WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 12
LHPPR 2024

Research on International Cooperation in Cracking down Cross-border Cyber-telecoms Fraud

Ho Ming Wong*

Department of law, Wuhan University, Wuhan, China

*Corresponding author: 2021311061186@whu.edu.cn

Abstract. Recently, the rampant criminal activities of Scam Clan in Northern Myanmar have attracted international attention. In combating such crimes, international cooperation is crucial. However, numerous challenges arise in the fight against cyber-telecoms fraud, including differences in national, difficulties in gathering criminal evidence, and inadequacy of extradition mechanisms, among others. Based on this, exploring the theoretical aspects of cross-border phone fraud crimes, reviews the current state of legal regulation both domestically and internationally, and analyzes the difficulties in cracking down cross-border cyber-telecoms fraud. Seeking to find feasible solution to these, law enforcement dilemmas by addressing the resolution of conflicts in legal regulations and enhancing extradition mechanisms. Such means can help increase the efficiency of combating cross-border telecommunications network fraud, better protect the personal and property safety of individuals, and maintain social stability and national security.

Keywords: Cross-border cyber-telecoms fraud; International cooperation; Judicial assistance; Legitimate review of the evidence; Extradition mechanisms.

1. Introduction

While the high-speed development of the era of instant information brings great convenience to human beings, it also leads to numerous criminal acts, among which phone fraud is one of the most typical. Nowadays, telecommunications fraud exhibits characteristics such as concealment, transnationality, and universality, posing a great threat to both personal and national security. It has also become one of the key crimes targeted by various countries. International cooperation is a crucial component in the fight against cyber-telecoms fraud, especially when dealing with cross-border cases. Effective International cooperation can greatly enhance the efficiency of efforts to combat cross-border cyber-telecoms fraud and help achieve desirable outcomes in the crackdown activities.

However, due to the differences in the legal system of various countries, international cooperation in cracking down on cross-border cyber-telecoms fraud is not so ideal as we might think. There are many practical problems, such as conflicts in legal regulations, challenges in evidence collection and reviewing its legality, and limitations in extradition mechanisms, among others. To improve the efficiency and proactivity in combating cross-border cyber-telecoms fraud and to maintain the harmony and stability of the international community, it is urgent and crucial for both theoretical and practical communities to deeply study the problems mentioned above. Furthermore, solutions to these conflicts and problems should be sought in practice.

2. The Theoretical Basis of Cross-border Cyber-telecoms Fraud

2.1. Background and Characteristics of Cross-border Cyber-telecoms Fraud

The rise of cross-border cyber-telecoms fraud can be traced back to the 1990s, originating in Taiwan, China. With the creation and development of telephone and mobile contact services, some law-breakers started to use this type of basic communication equipment to carry out fraudulent activities. The original methods of telecom fraud were only limited to telephone, text message, and fax because of the limitation of technology. Due to the low cost and the minimal technical threshold, this kind of fraud is still widespread today.

In recent years, with the popularization of the Internet and the continuing development of IT and Internet finance service, the methods of cyber-telecom fraud have also been improving and evolving. Besides, the traditional methods we mentioned above, telecom fraudsters started to use new communication tools such as networks, mobile terminals to implement new scams. In 2009, Taiwan and Chinese Mainland signed the Cross-Strait Agreement on Combating Crime and Mutual Legal Assistance (Assistance Agreement). Based on this, the police of cross-strait cooperated in investigating a large number of cross-strait fraud cases. Under the high pressure from the police of cross-strait, the fraud criminals moved their crime dens to other countries and the rudiment of cross-border cyber-telecoms fraud gradually took shape [1]. At the same time, with the development of economic globalization, the crime of telecommunications fraud has gradually taken the form of cross-border syndicate, taking advantage of the differences in the legal systems of various countries to find legal loopholes and carry out systematic transnational fraud activities.

Besides, due to the concealment of the Internet, cross-border cyber-telecoms fraud exhibits characteristics of spatial virtualization and concealment of its behavior. The criminals can camouflage themselves and erase their traces through technological means, which makes tracking actions much more difficult. Moreover, the target of the crime is extremely wide-ranging, spanning all ages. That means everyone is possible to become the target of the crime in an era where people heavily rely on the Internet. In terms of the location of the crime, this kind of crime demonstrates characteristic of being trans-regional and industrialized. The criminals usually set their criminal dens in other countries or regions, taking advantage of differences in legal systems to escape the punishment of the law. At the same time, other crimes such as kidnapping, human trafficking, and illegal detention have emerged in the process of committing crimes, forming a vast criminal network.

2.2. The Harm of Cross-border Cyber-telecoms Fraud

The dangers of cross-border cyber-telecoms fraud are self-evident. Whether analyzing real cases or examining film and television works, we can perceive the extremely serious harm of cross-border cyber-telecoms fraud on individuals, society, countries and even the entire international community. For victims themselves, not only is there the lost of personal property but there may also be the possibility of the destruction of their family. In addition to the loss of property, the mental and physical damage inflicted is also extremely serious. For the society and the country, it can result in the loss of workforce and unknown flow of funds, which can have an extremely negative impact on the development of social economy. For the international community, cross-border cyber-telecoms fraud will undermine the stability of the international community, trample on the dignity of the international legal system, and affect the in-depth cooperation among various countries in various political and economic aspects. All in all, it is necessary to intensify the crackdown on cross-border telecommunications network fraud.

3. The Current Status of Domestic and Foreign Practice of Cross-border Cyber-telecoms Fraud

As we all know, cross-border cyber-telecoms fraud has an extremely negative and far-reaching impact, causing very serious harm to individuals and even to entire countries and societies. In the face of increasingly rampant cross-border cyber-telecoms fraud, the international community is also constantly introducing various diversified and targeted measures to deal with it.

3.1. The Current Status of Foreign Practice of Cross-border Cyber-telecoms Fraud

Since the harm of cross-border cyber-telecoms fraud has deeply affected almost all fields of the international community, an international consensus on fighting against cross-border cyber-telecoms fraud has been formed. Most international organizations and countries have successively introduced relevant laws and regulations to crack down on cross-border cyber-telecoms fraud, so as to better protect people’s personal and property security.

3.1.1. U.N. Convention Against Transnational Organized Crime

On 15th November 2000, the United Nations promulgated the U.N. Convention Against Transnational Organized Crime (the Convention). Although countries around the world have conducted extensive theoretical research and judicial practice on transnational organized crime, the effect has not been satisfying. Not only has the momentum of organized crime not been effectively curbed, but it has also shown a transnational trend along with the "globalization process" [2]. It was in this context that "the Convention" was born. Firstly, "the Convention" clarifies the concepts of organized criminal groups and transnational crime and stipulates the principles and measures to be taken in the process of international cooperation in judicial assistance, investigation, prosecution, and the recovery of stolen goods, which provides a legal basis and institutional measures for member states to jointly combat transnational organized crime. Secondly, by definition, cross-borer cyber-telecoms fraud meets the Convention's requirements for "organized criminal groups". In addition, since the criminal acts of cross-border cyber-telecoms fraud endanger social and economic development, the Convention can play a guiding role in international cooperation in combating cross-border cyber-telecoms fraud.

3.1.2. ASEAN

Telecom fraud has always been one of the biggest obstacles to the development of Southeast Asia, especially in the Golden Triangle region. Due to geopolitical tensions and the lack of social security, the cyber security situation in Southeast Asia is becoming increasingly severe. In order to prevent and control telecommunication network fraud and safeguard people's property and personal safety, ASEAN countries have continuously improved their network technical standards and legal system construction to enhance the governance capacity of comprehensive network security. For example, in terms of network technical standards, ASEAN has successively issued documents such as the ASEAN Digital Data Governance Framework and the Key Approach to ASEAN's Cross-border Data Flow Mechanism, establishing unified data flow and technical standards [3]. In terms of legal system construction, Singapore, Thailand and other countries have also successively promulgated Cybersecurity Law. In 2023, Singapore's parliament passed "the Cybercrime Endangerment Bill" to further help it maintain the nation's cybersecurity. Besides, to enhance international cooperation, combat cross-border telecommunications cyber fraud, and better address the "unique threats posed by cybersecurity, disinformation and misinformation to defense agencies," ASEAN member states opened the Cyber Security and Information Centre of Excellence (ACICE) at Singapore's Changi Naval Base in July 2023 [4].

3.2. The Current Status of Practice of Cross-border Cyber-telecoms Fraud in China

Combined with the characteristics of cross-border telecommunication fraud cybercrime, China has implemented diversified and targeted governance measures to prevent and control cross-border cyber-telecoms fraud from multiple aspects. Among these, the legal basis for the conviction and punishment of telecommunications fraud cybercrime is mainly found in Article 266, Article 287 and Article 287/1 of Criminal Law of the People's Republic of China. In 2016, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security jointly issued the Opinions on Several Issues Concerning the Application of Law in Handling Criminal Cases such as Telecommunications Network Fraud (the Opinions on Several Issues). This document provides detailed provisions on the basis for the determination and punishment of telecommunications fraud, in particular, it increases the punishment for cross-border telecommunication network fraud crimes, and adds provisions on the punishment of related crimes. What is worth noting is that the Anti-Telecom Network Fraud Law of the People's Republic of China (the Anti-Telecom Network Fraud Law) promulgated in 2022. Anti-Telecom Network Fraud Law provides for the prevention and punishment of telecommunications network fraud from four aspects: telecommunications governance, financial governance, Internet governance, and comprehensive governance.

Besides, in terms of law enforcement, China's law enforcement agencies have adopted methods such as "breaking cards" and "cutting off flows" to cut off the capital chain and information flow of

criminals from the source, thereby better facilitating follow-up law enforcement efforts [5]. In terms of publicity, they have joined forces with multiple industries to conduct legal publicity and legal education in various forms, and launched the National Anti-Fraud Center APP to protect the personal and property safety of citizens at a technical level.

4. Analysis of the Law Enforcement Dilemma of Cross-border Cyber-telecoms Fraud

In August 2023, the police of China, Thailand, Myanmar, and Laos achieved remarkable results in a special joint operation against cross-border gambling and fraud syndicates [6]. This action not only dealt a heavy blow to the cross-border cyber-telecoms fraud group but also highlighted the determination of various countries to crack down on cross-border cyber-telecoms fraud. With the development of economic globalization and network information technology, more and more cross-border cyber-telecoms fraud groups have been established. Criminals set up criminal dens outside the country, making it more difficult to crack down on them. At present, international cooperation in combating cross-border cyber-telecoms fraud is facing many difficulties, including the following aspects.

4.1. Conflicts in Different Legal Systems

At present, the laws governing the punishment of cross-border cyber-telecoms fraud in most countries are not that perfect. For example, China's prosecution of cross-border cyber-telecoms fraud is primarily based on the Criminal Law and some judicial interpretations. Article 286 of the Criminal Law provides for the crime of fraud but does not explicitly stipulate the crime of cross-border cyber-telecoms fraud, leading to the legislative provisions lagging far behind the requirements of judicial practice. In addition, the normative documents such as the Opinions on Several Issues issued in 2016 are of a low level and have limited effectiveness; they only address the symptoms but not the root causes of combating cross-border cyber-telecoms fraud [7].

Furthermore, huge differences between different countries' legal provisions also create opportunities for criminals. For example, while Article 303, paragraph 3 of the Criminal Law clearly prohibits cross-border gambling [8] in one country, another country like Myanmar introduced the Gaming Law in 2019 to allow foreigners to open casinos and gamble within its borders. This situation can easily lead to a scenario where the gambling behavior committed by the perpetrator in their home country may constitute a crime, but not in another country. Simultaneously, the perpetrator's own country may face obstacles in prosecuting crimes committed in other countries, such as extradition. This not only dampens the enthusiasm for international cooperation in combating cross-border cyber-telecoms fraud but also allows criminals to exploit conflicts stipulated by the laws and regulations of various countries to evade their legal responsibilities.

4.2. The Collection of Evidence and The Review of Legality

One of the main characteristics of cross-border cyber-telecoms fraud crimes is that evidence mainly exists in electronic form. Compared to physical evidence, electronic evidence is more fragile, scattered, hidden, and susceptible to tampering and destruction, making the process of electronic evidence collection more complicated and challenging [9]. Additionally, since most cross-border cyber-telecoms fraud crimes primarily rely on online social platforms, electronic evidence may involve the mails, communication records, and Internet browsing histories of individuals other than the perpetrator. Therefore, the collection of electronic evidence may potentially infringe upon the privacy of others, violating the privacy regulations of the country where the actions are taken and potentially resulting in the invalidation of evidence due to the illegal acquisition method.

Moreover, as mutual legal assistance remains the primary form of international cooperation in combating crime, the procedures for investigating and collecting evidence have become more cumbersome, requiring careful scrutiny of the legality of evidence. Typically, law enforcement agencies in the country where the crime was committed will conduct relevant investigations and evidence collection activities within their own jurisdiction. After confirming the evidence, they will

collaborate with law enforcement officers from other countries to carry out arrest activities and then extradite the suspect. During this process, law enforcement officials from other countries do not possess enforcement powers within the jurisdiction of the country where the crime occurred. All actions, including investigation, evidence collection, assistance in arrest, and court testimony, must be conducted within the scope of authorized jurisdiction. Overstepping these bounds is likely to result in international disputes.

4.3. Limitations of Extradition Mechanisms

Extradition is the primary method for addressing cross-border crimes. In case of cross-border cyber-telecoms fraud, the "dual criminality rule" must be adhered to, which means extradition can only take place if both parties consider the matters to be in accordance with the laws and regulations of their respective countries [10]. However, due to the imperfection in the extradition mechanism, the extradition of perpetrators of cross-border cyber-telecoms fraud between countries is heavily influenced by their own laws. The activation of the mechanism requires that an extradition treaty has been signed between the two countries, thus imposing certain limitations. Taking China as an example, in practice, the application of extradition regulations in China is not sufficiently flexible. Additionally, due to the late start, the extradition regulations are not yet perfect. For example, in the case of Jiang Ge, even though both the victim and the criminal suspect were Chinese citizens, the jurisdiction belonged to Japan as the case occurred within its territory, and since China and Japan had not signed an extradition treaty at that time, the extradition of the criminal suspect, in this case, proved to be quilt challenging.

5. Improving Paths for International Cooperation in Cross-border Cyber-telecoms Fraud

5.1. Complementing on International Treaties on Judicial Assistance in Criminal Matters

Resolving conflicts among countries regarding laws and regulations on cross-border cyber-telecoms fraud is intimately linked to the issue of extraditing criminals. Finding ways to enhance cooperation without compromising the standards of criminalization is a challenging aspect of this research. Effective communication between countries is crucial in this regard. Firstly, countries and governments should actively promote the signing and improvement of relevant treaties on judicial assistance in criminal matters. They can also refer to the relevant provisions outlined in "the United Nations against Transnational Organized Crime", such as Article 5, which addresses the criminalization of participation in organized criminal groups [11]. Secondly, countries and governments can engage in negotiations to determine how to convict criminals without lowering the standard of guilt. This can include setting uniform penalty amounts for specific offenses. By stipulating that a certain threshold of cross-border cases must be criminalized, it helps prevent criminals from exploiting legal loopholes to evade punishment. Lastly, in judicial practice, other crimes can be used to regulate criminals involved in cross-border cyber-telecoms fraud. Since this type of crime often involves derivative offenses like kidnapping, illegal detention, and human trafficking, they can be regulated through these related crimes when necessary.

5.2. Improving the legality of evidence collection and review procedures

In the process of investigating and collecting evidence, it is necessary for both sides to enhance their sense of cooperation, timely feedback and information synchronization to each other, so as to improve the efficiency of crime fighting. Since cross-border cyber-telecoms fraud is one kind of cybercrime, we can also use the internet to fight back. Establishing of a common information exchange network and promoting the digitization of cross-border evidence documents can effectively promote the exchange of information, for example, we can build a platform for the transmission of evidence documents between the two sides. At the same time, measures such as simplifying the format requirements of documents and materials and simplifying the procedures for the transmission of

intelligence can also improve the efficiency of evidence collection, intelligence exchange, and case handling.

When considering the various provisions of each country regarding privacy protection, the level of protection can be categorized based on the sensitivity of the information, and the extent of evidence extraction can be determined accordingly. For example, data extraction that could potentially impact national security or seriously harm the interests of other individuals should strictly prohibited. It is crucial to safeguard the interests of the state, society, and the third parties, and investigators shall be required to strictly follow the principle of confidentiality, implement a confidentiality system, and impose heavy punishments for acts that leak privacy.

5.3. Optimizing the Extradition Mechanism and Introduce Alternative Mechanisms

Due to the delayed initiation of extradition regulations in China, certain limitations still exist. Therefore, this paper suggests that, firstly, the national legislature should introduce relevant interpretation measures as soon as possible to make the application of China's extradition regulations more flexible, and constantly improve the extradition treaty and add specific standards for extradition. Secondly, our government should engage in signing extradition treaties with more countries to strengthen the relative consistency of criminal law standards for cross-border cyber-telecoms fraud and increase the severity of penalties so that criminals have nowhere to escape [9].

Otherwise, due to the highly complex extradition procedures and the presence of numerous stringent conditions like "the non-extradition by death penalty" and "reciprocity principle", extraditing criminals involved in cross-border cyber-telecoms fraud has become extremely challenging. In order to further improve the efficiency of the case, other alternatives to extradition mechanisms could be found, such as the repatriation. As an informal form of international assistance, repatriation occurs mainly between two countries that have not signed an extradition treaty and can therefore be used as a complementary form of extradition.

6. Conclusion

In conclusion, there are still challenges in combating cross-border cyber-telecoms fraud in practice, highlighting the crucial role of enhancing international cooperation to boost governance efficiency and combat effectiveness. In response to the problem of conflicts in legal regulation, it is necessary to strengthen cooperation and communication between countries and improve relevant treaties to carry out subsequent judicial activities. To tackle issues related to evidence collection and legality review, establishing an information communication network, setting up a platform for exchanging evidence documents between both sides, simplifying document and material format requirements, and streamlining intelligence transmission procedures can enhance efficiency while also prioritizing the protection of citizens' privacy. Regarding challenges within the extradition mechanism, it is essential for the state to interpret, sign extradition treaties with more countries, and explore additional convenient methods as supplements to the extradition process.

Whether it involves negotiating and determining crime standards, advancing intelligence-sharing platforms and electronic evidence documentation, or signing extradition treaties and enhancing the repatriation system, while these measures may not entirely resolve the predicament of international cooperation, they can help to improve the current dilemma of international cooperation in combating cross-border telecom and internet fraud, thus improving case handling efficiency. Given the severe and extensive impact of cross-border telecom and internet fraud crimes, every country should actively engage in combating such offenses and contribute to their deterrence.

References

[1] Yang Jiayu. Research on the development process and development trend of cross-border telecommunication fraud crime. Legal System and Society, 2018, (02): 209-210+216.

[2] Zhao Bingzhi, Zhang Weike. The legislative evolution and prospect of China's punishment of organized crime: Coordination with the United Nations Convention against Transnational Organized Crime. Xuehai, 2012,(01): 179-189.

[3] Zhang Jie. International law enforcement cooperation in southeast Asia to cope with new cross border crimes. Journal of Yunnan Police Academy, 2022, (05): 95-101

[4] Liu Lei. ASEAN strengthens cybersecurity cooperation through multiple approaches. World Knowledge, 2024, (03): 32-33.

[5] Wang Zhi. Research on the Governance of Cross border Telecommunications Network Fraud Crimes. Yunnan: Yunnan University of Finance and Economics, 2024.

[6] Ministry of Public Security of the People's Republic of China. The police of China, Thailand, Myanmar and the Laos four countries initiate a special joint action to cooperate in combating gambling fraud groups. 18 Aug. 2023, Retrieved from: https://www.mps.gov.cn/n2253534/n2253535/c9159256/content.html

[7] Ma Jun. Legislative review and dilemma reflection on telecom network fraud crimes. Legal Expo, 2022, (02): 35-38.

[8] Article 303 of the Criminal Law of the People's Republic of China.

[9] Ge Zhiwen. Challenges and responses to international criminal justice assistance in transnational cybercrime. Cybersecurity Technology and Applications, 2023, (10): 145-146.

[10] Cheng Liangwen. Basic principles of international criminal judicial assistance. Chinese Journal of Law, 2002 (03): 179-181.

[11] Article 5 of the United Nations Convention against Transnational Organized Crime.