The Legal Dilemma of Criminal Jurisdiction of Cybercrime in China and the Way to improve it

Yuxuan Li [1*]

[1] Zhejiang University of Science and Technology, Shaoxing NJ 312000, China

*100236@yzpc.edu.cn

Abstract. By studying the extensive literature review, this paper can conclude that there is a growing concern about cybercrime in the current situation in China. For this reason, China also increased the supervision of network crime and category combined with concrete practice to promote the corresponding legislative improvement. Based on the real point of view, although the constant optimization in network crime legislation in our country, as a whole, network crime our country, legislation still has a relatively low level. It also leads to work on particular. There are more problems, and the insufficiency, resulting specific legislation execution, will have more conflict or lack of pertinence. Therefore, in the legislation of network crime, this essay should pay attention to the further improvement of the existing legislation to provide support for the regulation of network behavior and the reduction of network crime. In terms of research objectives, this paper makes an in-depth analysis of the causes for the formation of cybercrime jurisdiction. This paper gives a clear explanation for the jurisdiction of cybercrime, and puts forward the principles and suggestions for dealing with cybercrime jurisdiction. Through the research, the author puts forward some views on cybercrime jurisdiction article mainly discusses the current criminal law legislation on cybercrime in China. It is primarily because the definition of territorial jurisdiction is not clear, the rules of personal jurisdiction of cybercrime protection jurisdiction are not detailed, and so on. Corresponding measures to improve the Internet legal mechanism and the bilateral extradition treaty must be token.

Keywords: Criminal jurisdiction of cybercrimes in China, The legal dilemma of the jurisdiction of cybercrimes, Principles of handling cybercrime

1 Introduction

The rapid development of the network gave birth to network crime. Considering the characteristics of web, it can effectively break through the constraints of time and space in the dissemination and distribution of information. In the process of information dissemination and diffusion, it will be challenging to explore the source of information, due to these factors, cybercrime will have more apparent complexity, concealment, and global. Because of these characteristics, this essay also gives birth to in-depth thinking on the jurisdiction of cybercrime, and also put forward a challenge to the jurisdiction

A. Holl et al. (Eds.): ICHESS 2022, ASSEHR 720, pp. 3–15, 2022.
https://doi.org/10.2991/978-2-494069-89-3_2

of cybercrime. There are also been many cybercrimes in China. The occurrence of these crimes is not only unfavorable to the maintenance of Chinese network security, but also brings negative and negative impacts on the information security of netizens. With the continuous cybercrime, the problem of cybercrime in China is that most of them are overseas cybercrime such as protecting national interests in international cybercrime. However, these cases are challenging to deal with due to incomplete laws. There are international issues behind them such as historical issues, national boundary issues, national power gap issues, and so on. The global response to cybercrime needs to be consistent and shared so that it can be tackled beyond national borders and returned to the pure land of national networks.

Because of these problems, many scholars have made in-depth discussions on the jurisdiction of cybercrime. It also provides an in-depth analysis of the principles and recommendations for dealing with cybercrime jurisdiction [1]. China also attaches significant importance to this point and has formulated corresponding laws and Regulations to combat cybercrime and promote the improvement of legislation related to cybercrime. Even so, there is no consensus on what constitutes cybercrime in China. According to the definition of cybercrime by academic scholars, there are mainly three different views. The first point of view is that the so-called network crime, refers to the application of computers and networks in violating network information security, thus causing a serious social severe impact on criminal behavior. The second view is that so-called network crime refers to the network as the carrier and object of the crime. The third point of view is that the so-called cybercrime refers to the full use of computer and network technology to cause a serious threat to society when committing criminal acts. No matter what kind of view, the consensus is that the network crime is carried out on the network, there are more socially severe harmful criminal acts.

Through these analyses, this essay can have a more precise interpretation of the jurisdiction of cybercrime. It can also provide some experience sharing and references for curbing cybercrime. In terms of viewpoint discussion, this paper mainly discusses the handling principles and suggestions of the jurisdiction of cybercrime, hoping to provide some experience sharing and reference for the academic community to study the jurisdiction of cybercrime through research.

The first part is the introduction. The second part is that the legal dilemma of the jurisdiction of cybercrimes. The first point of the second part is about the concept of territorial jurisdiction in cybercrime is not well defined. Part 2 determining a state assembly is limited in determining our jurisdiction. The third point of the second part is about difficulties in Judicial assistance under international jurisdiction. The third part is about suggestions on the principles of handling cybercrime cases with complaints. In the third part, the first point is about improving the Internet legal mechanism. The second point is about the conclusion of bilateral protection. The fourth part is the conclusion.

The rapid development of current technology has also promoted the increasing popularity of online behavior. It can be said that under the current background, the Internet plays a very crucial role in people's daily life. Whether it is information consulting or shopping, the Internet has provided greater convenience. However, the rapid growth of

the Internet can significantly facilitate people's lives and reduce the cost of communication. This essay should realize that the rapid development of the Internet brings some positive impact, In contrast, the existence of cybercrime can bring effects to the development of the Internet. Therefore, it is imperative to pay attention to preventing network crime. However, considering the characteristics of the network, it can break through the restriction of time and space in information diffusion, on this basis, the proliferation and dissemination of global information are achieved. In this case, it will lead to some difficulties in defining the jurisdiction of cybercrime. Therefore, in dealing with cybercrime, how to determine the jurisdiction of cybercrime is a problem the essay must face and must solve. Only by fully addressing this problem can this essay achieve greater success in combating cybercrime and maintaining cybersecurity.

2 The legal dilemma of the jurisdiction of cybercrimes

The conventional meaning of criminal space refers to the place where the offender commits the crime. This is an actual physical space with three-dimension space. Thus, one jurisdiction of traditional criminal law over crime is based on the real of physical space. Adhering to the jurisdictional viewpoint of "territorial jurisdiction doctrine is the main and personal principles. the principle of protection and universal Jurisdiction as a complementary principle." However, territorial jurisdiction of cyberspace does not belong to the traditional criminal law theory of the "four spaces." The globalization of cyberspace and virtualization broke the boundary of sovereign territory. In cyberspace offenders cross some countries simultaneously, protection principle is complementary to traditional criminal jurisdiction is challenging to adapt. In practice, the dilemma of determining the criminal jurisdiction of cybercrime lies in the following aspects.

2.1 The concept of territorial jurisdiction in cybercrime is not well defined.

It is difficult to use crime scenes or crime locations as a basis for territorial jurisdiction for cybercrime. [2] The jurisdiction of law is based on relatively stable relationship. One theory holds that traditional territorial jurisdiction is based on the requirement that one of the places where the crime occurred or the result should be that in a given jurisdiction. That is to say. It has a stable connection to real physical space. The Internet is a global, open system. There is no necessary connection between online addresses and geographical locations in reality. For behavior in cyberspace, it is generally challenging to determine their proper geographic location, and the judgment of the act and result of cybercrime as containing arbitrariness and contingency. On the one hand, the global nature and uncertainty of cyberspace make it impossible for a network behavior to point to a specific jurisdictional factor, thus making the relationship between network behavior and traditional jurisdictional basis uncertain. On the other side, as a global whole, the characteristics of cyberspace encompass the virtual and the intangible, and it is impossible to divide the various jurisdictions as in the case of physical space.

To sum up, territorial jurisdiction is complex due to fuzzy network connection points. The network service provider cannot perform the work need for the network service supervision, program processing, etc., and bear the legal responsibilities.

Territorial jurisdiction is unclear jurisdiction due to fuzzy network connection points. In the definition of criminal jurisdiction of network crime, there are still many problems, which are reflected in. Territorial jurisdiction is the core of the principle of criminal jurisdiction. Article 24 of the code of Criminal Procedure states that "Criminal cases are under the jurisdiction of the people's court where the crime was committed. It is more appropriate if the trial is conducted by the people's court in the place where the criminal suspect resides. The trial can be in the people's court of the place where the criminal suspect lives." In cyberspace, physical connections become unstable. It is debatable whether to apply territorial jurisdiction completely. For example, in the case of violation of citizens' information committed by many people, the criminal suspects only communicate with each other through WeChat and QQ. The criminal acts of the criminal suspects take place all over the country. The residence of the criminal suspects is distributed all over the country, and the arrival time of the case is different. Territorial jurisdiction is jurisdiction that arises because of a vague network of connecting points. Two things require careful consideration including whether the law should be addressed separately and where it should govern. If fully integrated, where does jurisdiction make the most sense? If treated separately, would judicial resources be wasted?

To sum up, territorial jurisdiction is difficult due to fuzzy network connection points. The network service provider cannot perform the work needed for the network service supervision, program processing, etc., and bear the legal responsibilities [3].

Although the rapid development of technology poses a full range of challenges to the traditional jurisdiction rules, this paper should not blindly assume that the general jurisdictional rules are now extremely backward or lack current value. The correct behavior is to maintain the inherent stability of criminal law theory, give full play to the relevant flexibility and relevant adaptability of the existing judicial system, respond to the jurisdictional problems of cybercrime by the traditional knowledge of jurisdictional theory and make adjustments as technology advances. Only this approach can fill and reduce the gaps and conflicts of criminal jurisdiction in cyberspace to the maximum extent.

Its jurisdiction should be judged based on the location of the network server or computer terminal where the infringing content exists. [4] For cases of intellectual property crimes related to use computer networks to infringe copyright, damage the commercial reputation and merchandise reputation of others. The site where the network server or computer terminal equipment where the infringing content acts are located is considered to be the home where the criminal act occurs. However, there is no unique judicial interpretation of the determination of the place of crime in cybercrime cases. Article 1 of *The Interpretation on Several Issues Concerning the Application of Law in the Trial of Disputes over Computer and Network Copyright issued by the Supreme People's Court* on December 19, 2000 stipulates the jurisdictional issues. Article 1 is about copyright disputes shall be under the jurisdiction of the people's court in where the infringement is committed or where the defendant has his domicile. The site of infringement includes the area where the network server, computer terminal and other equipment are

located. Where it is challenging to determine the place of the infringing act or the domicile of the defendant, the location of the computer terminal equipment where the infringing content is discovered by the plaintiff may be regarded as the place of the infringing act. To some extent, this explanation solves the problem that tort is difficult to determine.

Jurisdiction shall be determined based on the location of the victim's system or personal system, network server and computer terminal equipment, in the case where the perpetrator commits a cybercrime by the act of intruding or modifying the system program or system parameters of the victimized related units or individuals. The location of the infringed relevant computer network system or equipment terminal can be considered where the cybercrime act takes place. For the use of computer information system and remote login and other means to invade others illegally obtaining commercial secrets, or modify the information system of the financial unit, network crimes such as stealing property, due to the infringement of computer network system. The location of the terminal equipment is one of the main spaces of behavior person committing crimes. Therefore, these sites can be seen as a crime.

Jurisdiction is judged by the purpose of the perpetrator and the location of the profit. For the criminal cases of theft, embezzlement, misappropriation of public funds, duty encroachment, misappropriation of funds, fraud and other crimes carried out by the use of computer network, the venue where the criminal actor operates the computer. The destination judged by the cyber act and the place where he profited can be considered the result of the crime. Although the rapid development of science and technology has brought all-around challenges to the traditional jurisdiction-related rules, this article should not blindly think that the conventional jurisdictional rules are too backward and lack the value of "The Times," The correct choice should be to maintain the corresponding internal stability of the criminal law theory and give full play to the flexibility and flexibility of the existing judicial system, calmly think about the jurisdiction of cybercrime according to the traditional jurisdiction theory, and make adjustments along with the progress of technology. Only in this way can the gaps of criminal jurisdiction and conflicts in cyberspace be filled and reduced to the maximum extent.

2.2 Traditional jurisdiction is limited in determining jurisdiction

According to the regulations of criminal law in China, an essential premise of exercising personal rights and protection rights is to distinguish whether crime occurs in the criminal realm or outside the criminal field. In cybercrime, however, has no definite boundaries and fixed scope. [5] It is a borderless, global and open system, and it is difficult to distinguish whether a cybercrime takes place in our field or outside it. Since it is difficult in determining whether Chinese citizens or foreigners are engaged in cybercrime outside or within the domain of China, the provisions of the criminal law on personal jurisdiction and protective jurisdiction are meaningless to determine the jurisdiction of cybercrime. In other words, the traditional focus of personal jurisdiction and the principle of protection jurisdiction can’t address the question of international jurisdiction of cybercrime.

Because cybercrime is a borderless crime, the negative impact it causes may be global, and its wide range of influence and the number of countries involved are not comparable to traditional crimes. To apply the principle of universal jurisdiction to cybercrime, states must meet the following conditions. Firstly, cybercrime constitutes a criminal act not only in the country, but also in other countries constitute criminal acts, which can be considered, have constituted "crimes under the common control of the state." Secondly, it should be based on international treaties in which both parties have participated or concluded. According to the current national legislation and global practice, no international accord on the jurisdiction of cybercrime has been reached. Therefore, the application of the principle of universal jurisdiction in cybercrime lacks legal basis and practical basis.

In addition, the current social background of cybercrime is very complex. From the perspective of China, the problem of cybercrime in China is that most of them are overseas cybercrime, such as the protection of national interests in international cybercrime. However, due to the imperfection of the law, these cases are difficult to be handled. Behind this, there are international issues, not only China's reasons, but also international issues, specifically, such as historical issues, the borders of countries, the gap in national strength and so on. However, the global approach to solving cybercrime should be consistent and a typical attitude should be maintained, to solve cybercrime outside the borders of each country and return a pure land of national networks. Due to the rapid development of web, there have been many cybercrime behaviors in our country. The occurrence of these criminal acts is not conducive to the maintenance of Chinese network security, but also brings adverse and adverse effects to the information security of netizens. Along with the increase in network crime, China has also paid full attention to this, and the corresponding laws and regulations have been formulated against the network crime, promoting the improvement of the appropriate legislation on network crime. Even so, there is no consensus on the definition of cybercrime in China [6].

There is a trend towards pan-administration of international jurisdiction. Due to various overlaps between the target of jurisdiction and the specific connection points. The imbalance of power and responsibility in "territorial management" can easily lead to the cycle of the responsibility avoidance strategy of the special unit and the reverse responsibility avoidance strategy of the subordinate unit. The continuous iteration of the responsibility avoidance strategy will hinder the effective promotion of decision-making, affect the implementation of policies, and weaken the implementation of policies. When the superior unit feels that its "power" is more tremendous than its "responsibility", it will often adopt a top-down strategy to avoid responsibility under the name of "keeping the soil and having responsibilities," It takes advantage of its "position advantage" in the network of management subjects to transfer the tasks and responsibilities that should be borne by itself to the subordinate unit. However, in reality, lower-level units may not always follow the logic of vertical management, earnestly implement the instructions of higher-level units with high quality, and even may adopt the "reverse avoidance of responsibility" strategy. That is, in view of the fact that the responsibility is more significant than the power, and the lack of authority and resources needed to take responsibility and get things done. To eliminate the risk of accountability, the lower-level units often transfer the 0064ecision-making power to the higher-

level units requests for instructions and reports. At the same time, the responsibility and risk will be transferred together, because this has a great impact on the court, which is related to the source of cases in the later period and the social influence generated, as well as the court's own interests [7].

Lanzhou, Gansu Province "February 12" network "routine loan" crime case. In March 2019, the public security organ of Lanzhou, Gansu province broke up Wang Matao's network "routine loan" gang-related, destroyed six criminal dens, captured 269 suspects, solved 309 criminal cases, and seized and froze 1.5 billion yuan of assets involved. The case seriously disrupted the order of Internet and financial management, disrupted the order of economic and social life, and caused significant impact and severe harm. [8] After investigation, since 2018, Wang Matao et al. have successively registered more than 20 shell companies, developed 24 online loan platforms such as "Sweet Rabbit," and recruited professionals to engage in online loan business through "routine loan" and in the form of "corporate operation" management, defraud victims of borrowing and charging ultrahigh interest. Through multiple platforms "borrowing new to pay off the old" way "to mortgage" malicious extortion "debt" to cheat others, the establishment of outsourcing companies with 24 collectors of collection insults, threatening phone calls. Some companies send PS naked strips and other "soft violence" means of illegal collection, illegal profits of more than 2.8 billion yuan, illegal arrears but have not yet received about 9.8 billion yuan, more than 475,000 people were victimized. On September 28, 2020, the Lanzhou Intermediate People's Court issued a verdict on the case, and Wang was sentenced to life imprisonment for the crimes of organizing and leading a mafia-style organization, fraud and picking quarrels and provoking trouble.

The judgment and review of the case by Lanzhou Intermediate People's Court is of significant significance to society and has exerted great social influence, which has excellent reference significance for the later processing of network crimes. The crack of this case to Lanzhou Intermediate People's Court added authority [9]. On the contrary, for some cases involving small amounts of money, the court's territorial jurisdiction has crossover and complexity. The court's handling of such cases is more complicated, so the enthusiasm is not high.

In the definition of criminal jurisdiction of network crime, there are still many problems, which are reflected in. Territorial jurisdiction is the core of the principle of criminal jurisdiction. Article 24 of the Criminal Procedure Law states, "Criminal cases shall be under the jurisdiction of the people's court in where the crime was committed. If it is more appropriate for the trial to be conducted by the people's court where the criminal suspect lives, the trial may be conducted by the people's court in the place where the criminal suspect lives." In cyberspace, physical connections have become unstable. It is debatable whether to apply territorial jurisdiction thoroughly. For example, in the case of violation of citizens' information committed by many people, the criminal suspects only communicate with each other through WeChat and QQ. The criminal acts of the criminal suspects take place all over the country, and the residence of the criminal suspects is distributed all over the country, and the arrival time of the case is different. Whether it should be handled separately, and where it should be governed, requires

careful consideration. Where would be the most proper jurisdiction if it were thoroughly integrated? Will judicial resources be wasted if the case is handled separately?

To sum up, territorial jurisdiction is complex due to fuzzy network connection points. The network service provider cannot perform the work needed for the network service supervision, program processing, etc., and bear the relevant legal responsibilities [10].

Although the rapid development of technology poses a full range of challenges to the suitable jurisdiction rules, this paper should not blindly believe that the traditional jurisdictional rules are too backward and lack the value of the times. The right choice is to maintain the relevant inherent stability of criminal law theory and give full play to the relevant flexibility and relevant adaptability of the existing judicial system. It calmly thinks about the jurisdiction of cybercrime according to traditional jurisdiction theory, and makes adjustments along with the progress of technology. Only in this way can the gaps of criminal jurisdiction and conflicts in cyberspace be filled and reduced to the maximum extent.

The jurisdiction shall be determined according to the location of the network server or computer terminal where the infringing content is found. [11] In the case of intellectual property crime such as infringement of copyright and damage to others' business reputation and commodity reputation by using computer networks. The location of the relevant web server or computer terminal equipment with infringing content may be considered the location of the offense. However, there is no specific judicial interpretation of the determination of the place of crime in the relevant cybercrime cases. Article 1 of *the Interpretation on Several Issues Concerning the Application of Law in the Trial of Disputes over Computer and Network Copyright issued by the Supreme People's Court* on December 19, 2000 stipulates. The issue of jurisdiction means that copyright disputes should be under the jurisdiction of the people's court where the infringing act or the defendant's domicile is located. The area of infringement includes the location of network servers, computer terminals and other equipment. Where it is complex to DETERMINE the site of the infringing act or the domicile of the defendant, the location of the computer terminal equipment where the infringing content is discovered by the plaintiff may be regarded as the place of the infringing act. To some extent, this interpretation addresses the difficulty of identifying infringement.

Jurisdiction shall be determined based on the location of the victim's systems or personal systems, network server and computer terminal equipment, in the case of the perpetrator committing cybercrime using intruding or modifying the system program and system parameters of the victim unit or individual. The location of the infringed computer network system or equipment terminal can be recognized as the place where the criminal act of the relevant cybercrime took place. For computer information system and remote login and other means to invade others illegally obtaining commercial secrets, or modify the information system of the financial unit, network crimes such as stealing property, due to the infringement of computer network system. The place of the terminal equipment is one of the main spaces of behavior person committing crimes. Therefore, these sites can be seen as a crime.

Jurisdiction is determined by the final purpose of the perpetrator and the relevant place of profit. For the criminal cases of theft, embezzlement, misappropriation of public funds, duty encroachment, misappropriation of funds, fraud and other crimes carried out by the use of computer networks. The location where the perpetrator operates the computer, the final destination to which the network behavior is directed. The location where he acquires the property can all be considered the result of the crime. Although the rapid development of technology poses a full range of challenges to the traditional jurisdiction rules, this essay should not blindly believe that the traditional jurisdiction rules are too backward and lack the value of The Times. The right choice is to maintain the relevant inherent stability of criminal law theory and give full play to the relevant flexibility and multilateralism of the existing judicial system, calmly think about the jurisdiction of cybercrime according to the traditional jurisdiction theory, and make adjustments along with the progress of technology. Only in this way can the gaps of criminal jurisdiction and conflicts in cyberspace be filled and reduced to the maximum extent.

2.3 Difficulties exist in judicial assistance under international jurisdiction

With the increasing globalization of the economy, the increase of transnational crimes and the expansion of the scope of interaction between States, the current agreements of criminal judicial assistance with foreign countries are far from being able to solve the existing contradictions. Currently, the contradiction or inconsistency of Chinese international criminal judicial service is the contradiction or inconsistency between Chinese criminal legal norms and foreign criminal legal norms or provisions of relevant international conventions.

According to the criminal judicial assistance agreement signed between China and foreign countries. This agreement generally has three aspects. The First point is the communication and service of judicial and foreign judicial documents. The second one is the investigation and collection of evidence. The third point is the exchange of legal information. That is to say. The contracting parties provide each other with information about national laws and judicial practices through the central authority, as well as exchange of legal publications. [12] However, in today's increasingly globalized economy, increased transnational crime, and expanded interstate contacts, the current foreign criminal MLA agreements are far from being able to resolve the existing conflicts.

The perpetrator or his criminal acts were not committed within the territory of a particular country, but only across the border of another country using signal conversion or data transmission over the Internet. In this case, whether the condition has jurisdiction or not is the focus of discussion and concern in legal circles. The impact on the traditional theory of criminal jurisdiction is inconceivable if the state being crossed has jurisdiction. If jurisdiction is not considered, the judicial sovereignty of the transited state must be challenged. The same kind of "abstract crossing" can happen at home. This "environment" refers to the jurisdiction of each jurisdiction. If criminals commit cybercrime in Zhejiang province, the signal crosses Shanghai and is finally transmitted to Beijing, where the police in Shanghai first get hold of the criminal facts. Is Shanghai

the place where the crime was committed and did the public security organ in Shanghai have the right of jurisdiction? This is worth discussing. From the perspective of protection jurisdiction, if purely based on the theoretical perspective, it was evident that both traditional crime and network crime should have corresponding jurisdiction subjects. However, it is essential to note that not all subjects are willing to govern. In specific judicial practice, whether it is traditional crime or cybercrime, most countries generally give jurisdiction claims for crimes that cause serious harm to the interests of their citizens and have relatively bad social influence in terms of the protection of jurisdiction. In some transnational crimes, extradition to the host country or international judicial assistance is also sought.

For example, specifically, punishing corrupt officials fleeing international criminal judicial assistance settlement mechanism. On May 6, 2009, a district court in Las Vegas to fraud, money laundering, international operations to steal money, forged passports and visas. The former president of the Bank of China Guangdong Kaiping Branch and Xu Guojun were sentenced to 25 and 22 years in prison, respectively, and husband and wife Yu Ying and Jardine Wanfang were sentenced to eight years each for having a relationship. In addition, the judge also ordered the four defendants to face three years of supervision after being released from prison and ordered them to return $482 million in stolen money (" Erxu "case). This is the first time that corrupt Chinese officials on the run have been sentenced abroad, which marks the stage of victory of international criminal judicial assistance against corrupt officials in many years. However, in the face of the fugitive corrupt official extradition, persuasion, repatriation, recovery of stolen money and other problems, it is still tricky.

3 Suggestions on the principles of handling cybercrime cases with jurisdiction

Although the rapid development of technology has posed an all-around challenge to the traditional jurisdictional rules, this paper should not blindly believe that the traditional jurisdictional rules are too backward and lack contemporary values. The right choice is to maintain the inherent stability of criminal law theory, give full play to the relevant flexibility and adaptability of the existing judicial system, reason about the jurisdictional issues related to cybercrime according to the conventional jurisdictional theory, and make effective adjustments with the progress of technology. Only in this way can the gaps of criminal jurisdiction and conflicts in cyberspace be filled and reduced to the maximum extent.

3.1 Improve the Internet legal mechanism

At present, there are indeed problems in cyberspace governance. There are multiple network terminals, and the epidemic has reduced the frequency of offline transactions and aggravated the frequency of online transactions.

Establish the Internet court, the Internet court is the original concept of China. Is the era of the significance of the information background in the history of world justice. Is

the latest component of human legal civilization. [13] It has opened up a new frontier of justice. With a series of significant innovations in the judicial system, judicial principles, litigation procedures, and adjudication rules adapted to the characteristics of the Internet era, and cannot simply assert the rights and wrongs by traditional judicial theories such as having the aspects of industrial civilization. It is necessary to distinguish the "dual-track litigation" model from the "single-track litigation" model and adhere to the concept of "adjustment theory", so that the "dual-track litigation" model of the Internet Court meets the inherent substantive requirements of the direct trial principle, the principle of personal experience, the principle of verbal debate and the law of trial of Internet disputes. It is recommended to systematically promote the "three-step" development strategy of the Internet Court and further improve the system design: summarize the reform experience and grasp its basic laws; this paper authorizes the pilot program by the law to ensure that the reform is based on the law. This essay will improve institutions and systems, achieve high-quality development of Internet courts, and contribute China's wisdom and proposals for future judicial models to the world. However, at present, many rules are not perfect. China has set up Internet courts in Beijing, Hangzhou and Guangzhou, but there are many problems in the implementation and many legal loopholes. Because cybercrime is a new thing on the Internet, especially in the context of the epidemic, China may need to learn from foreign methods to deal with new things. Specifically, extraterritorial jurisdiction of the United States includes extraterritorial legislative jurisdiction, judicial jurisdiction and law enforcement jurisdiction, which is different from long-arm jurisdiction and extraterritorial application of American law. The United States believes its extraterritorial jurisdiction stems from the territorial, personal, protective and universal principles of international law. The US Congress enacts legislation with extraterritorial application clauses not only to ensure equal treatment of parties inside and outside the US, but also to safeguard the political, economic and diplomatic interests of the US. Although the US federal courts have restricted the use of US law by unfamiliar plaintiffs to seek compensation in extra-territorial tort cases, they have not limited the enforcement power of the US executive branch and the right of action of private parties in the US. The U.S. executive branch has even violated international and foreign law to enforce the law in foreign areas. In response to the extraterritorial jurisdiction of the United States, Canada, the United Kingdom and other countries as well as the European Union have adopted a series of political, legal and economic countermeasures that can be used for reference. In response to the extraterritorial jurisdiction of the United States, China should: cooperate with other countries to oppose the excessive extraterritorial jurisdiction of the United States. To assist Chinese enterprises and individuals in responding to individual cases, China will improve the law on foreign relations especially legislation on jurisdiction, international judicial assistance, and obstruction [14].

3.2 Conclusion of bilateral extradition treaties

There are various expressions of the concept of international criminal judicial assistance, among which the most representative ones are as follows. International mutual legal assistance in criminal matters refers to the sum of joint facilities, assistance and

cooperation provided by judicial organs of different countries for the purpose of performing criminal justice functions. International judicial assistance in criminal matters is an activity in which states offer mutual support, convenience, and assistance in criminal cases by acting on behalf of certain judicial acts.

International mutual legal assistance in criminal matters refers to the adequate sanctioning of international criminal acts by countries or regions worldwide. According to the provisions of relevant international treaties or the principle of bilateral reciprocity, directly or under the coordination of international organizations, a kind of judicial system to perform certain procedural matters on their behalf. In summary, international criminal judicial assistance refers to the countries or regions of the world for the effective sanction of international criminal acts. According to the provisions of relevant international treaties or the principle of bilateral reciprocity, directly or under the coordination of international organizations, a kind of judicial system to perform certain criminal procedural matters on their behalf. At present, the forms of international criminal judicial assistance mainly include extradition, international criminal investigation assistance, transfer of international criminal proceedings to jurisdiction, international assistance in the execution of criminal judgments, and other transnational criminal judicial service.

4 Conclusion

In short, along with the progress of The Times and the development, our country has made a better breakthrough in network technology. The technical level is constantly upgrading. Netizens can also have a more relaxed network of leisure and entertainment spaces. However, while seeing the advantages brought by the development of the Internet, this essay should also see that the popularity of the Internet has also led to the rise of cybercrime. Many countries are very concerned about cybercrime and have enacted legislation to combat it. Through the continuous improvement of legislation, institutional guarantees and constraints should be provided for the supervision of cybercrime.

For China, under the background of the continuous development of network technology, behavior of cybercrime is also more and more rampant in China. Therefore, in this case, it is crucial and necessary to pay attention to the jurisdiction of cybercrime, including reshaping cross-border cybercrime, establishing a new concept of judicial management, and seeking a unified mechanism of jurisdiction.

Through this point of view, this essay can expand the regional jurisdiction of cybercrime and fully highlight the fairness and justice of the law. However, in concrete implementation, there will still be a certain degree of implementation difficulty. In addition, considering since cybercrime itself can involve more jurisdictional issues, in this case, jurisdictional conflicts will also arise. However, many countries have also introduced the concept of expanding territorial jurisdiction in defining the principles of cybercrime jurisdiction. Through the introduction of this point of view, this essay can provide some experience sharing the purpose of regional jurisdiction of cybercrime.

References

1. Sun Shengda. Research on Criminal Jurisdiction of Transnational cybercrime Shenyang University of Technology, 2021.
2. Lyu H S. Investigation Dilemma of network Fraud Cases and countermeasures Research. Northwest University of Political Science and Law, 2021.
3. Li Simeng. Research on Investigation Jurisdiction of Telecom Fraud Crime Zhengzhou University, 2021.
4. Xu Xueyan. Research on the Jurisdiction of cybercrime Cases Shandong University of Finance and Economics, 2021.
5. Lu Ping. Analysis on Criminal Jurisdiction of cybercrime. Law and Society (10): 2122 (2021).
6. Zhang Chen. Thinking on Criminal Jurisdiction of cybercrime. Taiyuan University of Science and Technology,2021.
7. Qu Xualing. On the determination of criminal places in regional jurisdiction Southwest University of Political Science and Law,2020.
8. Jiao Yuanbo. Research on International Law Governing cybercrime Xiangtan University, 2020.
9. Xu Yali. Research on International Criminal Judicial Assistance in Transnational cybercrime Nanchang University, 2020.
10. Xu Xiuzhong. Network and Network Crime. Citic Press (2003).
11. Yu Zhigang. Criminal Thinking of quasispace. China Founder Publishing House (2003).
12. Huang Zelin. Application of Criminal Law to cybercrime. Chongqing Press (2005).
13. PI Yong. Comparative Study on cybercrime. China People's Public Security University Press (2005).
14. Li Xiaoming and Li Wenji. Journal of Soochow University (2018).