echoing the global theme of cyberspace governance.

(A-d) Subsequently, this article redefines cybercrime by fusing relevant criminological theories with the characteristics of cybercrime reflected in the three terms mentioned above. This paper believes that cybercrime is a harmful deviant behavior taken for procuring improper interests forbidden by law and/or common social values, by the feature of the data and online transportation thereof, which abuse the advanced technologies and/or the information asymmetries that get from positional advantages.

(B) In researching the morphology of cybercrime, this dissertation first introduces different theories of the morphological classification of cybercrime. It then discusses the major morphologies of cybercrime in contemporary Chinese criminal law, specifically Chapter VI, Section 1 of the Chinese Criminal Law. This dissertation reveals the following:

(B-a) There are two primary methods for categorizing cybercrime morphologically in official and academic circles: particularization and generalization. The method of particularization delves into specific cybercrime morphologies as defined by the Budapest Convention of the Council of Europe. The classification system used by the United States Department of Justice summarizes the various types of cybercrime morphologies in general. The majority of academic morphological classifications are based on the generalization method.

(B-b) Using computers and technology as a reference system, there are three primary morphologies of cybercrime: (1) the computer or computer network is the target of crime; (2) the computer or computer network is a tool to commit a traditional crime; (3) the computer or Internet plays as an incident in committing crimes. This classification is relatively consistent with the official United States taxonomy and reflects an attitude toward cybercrime that places a computer or technology at the center or as a target.

(B-c) Using criminal behavior as a reference point, cybercrime can be classified into four distinct morphologies: (1) Cyber-theft and deception; (2) Cyber-porn and obscenity; and (3) Cyber-violence. This classification is based on specific criminal law provisions, indicating that some scholars have shifted their focus away from technology and toward behavior.

(B-d) Using the object of the criminal violation as a reference point, cybercrime can be morphologically classified into four broad categories: (1) cybercrime against the person; (2) cybercrime against property; (3) cybercrime against morality; and (4) cybercrime against the state. This classification focuses on cybercrime's "victims," indicating a shift away from criminal behavior and toward crime outcomes.

(B-e) China's cybercrime has a morphological structure that is primarily comprised of "*one catch-all clause + eight specific cybercrimes*." The "catch-all clause" reflects the Chinese government's continued belief in cybercrime as an abuse of computer information technology. The "eight specific cybercrimes," which include safeguarding computer information systems, prohibiting the abuse of computer information technology, and defining the criminal responsibilities of accomplices, neutrals, and legal persons in cybercrime, demonstrate that China's criminal law continues to view "technology" as a necessary characteristic of cybercrime.

(C) In applying criminology theory to understand and explain cybercrime, this dissertation relies heavily on the sociological approaches in criminology. By examining strain theory and general strain theory in social structure theory, differential association theory and social learning theory in social process theory, and radical criminology and feminist criminology in social conflict theory, this dissertation establishes the following:

(C-a) Merton's Strain Theory and Agnew's General Strain Theory belong to the macroscopic theory. They focus on the combination of socio-cultural background and behavioral adaptions of social members to figure out the causes of crime. Using these two theories to understand and explain cybercrime is feasible and profound. However, due to the macroscopic nature of these two theories, it usually takes a long time for social policy adjustment to solve the problems described in these two theoretical frameworks. If these two theories are used to guide the practice of crime governance, they cannot respond to people's demand for cybercrime control in the short term.

(C-b) Differential Association Theory and Social Learning Theory are micro-level theories. They have an advantage in understanding cybercrime, especially in explaining

hacking. However, these two theories also have shortcomings, embodied as follows: first, cyberspace is different from traditional physical space. The social process theory, which is derived from the study of crime in traditional physical space, does not fully consider the uniqueness of cyberspace in the explanation of cybercrime, at least in the existing research of scholars. Second, researchers mostly take students in school as the sample in the current research on explaining cybercrime by using social process theory; the characteristics reflected by the students in school do not have general promotion.

(C-c) Radical Criminology and Feminist Criminology are reflective theories. Based on social conflicts, they reflect on the causes of a crime arising from social conflicts. In terms of understanding cybercrime, Radical Criminology focuses on whether it is reasonable to criminalize specific behaviors, while Feminist Criminology focuses on protecting the rights of minority groups in particular crimes. This dissertation argues that neither of these theories has practical significance in guiding cybercrime governance. However, it has advantages in understanding the causes of a specific cybercrime.

In the third chapter—China's legislative practice of cyberspace and cybercrime governance, this dissertation mainly introduces and analyzes the legal means system of China's governance of cyberspace and cybercrime from both domestic and international dimensions and draws the following conclusions.

(D) Before discussing and analyzing China's legal means to govern cyberspace and cybercrime, this dissertation briefly introduces the basic characteristics of China's legal system and the source of law. Although Chinese officials and scholars describe China's legal system as a socialist legal system with Chinese characteristics, this dissertation demonstrates that it retains the essential characteristics of the civil law system. The formal source of law in China mainly includes the Constitution, laws formulated by the National People's Congress and its Standing Committee, administrative regulations formulated by the State Council, and departmental rules formulated by constituent departments of the State Council. Informal sources of law in China mainly include policies, guiding cases, and ethnic customs. Judicial interpretations formulated by the Supreme People's Court and the Supreme People's Procuratorate are not a formal source of law. However, judicial interpretation plays a function similar to laws in China, so this dissertation pays attention to this point in the subsequent research and discusses and analyzes it as a part of the source of Chinese law.

(E) This dissertation mainly introduces China's policies, cyber laws, and cybercriminal law in the domestic dimension of China's legal means system to govern cyberspace and cybercrime.

(E-a) This dissertation argues that China has established a legal means system to govern cybercrime, "*Guided by the policies of the Communist Party of China + Comprehensive governance of various aspects of society + The bottom means of criminal law*." The legislative practice of cybercrime governance in China shows that: cybercrime governance cannot leave cyberspace governance. Cybercrime governance is a part of cyberspace governance. Cyberspace governance is a systematic social project. Through all-around governance in cyberspace, China regulates deviant Internet activities that do not conform to social values, protects the rights and interests of women and minors, attaches great importance to protecting intellectual property rights, and maintains national cybersecurity and Internet economic development. At the same time, cyberspace governance needs the attention of the state. Cyberspace issues involve all aspects of social development, and it is wise to set up a coordinated and unified department dedicated to cyberspace, such as the Cyberspace Administration of China.

(E-b) As far as cybercriminal law is concerned, China has continuously revised the Criminal Code through criminal law amendments to adapt to the new situation of cybercrime governance. By analyzing the provisions on cybercrime in China's Criminal Code, this dissertation argues that China's criminal law in cybercrime governance: first is to strengthen the protection of citizens' personal information constantly; the second is to improve the criminal law protection of copyright; the third is criminalizing the assisting behavior and preparation behavior of illegal activities of cybercrime; fourthly, the criminal responsibility of the Internet service providers and online platform operators is stipulated; fifth, China attaches importance to maintaining social order in cyberspace.

(E-c) The Supreme People's Court and the Supreme People's Procuratorate of China have also supplemented the application of specific provisions of the Criminal Law by constantly formulating judicial interpretations of cybercrime. However, China's judicial interpretation of cybercrime seems too rigid in legislative technology. This dissertation argues that although it is desirable to adopt "qualitative + quantitative" legislative technology to clarify specific crime circumstances, too much emphasis on a quantitative approach will stimulate potential criminals to "reasonably" avoid punishment and thus stimulate the occurrence of cybercrime.

(F) In the international dimension of China's legal means system to govern cyberspace and cybercrime, this dissertation mainly introduces China's participation and role in regional international cooperation in the governance of cyber affairs under the framework of the Shanghai Cooperation Organization.

(F-a) This dissertation argues that the governance of regional international cooperation in cyber affairs under SCO's framework mainly includes cooperation in cyberspace governance, cooperation in maintaining cybersecurity, and cooperation in combating cybercrime. China has actively participated in regional international cooperation in cyber affairs governance. However, the Shanghai Cooperation Organization with China and Russia as its core has the following problems in the cooperative governance of cyber affairs: First, the cooperation of the Shanghai Cooperation Organization is a mere formality, and much cooperation is embodied in the formulation of regional treaties and the issuance of conference declarations. Second, the SCO cooperation lacks a long-term mechanism, and only one practical exercise has been carried out in some areas of cooperation. The third is the lack of substantive cooperation clauses in the treaties formulated by the SCO to deal with cybercrime. It is more a declaration of political attitude than a legally binding international convention like the Council of Europe's Budapest convention. Accordingly, this paper argues that considering the distinct national conditions of each country, not all regional international cooperation can reach the level of cooperation of European countries. In the long run, establishing a truly feasible global standard is positive for the global governance of cybercrime.

Conviction and sentencing are two critical steps in criminal justice practice. Chapter IV focuses on the conviction practice of Cybercrime governance in China, that is, the application of criminal law. Chapter V carries out empirical research, focusing on the sentencing practice of cybercrime governance in China.

(G) Chapter IV mainly studies three aspects:

(G-a) The first is to study China's Internet Real-name system and cybercrime prevention. According to the basic theory of crime prevention, the comprehensive implementation of the Internet Real-name system in China cannot prevent cybercrime well which goes against the original intention of China to establish this system. Meanwhile, the full implementation of the Internet Real-name system can enlarge the harm of cybercrime, restrict citizens' freedom of speech, infringe citizens' privacy, and increase the operating cost of Internet enterprises.

(G-b) The second is the study of China's governance of online obscene live streaming and the explanation extension of the current criminal law. This dissertation argues that China's current criminal law system is not compatible with the new form of spreading obscenity, such as live streaming; the campaign against pornographic crime cannot leave the support of criminal law. Therefore, the explanation extension of the current criminal law system is an inevitable choice. However, China's legislation and judicial practice in related fields show that China's crackdown on online obscene live streaming violates the principle of legality in criminal law to some extent.

(G-c) Third, taking the case of DiDi in China as a sample, the dissertation studies the culpable possibilities of online platform operators in the Internet sharing economy. According to the current Criminal Law of China, this dissertation argues that DiDi has management obligations for its online hitch service platform. Furthermore, DiDi should bear criminal responsibility for crimes committed in the hitch service, especially when it fails to fulfill its management obligations faithfully and refuses to correct them after being ordered by the government. Overemphasis on the criminal liability of online platform operators is equivalent to increasing their culpable possibilities. In the short term, it limits the development of online platform operators. In the long run, however, it is conducive to driving the health of the industry.

(G-d) Chapter IV shows (or Lessons that should be learned from China's practice) that three pairs of relationships should be well handled in cybercrime governance: first, the relationship between Cybercrime Prevention and Human Rights Protection should be well balanced. Pursuing cybercrime prevention cannot be at the expense of human rights protection. The second is to deal with the relationship between the Principle of Legality in criminal law and the Explanation Extension. In criminal justice, strict adherence to the Principle of Legality in criminal law is not only a requirement of the rule of law but also a guarantee of human rights. To realize cybercrime governance, the Explanation Extension of the current criminal law must follow the Principle of Legality in criminal law. The third is to handle the relationship properly between cybercrime governance and protecting the healthy development of the Internet economy and technology. On the one hand, it can't spare the rat to save the dishes and not interfere with cybercrime caused by the emerging network techniques and economic form. On the other hand, it should keep from going beyond and lead to the development and innovation of new techniques and new economic conditions being limited because of overemphasizing cybercrime governance.

(H) Chapter V conceptualizes Article 287(I) and 287(II) of the Criminal Law of China as the Auxiliary Cybercrime and studies its sentencing disparity.

(H-a) The fundamental questions of the research in chapter V include: In the case of the existence of sentencing guidelines in China, is there any disparity in the sentencing of the Auxiliary Cybercrime in judicial practice? If there is sentencing disparity, what are the factors that cause these deviations? Among these factors, which ones are legal factors (those in sentencing guidelines and provisions of the Criminal law) and extralegal factors?

(H-b) Combined with prior research on sentencing disparity, this dissertation takes focal concern theory, chivalry perspective, and uncertainty avoidance theory as the instruction, through statistical analysis of over 200 Auxiliary Cybercrime judgments, this dissertation found that: although China's courts have sentencing guidelines, there is still sentencing disparity of the Auxiliary Cybercrime. The factors that significantly influence these disparities are the severity of cybercrime cases, the gender of the accused, and the court location. Among them, the seriousness of the crime is the legal factor, while gender and court location are extralegal factors.

(H-c) The purpose of chapter V is to reflect on and evaluate the sentencing practices of cybercrime governance in China. As mentioned above, the sentencing of cybercrime is an essential aspect of cybercrime governance. Through the empirical analysis in chapter V, this dissertation believes that the sentencing disparity of cybercrime will have a negative impact on cybercrime governance. It may stimulate the occurrence of cybercrime to some extent and then deviate from the purpose of cybercrime governance. Therefore, to fully realize the goal of cybercrime governance, we must pay attention to the justice of sentencing of cybercrime.

Cybercrime governance is a comprehensive project. Legislation, conviction, and sentencing are all indispensable vital factors therein. In the context of global governance of cybercrime, China's practice and lessons are of reference significance.

VI. New Contributions For Future Research

This doctoral dissertation focuses on issues of cybercrime in China. The following are the novel contributions of this study to the field of cybercrime and China research:

The first is the breadth of research methods. This dissertation employs both normative and empirical analysis techniques. It emphasizes qualitative legal research techniques such as literature and comparative analysis and quantitative legal research techniques such as statistical analysis.

Second, the content of the research is relatively recent. This dissertation primarily examines the experience and lessons learned in China's recent ten-year history of cybercrime governance.

Thirdly, the research structure is fairly well-developed. The research for this dissertation on China's cybercrime governance encompasses policies, laws and regulations, judicial practice, and the entire process of cybercrime criminal governance.

Fourth, the research is interdisciplinary, encompassing criminal law doctrine and other fields of criminal law science, such as criminal policy and criminology.

Fifth, the dissertation's central concept is global cybercrime governance. This dissertation examines and summarizes China's practice in light of global governance to develop a Chinese solution for global cybercrime governance.

UNIVERSITY of DEBRECEN

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

Registry number: DEENK/182/2022.PL
Subject: PhD Publication List

Candidate: Dawei Song
Doctoral School: Géza Marton Doctoral School of Legal Studies
MTMT ID: 10067720

List of publications related to the dissertation

Articles, studies (6)

1. **Song, D.**: Rethinking the Evolution of Terminologies of Defining Cybercrime Outside China. *Kexue yu jishu = Journal of Science and Technology. "Accepted by Publisher"* (-), 1-4, 2022. ISSN: 1003-9716.
2. **Song, D.**: Sentencing Disparity in China: A Descriptive Research on Auxiliary Cybercrime Stipulated by Amendment IX of Criminal Law. *Iustum aequum salutare. 17* (2), 209-239, 2021. ISSN: 1787-3223.

   Level of HAS Committee on Legal and Political Sciences: A
3. **Song, D.**: Criminal Risk for Online-Platform of Sharing Economy: From the DiDi Hitch Service Case Study in China. *Public Goods and Governance. 4* (1), 16-22, 2019. EISSN: 2498-6453.

   Level of HAS Committee on Legal and Political Sciences: D
4. **Song, D.**: Internet Real-name System and Cybercrime Prevention in China: a Critical Perspective. *Jura. 25* (2), 470-481, 2019. ISSN: 1218-0793.

   Level of HAS Committee on Legal and Political Sciences: A
5. **Song, D.**: New legislation or new interpretation on cybercrime: on the analysis of online obscene live streaming in China. *Jog, állam, politika. 11* (4), 55-75, 2019. ISSN: 2060-4580.

   Level of HAS Committee on Legal and Political Sciences: A
6. **Song, D.**: What is Cybercrime?: A Criminology Perspective. *Public Goods and Governance. 3* (2), 11-15, 2018. EISSN: 2498-6453.

   Level of HAS Committee on Legal and Political Sciences: D

Conference presentations (3)

7. **Song, D.**: Regional International Organization on Cooperation of Combating Cybercrime: Shanghai Cooperation Organization and China.
   In: Tavaszi Szél = Spring Wind 2019. Szerk.: Bihari Erika, Molnár Dániel, Szikszai-Németh Ketrin, Doktoranduszok Országos Szövetsége, Budapest, 358-363, 2020. ISBN: 9786155586606

8. **Song, D.**: A Brief Introduction: China's Legal Systems on Cyberspace Governance.
   In: Doktoranduszok fóruma : Állam- és Jogtudományi Kar szekciókiadványa. Szerk.: Szabó Miklós, Miskolci Egyetem Állam- és Jogtudományi Kar, Miskolc, 17-24, 2019. ISBN: 9789633581919

9. **Song, D.**: Internet Real-name System in China: Policy, Doctrine, and Principle.
   In: XIV. Jogász Doktoranduszok Országos Szakmai Találkozója 2018. Szerk.: Miskolczi Bodnár Péter, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest, 375-382, 2019. ISBN: 9786155961021

By the directives of HAS Committee on Legal and Political Sciences:

Publications in periodicals level „A": 3, related to the dissertation: 3.

Publications in periodicals level „D": 2, related to the dissertation: 2.

The Candidate's publication data submitted to the iDEa Tudóstér have been validated by DEENK on the basis of the Journal Citation Report (Impact Factor) database.

12 April, 2022

DEBRECENI EGYETEM * Egyetemi és Nemzeti Könyvtár *