8th International Congress of Information and Communication Technology (ICICT-2018)

Research on Criminal Jurisdiction of Computer cybercrime

**Abstract**

This article mainly discusses the jurisdiction of computer cybercrime. This article introduces the new theory of cybercrime jurisdiction and puts forward the system of establishing cybercrime jurisdiction: the principle of "priority of power", the principle of "territorial superior rights", criminal jurisdiction dispute negotiation system and drawing on the civil jurisdiction of computer cybercrime system.

# Introduction

With the rapid development of Internet technology, the use of the Internet has penetrated into all fields of social life. The number of Internet users and the time spent on the Internet have been continuously increasing. According to the 40th "Statistical Report on Internet Development in China" (hereinafter referred to as the "Report") released by China Internet Network Information Center (CNNIC) on August 4, 2017. As of June 2017, the number of netizens in China reached 751 million with an Internet penetration rate of 54.3%. At the same time, with the development of the Internet, especially the rise of mobile phone networks in recent years, computer cybercrime has been constantly spreading. Crimes against cyber-systems, internet defamation crime,internet illegal business crime, internet extortion crimes and computer cyber-gambling continue to emerge, posing a serious threat to personal property, information and security, disrupting the overall social order. According to the U.S. think tank Strategic and International Studies Center, computer cybercrime is estimated to cost the world 445 billion U.S. dollars a year,

including over 45 billion U.S. dollars in economic losses in china. Therefore, it is a problem that the world needs to deal with to eliminate the computer cyber environment, crack down on computer cybercrime, safeguard citizens' legitimate rights and interests, and safeguard the order of the Internet. Among them, the jurisdiction of computer cybercrime is issues that need to be solved first.

# Overview of criminal jurisdiction

The jurisdiction of computer cybercrime includes two kinds of situations: First, which country is responsible for the crime. Second, which court in the country is under the jurisdiction of the crime? The former is the jurisdiction of criminal substantive law, that is, the issue of the space effectiveness of criminal law, which is a kind of static criminal jurisdiction. The latter is the jurisdiction of the trial in criminal proceedings, is a dynamic criminal jurisdiction.

Computer cybercrime occurring in China mainly involves the issue of geographic jurisdiction in criminal proceedings, which is generally governed by the criminal court, If the jurisdiction of the people's court where the defendant is domiciled is more appropriate, it may be under the jurisdiction of the people's court where the defendant resides. Transnational computer cybercrime jurisdiction is the issue of criminal jurisdiction in substantive law, mainly related to the conflicts of international jurisdiction. Due to its own virtual and transnational characteristics, computer cybercrime has an impact on the basic principle of the traditional space effect of criminal law. The basic principle of the space effectiveness of Chinese criminal law is based on the principle of territorial jurisdiction and adopts the principle of personal jurisdiction, protection of jurisdiction and universal jurisdiction. This principle can effectively protect the legitimate rights and interests of our country and citizens, but, how to apply the jurisdiction of transnational computer cybercrime needs further study.

In general, the criminal jurisdiction of computer cybercrime should be applied in accordance with the relevant provisions on the space effectiveness of the general principles of criminal law. Article 6 of the Chinese Criminal Law stipulates that, "Any person who commits a crime in the territory of the People's Republic of China shall apply this law unless otherwise specifically provided by law." Chinese criminal law has jurisdiction as long as one of the criminal acts or criminal consequences occurs in China, including ships, aircraft and other aircraft outside the territory as well as Chinese embassies and consulates abroad. Article 7, 8 and 9 of Chinese Criminal Law respectively stipulate personal jurisdiction, protection of jurisdiction and universal jurisdiction. According to personal jurisdiction, China has criminal jurisdiction of computer cybercrime committed by Chinese citizens outside China'sterritory. According to the principle of protection, China has criminal jurisdiction over foreigners in the field of computer cybercrime committed against Chinese countries or citizens outside China. In addition, for the international treaties that China participates in, if the treaty provides for computer cybercrime, China can apply Chinese criminal law within the scope of its treaty obligations and exercise its criminal jurisdiction.

# New issues of criminal jurisdiction of computer cybercrime

Traditional criminal crimes do not have the characteristics of virtuality and unlimited expansibility. Even transnational crimes, since the crimes themselves are non-covert, the targets of the crimes are tangible and the objects constituted by the real three-dimensional space , Each country may determine the criminal jurisdiction of the crime according to its own criminal law or the provisions of the relevant international (or bilateral) treaty. The criminal jurisdiction of computer cybercrime is different from the traditional crime. The typical one is "abstract cross-border" behavior. Since the criminal act involves many countries, it is difficult for this illegal computer cybercrime to point to a certain area of criminal jurisdiction. For example, several former Federal German students invaded the U.S. Department of Defense over the Internet for the purpose of stealing military secrets for the KGB, the students first log in to servers in Japan through the former Federal Republic of Germany network while using Japan's network data and signaling system to transfer to a university in the United States and finally invade the U.S. Department of Defense's computer through this U.S. university network system and steal important U.S. military secrets. In this case, several students' criminal behaviors spanned the Federal Republic of Germany, Japan and the United States in three countries. Whether all countries should have criminal jurisdiction over this case and whether

Japan has jurisdiction as a trans boundary state became the hot topics discussed by criminal law scholars. The issue of "abstract cross-border" has formed a great challenge to the traditional theory of criminal jurisdiction.

The nature of the network itself changes some of the content and form of traditional crime, and perpetrators can commit crimes through virtual spaces that span several or dozens of countries without close contact with specific or non-specific subjects and its result is far greater than natural crime. However, computer cybercrime requires terminal devices such as computers or mobile phones to implement crime through a web server, to access web pages of a target country, and also to output and input relevant data instructions, these new behaviors have greatly impacted the traditional criminal jurisdiction, and the two are hard to come into agreement. For example, it is a legal act for Jackie to establish a pornographic website in country A and a criminal act in country B, C and D, so the perpetrator set up a pornographic website in country A through the web server of country C , A country court does not exercise its jurisdiction. However, many citizens of country B visited the site. The citizens of the country, Mike, interacted with Jack's website and continuously uploaded pictures or videos. In this case, Court A does not exercise criminal jurisdiction; State B considers that the commission of a crime in connection with its own computer is criminalized in its own country and therefore claims jurisdiction in the case. Because perpetrator Jack is an pornographic website registered on the server of country C and the criminal act of establishing pornographic websites in country C, country C considers himself having criminal jurisdiction. The court of State D believed that the act of its own citizens, Mike, was an active and purposeful visit. It violated its criminal law provisions on the dissemination of obscene articles and violated its own good customs. Therefore, the court of State D should have full jurisdiction over the case. Based on the above new issues concerning the jurisdiction of computer cybercrime, all countries will inevitably compete for the criminal jurisdiction, resulting in conflicts of jurisdiction, detrimental to the trial of the facts of the case and the protection of the legitimate rights and interests of the victims.

# New Theories of Cybercrime Jurisdiction and Analysis

Therefore, how to solve the conflict between new computer cybercrime and traditional criminal jurisdiction has become a hot topic in the field of criminal law. Conservative scholars believe that we should still uphold the traditional criminal jurisdiction and should not change this tradition because of the appearance of special phenomena. Open scholars have proposed some new theories of jurisdiction. Mainly include:

* 1. *Theory of new sovereignty*

The theory of new sovereignty can be called the theory of network autonomy, or called "radical independent jurisdiction theory" and "the sovereignty of the virtual world is independent." The doctrine holds that computer cyberspace is creating a global civil society that has its own form of organization, values, and rules that are completely independent of the government and have the right to self-government[1].According to this theory, since the network itself has the characteristics of being different from those of other objects, the current legal norms should no longer be applied to the issue of jurisdiction over computer cybercrime. A separate system of laws applicable to computer cyberspace should be developed separately so that the jurisdiction of computer cybercrime is independent from the traditional criminal jurisdiction.

* 1. *Theory of jurisdictional relativity*

In order to solve the problem of criminal jurisdiction of computer cybercrime, Professor Darrel Menthe of Stanford University in the United States put forward another theory - the theory of jurisdictional relativity. The theory has become the "fourth international space theory" after Antarctica, outer space and the high seas. The theory holds that computer cyberspace should exist as a new jurisdiction, as in the high seas, Antarctica and outer space, establishing new rules of jurisdiction that are different from the traditional ones[2].If a citizen illegally enters the computer cyberspace and commits a crime in space, any country may exercise jurisdiction over the perpetrator according to the laws of its own country. At the same time, they also believe that the parties do not need to go to a court to respond, they only need to "go to court" in a court through computer cyberspace, and the court can execute the verdict they have made online. This theory is obviously the principle of nationality needed to establish

jurisdiction in the analogous application of the high seas, however, it is difficult for the virtual characteristics of the Internet to determine where a person's nationality is. Moreover, based solely on nationality as the basis for legislative jurisdiction, it is bound to make radical changes to the current principle of territorial jurisdiction, which is unacceptable to all countries [3].

* 1. *Theory of website jurisdiction*

As with other factors, the website must have two conditions if it is to be the basis for exercising jurisdiction: First, the website must be spatially and temporally stable, at least to be certain; second, there is a certain relationship between the website and jurisdiction[4] . There is a very close relationship between the web site and its owner. After the web site is registered with the server, as if the personal residence is located in a certain geographical area, it is consistent, and the perpetrator can accept and send messages on his own website, obviously in line with the first requirement. However, if the site's activites are confined to the field of the country and the site itself does not have the function of uploading and downloading information, then only its own country has criminal jurisdiction over the wrongdoing. If the owner of a web site takes the initiative to open a web site and send data messages to citizens of other countries outside of the country, or other citizens of the country take the initiative to download or upload the information, it can cause damages to many countries, Then the visit of citizens from other countries makes the site and the jurisdiction closely integrated. Therefore, the second condition is met that the website owner may also be subject to the jurisdiction of many countries that he has never visited before, which eventually leads to the conflict of jurisdiction. Therefore, it is clear that there are still many questions about determining the web site as a factor of criminal jurisdiction, which is not conducive to resolving conflicts of jurisdiction in various countries.

* 1. *The principle of limited jurisdiction*

The principle of limited jurisdiction refers to the determination of whether criminal jurisdiction exists beyond the personal jurisdiction on the basis of the relevance of the offense to the violation of or influence on the country and citizen of the country; If there is an association, then it has criminal jurisdiction; if there is no association, it will not have criminal jurisdiction[5].This theory is based on the principle of belonging to make a supplementary explanation, this supplement is no different from the protection of jurisdiction, but there are differences with the protection of jurisdiction. The theory of limited jurisdiction does not necessarily mean harming the country and citizen of the country. As long as its own nationals are somewhat affected by their behavior, the court of that country should have jurisdiction over this case, therefore, the core of limited jurisdiction is that as long as the influence or violation of a computer cybercrime has some connection with its own nationals, that country can exercise its jurisdiction in accordance with its own laws.

* 1. *The principle of minimum contact*

The principle of minimum contact means that the defendant in the case has no transaction or tort in the jurisdiction of the court and the court exercises criminal jurisdiction over the case, there should be some minimal contact between the accused and the court in order to meet the requirements of due process provisions and fairness[6]. This principle, established by the United States Supreme Court, is a principle commonly used by the United States when it comes to the application of criminal or civil and commercial jurisdiction in a computer cyber- environment. According to the principle of minimum contact, the establishment of the relationship of jurisdiction between the perpetrator and the court requires minimal contact. The criterion of such contact can be summarized as follows: Courts may exercise jurisdiction over unlawful acts of the network if the perpetrator is intended to be protected by the laws of other states, or if he proactively places his network activity under the jurisdiction of other state courts. If the perpetrator simply provides unilateral information or advertisements on the site and does not have any interaction with the interviewer, the court should not exercise jurisdiction over it; However, courts may be able to exercise jurisdiction over unlawful acts of computer cyber-law if the perpetrator, in addition to providing information and advertising, offers other related services or online transactions of the goods when interacting with visitors.

# Establishment and Perfection of Criminal Jurisdiction System of computer cybercrime

The criminal jurisdiction system refers to the territoriality principle, personal principle, protection principle and the principle of universal jurisdiction, complement each other and form a kind of criminal jurisdiction principle structure[7].The principles of criminal jurisdiction vary from one country to another. Some are single-unit structures (for example, only the principle of territoriality) and some are complex structures (one principle and other principles). China adheres to the principle of territorial jurisdiction as the main principle, supplemented by the principles of personal jurisdiction, protection of jurisdiction and universal jurisdiction. This model effectively protects the legitimate rights and interests of the Chinese nation and its citizens. There is a large degree of consistency between computer cybercrime and traditional crime. Although different from the traditional crime in the means and form of crime, the traditional criminal jurisdiction system still applies to the new type of computer cybercrime. The emerging fields such as the place of transmission, the location of the web site, the place of visit and the location of the network terminal proposed in the previous article are basically in accordance with the principle of territorial jurisdiction and personal jurisdiction and can solve the problem of space effectiveness according to the traditional criminal jurisdiction system. At the same time, the new theory of sovereignty, the limited jurisdiction, the theory of relativity and the jurisdiction of web site, which have been separated from the system of criminal jurisdiction, can resolve the conflict of criminal jurisdiction in a certain area, however, computer cybercrime does not constitute a crime that is completely independent of traditional crimes and still possesses the necessary elements of due diligence, illegality and accountability of constituent elements, and needs to be evaluated within the framework of law. China does not make any special regulation on computer cybercrime. Therefore, the criminal jurisdiction of computer cybercrime needs to be determined under the criminal jurisdiction system of our country.

* 1. *Apply the principle of "priority of power"*

The system of criminal jurisdiction should adhere to the principle of "priority of power", that is, the principle of territorial jurisdiction and the principle of personal jurisdiction. The principle of the protection of jurisdiction takes precedence over the principle of universal jurisdiction [8].The first three principles are exercised for the protection of national sovereignty and national interests. The principle of universal jurisdiction is exercised in accordance with the obligations in the international treaties concluded and acceded by a country. When conflicts of interests diverge, it is clear that national interests should be given the highest priority. Therefore, the first three principles stand out from the latter. When the exercise of universal jurisdiction conflicts with territories, nationalities and protection of jurisdiction, the state should uphold the principle of "priority of power." The principle of exercising universal jurisdiction on the precondition of safeguarding the sovereignty of a country corresponds to the original meaning of the principle of universal jurisdiction in the international community. Before there is no specific legislative provision on computer cybercrime, the criminal jurisdiction of computer cybercrime should also be exercised in accordance with the principle of "priority of power" and to exercise universal jurisdiction based on international treaties without prejudice to the interests of the state.

* 1. *Adhere to the principle of "territorial superior rights"*

Article 22 of the "Convention on computer cybercrime"(The first international convention on cybercrime by the European Council in 2001,) clearly stipulates the conflicts of jurisdiction between nations. For computer cybercrime stipulated in the "Convention", its criminal jurisdiction is subject to territorial jurisdiction and adopts the principle of belonging to persons. Territorial jurisdiction extends to a portion of "virtual territory" in addition to its own territory, including ships flying the flag of the country and aircraft registered under the laws of the parties. D of the first paragraph of the article also provides for the principle of personal jurisdiction as pertaining to cases where its own citizens should be punished for the commission of the crime or outside the jurisdiction of other States and the parties may exercise jurisdiction. Therefore, the provisions of the Convention uphold the superiority of territorial jurisdiction; adhere to the sovereignty of the country as the center. At the same time, it is stipulated that the relevant clauses can be reserved. And for the conflict of jurisdiction, the contracting parties can negotiate to resolve, it is a model for countries to establish the criminal jurisdiction system and resolve the conflict of jurisdiction.

* 1. *Establish criminal jurisdiction dispute negotiation system*

Computer cybercrime appears a short time, so computer cybercrime has not yet formed its own system as compared with traditional criminal offenses. The norms of computer cybercrime established by various countries on the basis of their respective national conditions differ. Therefore, it is inevitable that reunification will occur when contradictions arise. Article 22, paragraph 5, of the "Convention on computer cybercrime" clearly sets out the application of the system of consultation on controversial cases in the event of a conflict of jurisdiction in the parties, The consultation system can effectively solve the competing disputes of jurisdiction between different countries, which not only saves the judicial resources but also reduces the possibility of the perpetrators being punished by different countries. China does not establish a consultative system of jurisdictional dispute cases. However, the continuous escalation of computer cybercrime requires effective consultation and cooperation among all countries so as to jointly resolve the conflict over criminal jurisdiction.

* 1. *Draw on the civil jurisdiction of computer cybercrime system*

Conflicts of civil jurisdiction that also exist in the civil sphere exist only because of the extent of the legal interests infringed by unlawful conduct in two different areas. The conflict of jurisdiction in the field of civil litigation is mainly caused by the infringement of the Internet. At the same time, it also includes the emergence of the problems in the field of electronic contract. The most common one is the use of the Internet to infringe upon the copyright of others. The proportion of Internet infringement cases is constantly rising. It can be seen that there are also issues of jurisdictional conflicts in the international civil field, and such conflicts have prompted all countries to continuously expand their own civil jurisdiction. However, civil jurisdiction differs from criminal jurisdiction in that the principle of international coordination plays a crucial role in avoiding and eliminating conflicts of jurisdiction. The basic principles of international coordination of civil jurisdiction in network cases should include following the principle of the sovereignty of other countries, safeguarding the principle of international interests, the principle of effectiveness and convenience, the principle of international comity, and the principle of self-control of jurisdiction. These principles help all countries to better coordinate the conflicts in the jurisdiction of international civil cases and urge all countries to maintain the order and stability in the computer cyberspace and promote the harmonious development of human society while maintaining the sovereignty and national interests of the country. These principles are in line with the general principles of the international community and are worth learning from the system for international criminal jurisdiction.

China's provisions on the jurisdiction over civil cases under network environment are relatively clear. Article 1 of the Supreme People's Court's Interpretations on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Networks issued in 2004 stipulates: "Cases of copyright infringement on the Internet are governed by the courts of the place of infringement or the place of residence of the defendant, where the infringing acts include the web server of the infringing act, the location of the computer terminal and other equipment. Where it is difficult to determine the place of infringement and the place of residence of the defendant, the location of the computer terminal or other equipment where the plaintiff discovers the contents of the infringement can be regarded as the location of infringement." It can be seen that this judicial interpretation in china can effectively solve the conflicts of jurisdiction in practice. In addition to stipulating infringements and defendants' residences, this judicial interpretation also stipulates infringements including the location of the web server and the location of the computer terminal. However, there is no such requirement in the area of criminal justice. Although there is controversy on the theory of network servers and computer terminals, this clearness rule is conducive to the determination of civil jurisdiction in china, which is worth our reference in the field of criminal justice.