MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

International Collaborative Responses to Transnational Cybercrime: how China Strengthen its Capacity to Combat Transnational Cybercrime

Jiang N[1]* and Bing S[2]

[1]Law Professor, Beijing Normal University, China

[2]PhD, Beijing Normal University, China

***Corresponding author:** Jiang Na, Law Professor, Beijing Normal University, China, Email: na.jiang@bnu.edu.cn

Review Article

Volume 9 Issue 2

Received Date: March 26, 2024

Published Date: May 15, 2024

DOI: 10.23880/ijfsc-16000382

Abstract

The borderless nature of the Internet has greatly facilitated the growth of crime in cyberspace. Cybercrime today has caused huge economic losses worldwide and is violating the right to privacy on a massive scale. The consequences of cybercrime are serious and often occur in different countries and regions. The priority of territorial jurisdiction has been affected by transnational cybercrime., and its convenient application has been lost when the results of the crime are generalized. The basis of subjective territoriality and objective territoriality would be unclear. The abstract cross-border nature of cybercrime has led to frequent conflicts of jurisdiction among States and may even lead to the legal hegemony of cyber-technology powerhouses. The traditional extradition mechanism has gradually failed to respond to the interstate demand to combat transnational cybercrime. In recent years, China has not only introduced strategic policies at the national level to safeguard cybersecurity and combat cybercrime, but has also made progress in criminal legislation, administrative legislation and international cooperation legislation. China has also accumulated experience in police cooperation to combat transnational cybercrime. In order to better cooperate with other countries in international cybercrime , China should actively participate in the formulation of international conventions and regional multilateral agreements on the punishment of cybercrime. It should also further improve its domestic legislation.

Keywords: Cybercrime; Jurisdiction; International Cooperation

Introduction

We are in the age of high-speed development of information networks. While bringing convenience, efficiency and economic gains, the Internet has also become a natural breeding ground for crime. Mainly because the cross-border nature of the network facilitates the hiding and absconding of criminals. Transnational cybercrime has developed the characteristics of a wide area of harm, serious results and a low rate of prosecution. The continuous growth of cybercrime on a global scale has exposed the low effectiveness that to combat transnational cybercrime. International collaborative is the best choice at present. China, as a cyber-technology powerhouse, should take responsibility in addressing the issue of transnational cybercrime. This paper discusses three issues: first, why cybercrime requires international cooperation; second, what China has achieved in combating transnational cybercrime and what shortcomings remain; and third, what China should improve in order to enhance its ability to combat transnational cybercrime.

Why Cybercrime Requires International Collaboration

According to the provisions of the Budapest Convention, adopted by the Council of Europe in 2001, cybercrime can be categorized into the following four types: 1. Offences against the confidentiality, integrity and availability of computer data and systems. This category includes five offenses: illegal access illegal interception data interference system interference and misuse of devices. 2. Computer-related offences. This category includes two offenses: computer-related forgery and computer-related fraud. 3. Content-related offences. This category includes one offense: offences related to child pornography. 4. Offences related to infringements of copyright and related rights. This category includes one offense: offences related to infringements of copyright and related rights [1]. In China, cybercrime is divided into pure cybercrime and impure cybercrime. Pure cybercrime refers to crimes that can only be constituted in the form of cybercrime , such as the crime of intrusion into a computer information system. Impure cybercrime refers to crimes that can be constituted either in the form of cybercrime or in the form of non-cybercrime. For example, the traditional crime of theft can be committed both by network and non-network forms. In China, some scholars have categorized cybercrime into the following three types: (1) crimes against computer information systems; (2) traditional crimes committed through the use of computer networks; and (3) crimes against network order [2].

Cybercrime requires more inter-State cooperation than traditional cross-border crime. The main reason for this is that the continued high incidence of cybercrime and its incalculable harmful results have seriously undermined global economic security and order. Cybercrime can cross the physical territory of multiple countries in an instant, leading to jurisdictional conflicts in multiple countries and thus limiting the ability of criminal law to combat the crime. Traditional modes of international criminal justice cooperation, such as extradition and mutual legal assistance in criminal matters, have difficulty in fulfilling their basic functions in the face of cross-border cybercrime, which is closely related to the diverse forms of cybercrime and the cross-border storage of data.

Cross-Border Attributes and Serious Criminal Outcomes of Cybercrime

Computer information technology has revolutionized the way of production and life of mankind, and the emergence of cyberspace has greatly increased communication and interaction between people and brought people closer together. It can be said that the exchange of information in cyberspace has to a certain extent dissolved the prejudices and contradictions between countries, societies and groups. Human work synergy and exchange of ideas have reached an unprecedented scale, which in turn has influenced the progress and sustainable development of human science and technology [3]. However, cybercrime has also been iterated and upgraded with the continuous improvement of cyberspace. At the present stage, there are not only digitized traditional crimes in cyberspace, but also new types of crimes brought about by new cybertechnologies, such as cloud computing, artificial intelligence and cryptocurrencies.

Globally, cybercrime has shown a consistent growth. According to data released by the U.S. Center for Strategic and International Studies, the personal information of more than 2 billion Internet users around the world has been stolen or compromised, and cybercrime cost the global economy approximately $500 billion in 2014, or about 0.7% of global revenue [4]. The sophistication of cybertechnology and the increasing speed of global Internet connectivity, coupled with the anonymity of the Internet space, have made cybercrime a high-yield, low-risk criminal activity [5]. The ease with which criminals in large-scale cybercrime operations can acquire vast sums of money with few arrests or prosecutions has undoubtedly made cybercrime more and more prevalent [6]. For example, in 2021, Colonial Pipeline, the largest fuel pipeline company in the United States, was attacked by the “Dark Side”, a group of cybercriminals. The criminals succeeded in illegally obtaining 100GB of data and a large ransom before disappearing, and no arrests have been made to date [7].

Cybercrime is often committed against unspecified individuals and organizations. These crime targets have different nationalities or are located in different places, which results in a large base of crime targets, making it difficult to estimate the actual harm caused by the crime and greatly increasing the difficulty of investigation in various countries. For example, the Australian police cracked a cross-border credit card theft case. In this case, the criminals used network hacking technology to illegally obtain the credit card account passwords of more than 500,000 Australian residents, and then extracted cash through cross-border transfers after successfully stealing the account information. The case actually covered China, South Korea, the U.S. and some European countries [8].

In China, the threat of cybercrime also persists. In 2020, a total of 142,000 cybercrime suspects were prosecuted within China, up 47.9 percent year-on-year. According to data released by the Supreme People’s Procuratorate of the People’s Republic of China in 2021, 13 percent of the total number of prosecuted cybercrimes were committed across borders. In addition, in order to evade the Chinese police, criminals systematically transfer their criminal dens and

communication tools, etc., outside China, and purposefully target Chinese citizens to commit cross-border crimes. The most representative of these crimes is telecom, online fraud. In China, cross-border telecommunication online fraud crime has become the most serious cybercrime, and in 2021, Chinese police cracked down on 370,000 cases of telecommunication online fraud crime, and this number rose to 391,000 cases in 2022 [9]. In 2021, Chinese police cracked down on 370,000 cases of telecommunication online fraud crime, and this figure rose to 391,000 cases. In 2021, Chinese police cracked down on more than 10,600 illegal exit gangs of more than three people ganged up by Chinese public security organs, solved more than 5,300 criminal cases, and arrested more than 44,690 criminal suspects [10]. A huge number of cross-border network fraud has seriously jeopardized China's social stability and economic security. More notably, the use of the dark web and offshore communication software in cybercrime has increased significantly. in 2020, Chinese prosecutors handled nearly 70 percent year-on-year growth in cybercrime cases committed using the dark web or offshore communication software [11].

The high incidence of cybercrime on a global scale actually reflects the unsatisfactory effectiveness of states in combating cybercrime. The complexity of cyberspace provides criminals with opportunities to hide, and it is difficult for investigating authorities to identify and locate criminals after a crime has been committed accurately and quickly. The generalization of harmful outcomes has greatly increased the harmfulness of cross-border cybercrime. From the reality of enhancing the capacity to combat cybercrime, strengthening cooperation is the only option.

Failure of Traditional Jurisdictional Theories Due to Cross-Border Cybercrime

Since there is no physical field in cyberspace, and the interconnection of global networks is becoming more and more intense, cybercrime can be easily transnationalized with "one click". When the offender in country A uses the springboard software located in country B to steal the data on the server in country C, the abstract border crossing of cybercrime occurs. Abstract border-crossing means that the perpetrator himself or his criminal behavior is not implemented in the field of a country, but only in the form of network signals or data transmission across the transit of a country [12]. The perpetrator's criminal act crosses several countries at the same time in cyberspace. This poses at least three problems in terms of jurisdiction: first, the dismantling of the jurisdictional system based on the principle of territoriality; second, the jurisdictional difficulties posed by the varying characterization of criminal acts in different jurisdictions; third, the conflict of jurisdiction.

In international law, the term "jurisdiction" describes the rights of States to regulate conduct and the limitations on those rights [13]. The establishment by States of criminal jurisdiction over crimes is the basis of criminal law [14]. Under customary international law, the exercise of jurisdiction by States is based on three main foundations: nationality, territory and universality [15]. Since the scope territory jurisdiction is identical to the territorial scope of a State, the exercise of jurisdiction by the State is most justified within its territorial scope. National criminal jurisdiction is coterminous with sovereignty, and thus states usually require that an offence occur within their territory before they exercise jurisdiction [16]. Territoriality is practical—that's where the harm is done, that is where the evidence is, and that is where the interest in suppression is [17]. Although there was no hierarchy among the different bases of jurisdiction, international practice showed that the territorial State had preferential jurisdiction for the prosecution of international crimes [18]. Challenges posed by cybercrime to territorial jurisdiction are first and foremost the impact of the decentralization of the place of the results of the crime . The greatest challenge posed by cybercrime to territorial jurisdiction is the impact on the status of territorial jurisdiction of the decentralization of the place of result of the crime. According to the principle of effects, although the elements of an offence do not take place within the territorial boundaries of a State, the significant harmful consequences of the offence are actually felt in the territory of that State, which is then entitled to jurisdiction over the offence. Therefore, in some cases where the results are spread throughout an unspecified place, such as the network dissemination of obscene information, fraudulent information, terrorism information, according to territorial jurisdiction, any court in the place where the harmful result occurred may try the conduc t. At this point, the convenience of territorial jurisdiction of the advantage will be transformed into a disadvantage. Competing jurisdictions among countries have a negative impact on the investigation of cases, because when a country asserts jurisdiction, other countries will inevitably oppose it. At this time, on the contrary, personal jurisdiction is more applicable. The nationality of the perpetrator of the crime is not controversial. In addition, when the harm of a certain cross-border cybercrime spreads all over the world, it may even be regarded as an international crime. Then universal jurisdiction may replace territorial jurisdiction. Thus, both personal and universal jurisdiction have a tendency to overtake the status of territorial jurisdiction. Second, cybercrime also blurs the jurisdictional basis of territoriality. According to the principle of territoriality, a State may exercise jurisdiction over a criminal act when at least one of the constituent elements of the criminal conduct (subjective territoriality) or the result (objective territoriality) occurs in

the territory of that State. The criminal conduct and the result of the crime are the basis for territoriality. The problem is that in the case of cybercrime, it is difficult to define where the criminal conduct takes place and where the result of the crime occurs. For example, in the abstract border-crossing issue mentioned above, the perpetrator uses a server located in another country to commit an act that produces harmful consequences in another country. Is the location of the server the place of the criminal conduct, or is the country where the perpetrator is located the place of the criminal conduct? A representative case is the 1999 British case of Regina v Graham Waddon. In this case, Waddon engaged in large-scale Internet pornography from his home in the U.K. using a server located in the U.S. Waddon was prosecuted and argued that the U.K. courts had no jurisdiction to try him because the server he was using was not in the U.K. But the court have held that "In the instant case an act of publication took place when the data was transmitted by the defendant or his agent to the service provider, and the publication or transmission was in effect still taking place when the data was received. Both the sending and receiving took place within the jurisdiction of the court and it was irrelevant that the transmission may have left the jurisdiction in between the sending and receiving……" [19]. The court actually recognized that the location of the perpetrator at the time of the release of the information was the place where the offense was committed.

Under the principles of territoriality in effect and negative personal jurisdiction, States can assert jurisdiction in criminal cases involving serious violations of the interests of the State and its citizens. On a broader scale, the principle of protective jurisdiction allows States to establish jurisdiction over crimes where the elements of the crime are wholly extraterritorial and which have an impact on or threaten the sovereignty, security, integrity and governmental functions of the State. The dilemma posed by cybercrime is the difficulty of asserting jurisdiction due to differences in criminal justice systems and the varying characterization of cybercrime by States. For example, when a State is prepared to apply criminal law to a criminal act based on the principle of territoriality effect, the State where the criminal act was committed does not consider such an act to constitute a criminal offense. An example is Internet gambling. A more serious problem is that in countries with different standards of punishment for a given criminal act, especially when identifying norms that are strongly influenced by a country's political culture, national traditions, and social practices, current jurisdictional doctrines may disregard cultural pluralism and force the other side to accept their own values, thus moving towards cultural imperialism [20].

Another potential problem is that the generalization of the harmful results of cybercrime seems to place a demand on citizens - the need to know the laws of each country and to ensure that they do not commit crimes. Otherwise there is a risk of being sanctioned by a particular country because of the abstract cross-border nature of the behavior.

Cross-border cybercrime has brought about a new round of international discussions on extraterritorial jurisdiction. The establishment of extraterritorial jurisdiction is necessary to ensure that transnational criminals are not able to use national boundaries to avoid the law [21]. Extraterritorial jurisdiction is generally understood as the exercise of jurisdiction by a State over acts occurring outside its territorial boundaries [22]. A fundamental characteristic of extraterritorial jurisdiction is its transnational nature [23]. Therefore, when a State exercises extraterritorial jurisdiction, the question of conflicts of jurisdiction with other States inevitably arises. The problem is that how to resolve conflicts of jurisdiction is a real issue. In the absence of a universal principle of conflict of jurisdiction, the resolution of conflict of jurisdiction has a strong political dependency. Since the mechanism for resolving conflicts of criminal jurisdiction in the international arena has not been established, the rules for resolving conflicts of jurisdiction, such as the "principle of equity", the "principle of actual jurisdiction" and the "principle of priority jurisdiction", are still mostly applied between sovereign States and regions with similar political systems and criminal justice systems [24]. A further problem is that States competing for criminal jurisdiction over cybercrime will further expand the scope of the jurisdictional principle in cyberspace, which will reduce territorial States with clear physical boundaries to cybercolonies without physical boundaries [25]. In the current situation where the level of cyber technology varies greatly among countries in the world, cyber-technology powerhouses are expanding their jurisdictions in cyberspace on the basis of their developed technology, thereby compressing the sovereignty of other countries and realizing their legal hegemony.

Therefore, in order to avoid political conflicts and legal hegemony brought about by cross-border cybercrime, international cooperation and coordination are of particular importance. Effective international cooperation mechanisms, accepted by the vast majority of countries, are the best solution to jurisdictional conflicts. In addition, international rules for combating cross-border cybercrime can maximize the elimination of differences in criminal justice mechanisms between countries and are conducive to the protection of civil rights. The updating of jurisdictional theories and the resolution of jurisdictional conflicts also depended on the development of new, widely recognized jurisdictional principles among States with regard to transnational cybercrime.

Inadequacy of Existing International Cooperation Mechanisms Against Transnational Cybercrime

Generally speaking, the main purpose of traditional criminals in organizing and committing crimes in border areas is to evade justice. The State affected by the crime, for reasons of threat or reprisal, is required to bring the criminals, who are located outside its territory, back to the country for trial in order to maintain its judicial order. This process must be limited by the principle of sovereignty. The principle of sovereignty is the clearest and most prominent principle in public international law. Therefore, the exercise of extraterritoriality requires the authorization and cooperation of the State concerned. There are no national borders in cyberspace, so cyberspace provides a perfect haven for criminals' cross-border crimes. The ineffectiveness of the global fight against cross-border cybercrime actually exposes the failure of the inter-State cooperation model.

Extradition, as the oldest form of judicial cooperation among States, refers to the delivery of an accused or a convicted individual to the state where he is accused of or has been convicted of, a crime, by the state on whose territory he happens to be for the time to be [26]. There is no obligation to extradite under customary international law. The obligation to extradite generally arises in the context of an extradition treaty or on the basis of the principle of reciprocity [27]. There is no universal multilateral convention on extradition, but there are other regional conventions on extradition. For example, the 1981 Inter-American Convention on Extradition and the Council of Europe's 1957 European Convention on Extradition. In 1990, the General Assembly of the United Nations adopted the Resolution for the Model Treaty on Extradition 45/116, which provides a template for bilateral extradition treaties. The Model Treaty on Extradition enumerate mandatory grounds for refusing extradition and optional grounds for refusing extradition. Among these grounds, the principle of dual criminality and aut dedere aut judicare stand out as two of the current problems in inter-State cooperation in combating transnational cybercrime.

The principle of dual criminality means that the act for which extradition is requested constitutes a crime under the laws of both the requesting and requested States [28]. This is the embodiment of the principle of the legality of crime and punishment in the field of international criminal justice cooperation. However, at present, legislation on cybercrime is still in the developmental stage, and the provisions on cybercrime vary greatly from country to country. Therefore, in the case where an act is criminalized in the extradition requesting country, but the requested country does not criminalize the same act, the criminals can escape from trial according to the principle of double criminality. This is not only detrimental to the maintenance of domestic law and order in the requesting country, but also increases the risk of the requested country becoming a haven for criminals. In China, large-scale online cross-border gambling often involves huge amounts of money and hidden criminal means. However, due to the different criteria for determining the legality of the betting industry in the countries where the offenders are located, the investigation of cases often comes to a standstill. The existence of the principle of dual criminality hinders extradition, and criminals are likely to go unpunished.

In recent years, aut dedere aut judicare have been incorporated into almost all legal documents on international judicial cooperation in criminal matters. This principle, which means 'either extradite or prosecute' is invoked as an international effort to inhibit impunity and to ensure that states do not end up harboring criminals [29]. Professor Bassiouni gave the principle the highest praise. He considered the aut dedere aut judicare rule to be the cornerstone of the indirect enforcement regime of international criminal law [30]. The current situation was that States did not consider the obligation aut dedere aut judicare to be part of general international law, with the exception of some specific international crimes [31]. Thus, aut dedere aut judicare does not currently have the effect of a rule of customary international law. In the context of cybercrime, cybercrime has not yet been recognized as an international crime. It is then difficult to prove that the requested State has an obligation to prosecute cybercrime in cases where the requested State legally refuses to extradite (e.g., by following the principle of non-extradition of its own nationals or by invoking the humanitarian clause).

Progress and Shortcomings: The Current Status of China's Fight Against Cross-Border Cybercrime

In recent years, China has been committed to combating cross-border cybercrime in order to safeguard the country's cybersecurity, social order and the safety of people's lives and property. At the domestic legislative level, China had adopted a number of administrative laws relating to data and cybersecurity and had amended the provisions of its criminal law relating to cybercrime. To promote international cooperation, China had adopted legislation on judicial assistance in criminal matters. In terms of criminal law enforcement cooperation, China had entered into a number of police cooperation with neighboring countries to combat cross-border cybercrime.

Progress

The Chinese Government has always attached great importance to institution-building in cyberspace. Cybercrime

is the most serious threat to the healthy development of cyberspace, and thus combating cybercrime has been within the strategic framework of China's efforts to build order in cyberspace. At the policy and strategy level, the Chinese government released the National Cyberspace Security Strategy and the Strategy for International Cooperation in Cyberspace in 2016 and 2017 respectively. In the National Strategy for Cyberspace Security, the Chinese government proposed nine tasks, including strengthening international cooperation in cyberspace [32]. In the Strategy for International Cooperation in Cyberspace, the Chinese Government proposes that international cooperation in cyberspace should be promoted on the basis of the four basic principles of peace, sovereignty, common governance and reciprocity [33]. After the introduction of artificial intelligence technology, the Chinese government released the New Generation Artificial Intelligence Development Plan in 2017. This series of documents basically laid down the basic position of the Chinese government when facing the punishment of crimes in cyberspace.

At the level of administrative legislation, in 2016 China enacted the Cybersecurity Law, which is China's foundational legislation in the field of cybersecurity. The Cybersecurity Law not only defines what cybersecurity is [34], but also establishes China's six legal regimes in cyberspace: cyberspace sovereignty, the security and protection of critical information infrastructures, the localization and storage of important data, the protection of personal information, the cultivation of cybersecurity personnel, and the punishment of new types of cybercrimes [35]. In particular, it has formulated rules restricting the cross-border transfer of data [36]. In 2017, China promulgated the Data Security Law. This is the first foundational law in the field of data security in China. The Data Security Law not only clarifies the basic principles of data management, the regulatory mechanism of data and the basic system of data management, but also clarifies the jurisdiction of the Data Security Law. The Data Security Law has refined the rules on cross-border flow of data in the Cyber Security Law. It not only stipulates the rules for the regulation of data, but also clarifies the data export control system. For requests for data from foreign judicial or law enforcement agencies, the authorities shall handle the requests in accordance with the law and international treaties and agreements concluded or participated by China, or in accordance with the principle of equality and reciprocity. Without the approval of the competent authority of the People's Republic of China, a domestic organization or individual shall not provide data stored in the territory of the People's Republic of China to any foreign judicial or law enforcement authority [37]. 2021 China enacted the Personal Information Protection Law. This is the first law in China that systematically and comprehensively protects personal information. The Law on the Protection of Personal Information contains detailed provisions on expanding the scope of protection of personal information, constructing rules for the protection of sensitive personal information, and regulating the handling of personal information by State organs [38].

At the level of cybercrime, in 2015 the Standing Committee of the National People's Congress of China adopted the ninth amendment to the Criminal Law. This amendment, on the basis of the existing criminal law, added the crimes of refusing to fulfill the obligation of information network security management, illegal use of information network, and aiding information network criminal activities. The obligations and criminal liabilities of network service providers have been strengthened, and the act of assisting network crimes has been criminalized and punished. At the same time, entity is added as criminal subject for the crimes of illegal intrusion into computer information systems, illegal acquisition of computer information system data, illegal control of computer information systems, and the provision of programs and tools for the crimes of intrusion into or illegal control of computer information systems. The purpose of preventing the emergence of serious harmful consequences is achieved through the early intervention of criminal law in behavior.

In terms of international judicial cooperation in criminal matters, China introduced the Law of International Criminal Judicial Assistance in 2018 in order to solidify the legal basis of China's judicial assistance in criminal matters. In order to accelerate the access to electronic data outside China to achieve effective crime-fighting, in 2016 China's Supreme People's Court, Supreme People's Procuratorate, and Ministry of Public Security promulgated the Provisions on Several Issues Concerning the Collection, Taking , Examination and Judgment of Electronic Data in the Handling of Criminal Cases. In this provision, remote network inspection and electronic data taking were created. In 2019, China's Ministry of Public Security formulated the Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases. The rules refined the scope of application of remote network inspection and electronic data taking.

In the field of law enforcement cooperation, China has carried out a number of cross-border police cooperation with the Myanmar government in order to combat transnational telecommunication online fraud. 2023 On October 1, 209 suspects of cyber fraud were handed over from Myanmar to China. On October 9, 2023, a total of 706 suspects of fraud in Myanmar were handed over to the police of China's Yunnan Province.2024 In the same year, China has also handed over to the police of China's Yunnan Province a total of 31,000 suspects of cyber fraud. To date, a total of 31,000 suspected cyberfraud criminals have been handed over to China by the

Myanmar government in 2023, including 63 organizers and masterminds, and 1,531 suspects had been wanted by the police [39].

Problems

Chinese scholars have long recognized the problems of jurisdictional conflict and failure of territorial jurisdiction arising from the cross-border nature of cybercrime. As a result, an academic discussion on the improvement of jurisdictional principles in the age of information networks has been initiated. There is still no universally accepted conclusion as to whether cybercrime should be subject to protective jurisdiction, universal jurisdiction, the expansion of the scope of territorial jurisdiction or the establishment of special jurisdictional rules for cybercrime. In reality, however, overly obsessing over cybercrime jurisdictional rules and neglecting the resolution of jurisdictional conflicts is an act of putting the cart before the horse. Strengthening international cooperation, as well as formulating cybercrime conventions, and reaching bilateral or multilateral agreements or even case-by-case agreements in cases of jurisdictional conflicts, are the obvious choices for resolving transnational cybercrime jurisdictional conflicts. Unfortunately, China is not currently a party to the Budapest Convention. Nor has a multilateral cybercrime convention been reached within the framework of the United Nations. Nor has China signed a multilateral cybercrime treaty or agreement with neighboring countries. As a result, there is no universally applicable jurisdictional rule for resolving conflicts of jurisdiction over cybercrime, either in theory or in practice.

Furthermore, China's Extradition Law was promulgated in 2000. In the 20 years that the Law has been in force, the extradition systems of various countries have undergone considerable changes. In practice, some experience has emerged that is worth learning from. In particular, transnational cybercrime has brought some new challenges to the extradition system. However, China's Extradition Law has not been revised, which makes it difficult to meet the systemic demands of interstate cooperation in the age of information networks.

It is particularly noteworthy that, whether for the purpose of prosecuting national criminals or for the purpose of extradition, countries conducting criminal investigations into cross-border cybercrime cannot avoid cross-border access to electronic data. Although China's Criminal Procedure Law, the Law on International Criminal Judicial Assistance and the two Rules on Electronic Evidence have all made provisions for cross-border access to electronic evidence, China's current system for cross-border access to electronic data still suffers from significant shortcomings. The scope of cyber access has been significantly limited in the electronic data forensics rules formulated by the Ministry of Public Security in 2019. In principle, investigative authorities can only directly access data located in computer systems outside China that have been made public, but not data that have not been made public. As for data within China, investigative authorities can directly collect and extract them. This rule was originally designed to prevent infringement of the sovereignty of other countries by accessing electronic data outside China, as law enforcement jurisdiction is strongly territorial. However, the consequence of the difference in the scope of data access within and outside the country is the weakening of the protection of the rights and interests of data subjects within the country. Raising the threshold for data access outside the country sends a message to criminals that transferring data involved in a case outside the country can make investigation more difficult. Instead, it increases the chances that data will flow out of the country, thereby reducing China's actual effectiveness in combating cybercrime. In addition, neither the Criminal Procedure Law nor the relevant electronic evidence rules prohibit Chinese investigative authorities from accessing electronic data from abroad. However, the Law on International Criminal Judicial Assistance prohibits relevant units, organizations and individuals in China from providing data to law enforcement authorities abroad without the permission of the competent authorities. In other words, Chinese investigative authorities cannot independently cooperate with foreign investigative authorities to retrieve data located in China. This kind of differentiated data access rule actually carries a discriminatory color. It is not conducive to China's active participation in or leadership of cybercrime conventions in the future, or to international cooperation in combating cybercrime.

Recommendations

For the reasons mentioned above, international cooperation in combating cybercrime has become an international trend. China's participation in international cooperation to combat cybercrime still leaves much to be desired.

Improving the effectiveness of the fight against transnational cybercrime requires placing States within the framework of a harmonized international criminal law. The purpose of doing so is to reach a basic consensus among countries on the fundamental nature and jurisdictional principles of cybercrime. This will not only help to avoid the emergence of criminal havens, but also, and more importantly, greatly facilitate judicial and law enforcement cooperation among countries. China is not a member of the Budapest Convention. At present, China should actively participate in the formulation of a convention on cybercrime under the framework of the United Nations. It should also focus on the conflict of jurisdiction over cybercrime and reach a conflict resolution mechanism among countries.

China should reach bilateral or multilateral agreements with other countries to punish cybercrime and agree on solutions to jurisdictional conflicts. China is a member of several regional intergovernmental cooperation organizations, such as the Shanghai Cooperation Organization and the Lancang-Mekong Cooperation. It is easier for member countries to build on their existing cooperation and reach consensus on collaborative efforts to combat transnational cybercrime. China should actively promote the conclusion of multilateral agreements to punish cybercrime among the member countries of such organizations. In addition, while building international rules, attention must be paid to the reasonable docking of domestic laws and international rules. At the current level of law enforcement cooperation, China must meticulously compare domestic investigation and evidence-gathering techniques with foreign measures and, on that basis, consider promoting the regional integration of standards and conditions for the transformation of measures between different countries and regions [40]. In order to improve the practical effectiveness of international law enforcement cooperation. It is worth emphasizing in particular that cooperation mechanisms, whether under the framework of the United Nations or at the interregional level, should focus on the following two aspects: first, States should harmonize the definition of cybercrime terminology. What is cybercrime, what are the offences of cybercrime and what constitutes the offence must be harmonized across countries. It is important to avoid, at the source, situations in which criminals get away with it because of differences in the provisions of the domestic laws of various countries. For example, as mentioned above, the principle of dual criminality is not met, making it impossible to extradite criminals. Secondly, it is important to incorporate the principle of aut dedere aut judicare into the United Nations Convention on Cybercrime or regional cybercrime agreements. It is virtually impossible for a country to arrest and return all cybercriminals located outside its borders, not only because of the cost of prosecution, but also because of the limitations imposed by the decentralization of cybercrime results. Aut dedere aut judicare among States would be conducive to more efficient prosecution of offenders. In addition, attention should be paid to the transfer of criminal procedure as a means of cooperation. The threshold for the transfer of criminal procedure should be lowered and the procedural requirements for transfer should be appropriately simplified.

In fact, there is no doubt about the difficulty of developing norms of uniform law. Until international norms to punish cybercrime are in place, the most important thing is to implement existing cooperation mechanisms more effectively. As mentioned above, China's Extradition Law is no longer able to meet the real needs of efficient interstate cooperation in the face of rapidly changing cybercrime. Although electronic data in cyberspace is easier to back up than physical data, it is also easier to be tampered with and destroyed. The excessively lengthy extradition process provides an opportunity for anyone in cyberspace to hide, transfer or destroy electronic data. Therefore, China's Extradition Law should be revised and improved as soon as possible. Consideration can be given to clarifying the simplified extradition system so that under the condition that the requested person agrees to accept extradition voluntarily, the requested country can omit the general examination procedure and quickly hand over the person to the requesting country. That would save judicial resources and speed up the process of international cooperation, thus increasing the efficiency of combating transnational cybercrime..

The interconnectedness of networks results in spillover effects of domestic laws. Transnational cybercrime facilitates the frequency of cooperation between States and makes it possible for a country's domestic law to play a role in international cooperation or to be scrutinized frequently. Therefore, China should transform its existing unilateral legislative thinking. It should be based on its own position of cyber sovereignty, while avoiding differential treatment of the same situation at home. At the same time, China should pay attention to the possible damage to rights and interests brought about by the principle of reciprocity while innovating its legislation.

Conclusion

The principle of State sovereignty is always at the center stage of public international law. Although cyberspace has no physical boundaries, the governance of cybercrime still needs to comply with the principle of national sovereignty. Otherwise, jurisdiction over cybercrime will become a magnificent excuse for violating the sovereignty of other countries. This is not only unfavorable to the development of equal and mutually beneficial diplomatic relations between countries, but also gives criminals an opportunity to take advantage of. This paper discusses the negative impact of cybercrime on the international order and the principles of international law, and concludes that there should be concerted efforts among countries to govern transnational cybercrime. As a country with advanced cyber technology, China bears an important responsibility for maintaining international cyber security. Although it has made some achievements in punishing cybercrime, China still has a long way to go on the road to order in cyberspace.

References

1. (2024) The Budapest Convention (ETS No. 185) and its Protocols. Cybercrime.

2. Xingliang C (2021) Types of cybercrime and their judicial

definition. Research on Rule of Law.

3. Jun L, Xue J (2023) Cross-border cybercrimes: preventive governance model and its development. Journal of Shanghai University (Social Sciences Edition) 40(3): 122-137.

4. Lewis J (2018) Economic impact of cybercrime-no slowing down. U.S. Center for Strategic and International Studies, Report pp: 1-28.

5. Peters A, Jordan A (2020) Countering the cyber enforcement gap: strengthening global capacity on cybercrime. Journal of National Security Law and Policy 10(487): 487-524.

6. Xiao H (2022) Dissimilation and regulation: research on criminal jurisdiction of new cross-border

7. (2022) Colonial Pipeline hack explained: Everything you need to know. crimes in cyberspace. Criminal Law Review.

8. (2022) Law on Combating Telecom and Online Fraud Passed. The National People's Congress of China.

9. (2021) This year of combating electronic fraud: more than 370,000 cases were uncovered and the number of cases continued to decline. The State Council of China.

10. (2021) Prosecutions for alleged cybercrime rose nearly 50% last year. The Supreme People's Procuratorate of the People's Republic of China.

11. Ming XL, Wenji L (2018) Analysis of criminal jurisdiction over transnational cybercrime. Journal of Soochow University (Philosophy & Social Science Edition).

12. Ireland-Piper D (2013) Prosecutions of extraterritorial criminal conduct and the abuse of rightsdoctrine. Utrecht Law Review 9(4): 68-89.

13. Boister N (2012) An introduction to transnational criminal law, In: 1st (Edn.), Oxford University Press.

14. Staiano F (2022) Transnational organized crime: challenging international law principles on state jurisdiction. Edward Elgar Publishing

15. R vs Graham Waddon (1999) Southwark Crown Court (HH Judge Hardy) 30/6/99.

16. Yanhong L (2018) On the effectiveness of criminal law in cyberspace. China Legal Science

17. Sekati PNM (2022) Assessing the effectiveness of extradition and the enforcement of extra-territorial jurisdiction in addressing transnational cybercrimes. Comparative and International Law Journal of Southern Africa 55(1).

18. Feng H (2008) Rules and practices of international juridical cooperation in criminal matters. Peking University Press.

19. (2012) Questions relating to the Obligation to Prosecute or Extradite (Belgium v Senegal). International Court of Justice.

20. Bassiouni MC (2006) Introduction to international criminal law. Law Press China.

21. The nine tasks include: defending cyberspace sovereignty, safeguarding national security, protecting critical information infrastructure, strengthening cyberculture, combating cyberterrorism and illegal crime, improving the cybergovernance system, consolidating the foundation of cybersecurity, upgrading the protection capacity of cyberspace and strengthening international cooperation in cyberspace. (2016) State Internet Information Office releases National Cyberspace Security Strategy. The Government of China.

22. (2017) China Releases Strategy for International Cooperation in Cyberspace. The Government of China.

23. "Cybersecurity" means the capabilities of, by adoption of necessary measures, preventing network attack, intrusion, interference, and destruction, illegal use of network as well as network incidents, making the network stay in a state of stable and reliable operation, and guaranteeing the integrity, confidentiality and availability of network data. Cyber Security Law of the People's Republic of China. Article 36.

24. Chunhui W (2017) Analysis of six legal systems on Cyber Security Law. Journal of Nanjing University of Posts and Telecommunications(Natural Science Edition).

25. Personal information and important data collected and produced by critical information infrastructure operators during their operations within the territory of the People's Republic of China shall be stored within China. If it is indeed necessary to provide such information and data to overseas parties due to business requirements, security assessment shall be conducted in accordance with the measures developed by the national cyberspace administration in conjunction with relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation. Cyber Security Law of the People's Republic of China. Article 33.

26. Data Security Law of the People's Republic of China.

Article 36.

27. Liming W & Xiaodong D (2021). On the highlights, characteristics and application of personal information protection law. The Jurist.

28. (2024) 44,000 suspected telecom online fraudsters in northern Myanmar handed over to us. Xinhua Net.

29. Pei W (2022) Digitalization of the extraterritorial jurisdiction of criminal justice in the cyberspace. Law Science Magazine.