Journal of Politics and Law; Vol. 17, No. 2; 2024
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Study on International Cooperation to Address Cross-border Telecommunication Network Fraud Offence

Lan Yu[1†], Qiyan Cong[2†] & Sixin Li[3†]

[1] Law, School of Economics and Law, University of Science and Technology Liaoning, Anshan, China

[2] Architecture, Faculty of Architecture, Civil and Transportation Engineering, Beijing University of Technology, Beijing, China

[3] Law, Department of Customs Law, Shanghai Customs College, Shanghai, China

[†]These authors contributed equally to this work and share first authorship.

Correspondence: Qiyan Cong, Architecture, Faculty of Architecture, Civil and Transportation Engineering, Beijing University of Technology, Beijing 100124, China. E-mail: wangyiyouxiangcqy@163.com

Received: March 6, 2024 Accepted: May 23, 2024 Online Published: May 29, 2024

doi:10.5539/jpl.v17n2p51 URL: https://doi.org/10.5539/jpl.v17n2p51

Abstract

In recent years, under the new technological environment of the international society, cross-border telecommunication network fraud crime cases are high, and various countries are faced with difficult problems of law enforcement cooperation, such as: less channels of information exchange, difficult investigation and evidence collection, low efficiency, more obstacles to investigation and arrest cooperation, slow speed and low effectiveness of recovering stolen goods. In order to achieve effective international governance of cross-border network crimes and strengthen cooperation between China and other countries, this study is based on the collection of cross-border telecommunication network fraud crimes of international cooperation cases and literature, combined with the current situation of cross-border international cooperation in China, proposed to effectively solve the problem of cross-border telecommunication network fraud international cooperation from the prevention and governance level. In order to achieve a higher level of international cooperation and governance between countries, and continuously reduce the occurrence of cross-border telecommunication network fraud cases.

Keywords: cross-border telecommunication network fraud, network crime, international cooperation

1. Introduction

1.1 Background

In the era of information globalization, internet is like a "double-edged sword". On one hand, it promotes the sharing of resources, but on the other hand it threatens the safe development of cyberspace. The unprecedented interactivity and sociability brought by the internet provide criminals with a new mode, which is taking the network as the space to carry out criminal acts in an one-to-many, making traditional crimes enter the network space and breeding many security problems, mainly telecommunication network fraud. Meanwhile, the legal and judicial differences between countries cause telecommunication network fraud to break through the regional and national boundaries. Due to the high incidence of cross-border telecommunication network fraud, it poses a great threat to the personal safety and property safety of people all over the world as well as the social security and stable development of the country. In the face of complex and severe cross-border cybercrimes, international cooperation among countries on combating cyber-crimes has become particularly important.

1.2 Literature Review

The current research of cross-border telecommunication network fraud are as followed. From the perspective of the problems and difficulties in combating related crimes, some scholars believe that it is difficult to crack down on the whole chain, and the resistance of recovering stolen goods is greatly prominent. Some scholars believe that the differences in laws and regulations between countries and the difficulty in controlling the illegal crossing of national borders are the main difficulties. Other scholars believe that the judicial problems such as the difficult formation of evidence chain, the inconvenience of electronic evidence collection, and the difficulty of verifying criminals are more serious.

From the perspective of strategies to deal with related problems and difficulties, some scholars believe that we should strengthen the effective crackdown on related crimes from the research and development of countermeasures technology, the improvement of anti-reconnaissance paths, and the improvement of information supervision. Other scholars believe that specific management measures should be specified according to the characteristics of cross-border network telecommunication fraud. With the enhancement of the trust mechanism and cooperation consciousness among participating subjects, a good collaborative governance system will be built.

1.3 Study Purpose and Significance

Most of the previous studies on combating cross-border telecommunication fraud were aimed at various issues such as the differences in laws and regulations between countries and the judicial obstacles in investigation and collection of evidence and gave the upper and macro coping strategies. But there were few studies on international cooperation specifically aimed at combating cross-border telecommunication fraud.

In fact, work such as the cross-border evidence and electronic data forensics involved in the processing of cross-border telecommunication network fraud crime, the international joint investigation of the criminal chain all involve international cooperation issues, to provide a strong rule of law enabling multidimensional aspects such as combating and maintaining national security and the stable development of the international community.

At present, China mainly engages in international cooperation with sovereign states such as Vietnam, Cambodia and Thailand in dealing with cross-border cyber fraud crimes. Law enforcement agencies of these countries communicate with each other, exchange information, investigate and collect evidence, submit judicial procedures, pursue foreign criminal suspects in China, and conduct cross-border pursuit and repatriation abroad. In view of the rapid development of the information network, cross-border online fraud crimes are gradually showing the characteristics of geographical spread and decentralization, diversified means, strong hidden subjects, and high scientific and technical degree, which also makes the law enforcement process of international cooperation face many difficulties and challenges.

Therefore, the research on international cooperation in dealing with cross-border telecommunication network fraud crimes is of certain practical significance. This paper will analyze the specific problems in detail and put forward the corresponding solutions from the two levels of prevention and management of the problems.

2. Problems of International Cooperation in Cross-border Telecommunication Network Fraud Offence

After recent years of co-operation in the fight, the number of telecommunication fraud cases against our citizens has shown a certain downward trend, but it is still a heavily weighted crime against property, and the challenges faced by the investigating authorities are still very serious. Therefore, cross-strait police, judicial and other authorities on both sides of the Taiwan Strait to carry out joint cross-border cooperation to combat crime is an important means to effectively curb criminal activities involving each other across the Taiwan Strait. The following are some of the results of cross-border co-operation in the investigation of telecommunication network fraud cases.

Table 1. Cross-border co-operation in the investigation of telecommunication network fraud cases

Name	Time	Overview	Area	Effectiveness
The Great Wall joint operation between Chinese and Western	2016.Jan.	Setting up fraud dens in Barcelona and Madrid, Spain.	Spain, Taiwan and other places.	The operation on December 31, 2016 resulted in the arrest of more than 200 suspects, mainly from Taiwan, and the identification of a fraud amounting to more than €16 million.
The "network brush single" series of fraud cases	2018.May.	Fraud is carried out on social platforms such as QQ in the name of online shopping and swiping.	Henan, Guangdong and other provinces. Laos and other countries.	In January 2019, the working group, together with the Lao police, carried out five operations to close nine fraud dens, knocked down 11 criminal gangs, arrested a total of 191 suspects, and seized numerous tools of the trade.
Fraud, smuggling and organizing others to steal across the border	2020.Mar.	Releasing fake news in the special QQ groups to lure the investment. Causing the loss of victim funds or account anomalies by modifying the websites' background data. Only did the victims continue to recharge or pay the commission, could they unblock the account or withdraw their cash, which was regarded as ways of decoy.	Guangdong, Yunnan and other provinces. Myanmar and other countries.	In November 2021, 24 suspects were arrested, and the total amount of fraud was more than RMB 3.09 million.
Infringement of Citizens' Personal Information	2021.Feb.	Purchasing WeChat registration information on the Internet and posting advertisements for the sale of the information in WeChat groups in areas with high incidence of telecommunication network fraud outside the country and using it to commit telecommunication network fraud offence.	Fujian, Guangdong and other provinces, Laos. Myanmar and other countries	A total of 1,548 pieces of WeChat registration information were bought and 1,214 pieces were sold, resulting in an illegal profit of more than RMB 30,000 yuan.

2.1 Few Channels for Information Exchange

Suspects have set up fraud dens in Southeast Asia, North Africa and even Southern Europe, which has brought many inconveniences to our law enforcement authorities in identifying the facts of the case and arresting the suspects involved. Cross-border network fraud involves a number of countries and regions, there are differences in laws and regulations and jurisdiction itself, and the law enforcement bodies responsible for cross-border network

fraud in each country are also different, and there are few docking windows, while the lack of effective information-sharing and joint law enforcement mechanisms leads to difficulties in the exchange of information. Especially in the current situation of endless cross-border crime cases, the amount of information related to the case is extremely large and complex. Therefore, with the help of big data technology, the information sharing mechanism can be strengthened so as to broaden the information exchange and docking channels between each other in cross-border joint case handling. However, for countries lacking cross-border police databases or cloud platforms, it will create certain difficulties for cross-border joint casework. Because of the small number of docking channels and the difficulty of broadening them, the difficulty of governance is greatly increased.

2.2 Investigations and Evidence Collection Are Difficult and Inefficient

First of all, it is difficult to carry out investigations and evidence collection work. Due to international political, geographical and cultural differences, the degree of cooperation between evidence collectors and local governments and people is not high, making it more difficult to collect evidence. Regarding international politics, some countries, out of national security considerations, have to a certain extent restricted the external mobility of their data, which has led to the exclusivity of network data in their territories. Thus, not being conducive to the investigation and collection of data for cross-border cases. On the geographical level, the large spatial distance between the countries involved in the case will inevitably increase the time cost of cross-border investigation. For the cultural aspect, unlike China's extensive and detailed collection of citizens' personal information data, some countries tend to protect citizens' right to privacy and the interests of citizens' personal data. Therefore, their collection of citizens' personal data information is not complete, thus bringing inconvenience to the relevant investigation and evidence collection work. Secondly, there are legal and political obstacles to the transnational pursuit of criminal suspects, different legal systems in different countries, and imperfect extradition treaties, which make the pursuit work difficult. For example, China's extradition treaties started relatively late and developed rapidly, so its mechanism is not mature enough, coupled with the authorities are not familiar with the extradition mechanism, so the extradition mechanism has not been widely used in our country and the relevant authorities of other countries to carry out joint investigations and evidence collection work. The fight against transnational crime requires the collaboration of all countries, but at present there is a lack of effective international cooperation mechanisms, making it difficult to form synergies. For instance, due to differences in investigation and evidence-gathering procedures between countries, evidence gathered outside the country cannot be admitted because it does not comply with the provisions of the country's procedural laws, thus weakening the role of joint evidence-gathering in promoting the investigation phase of a case.

2.3 Many Obstacles to Cooperation in Investigation and Arrest

Fraudulent activities outside the country involves an extremely wide geographical area itself, including Southeast Asia, Africa, Europe and other places, coordinating the investigation of police forces and the corresponding human and material resources are more, consuming a larger cost of time. Cross-border network fraud gangs use variable fraudulent means and constantly updated, using a variety of false information, investment opportunities, betting and other means of enticement. For example, in the 509 mega cross-border telecommunication network fraud case, the fraud group lured victims to invest in virtual currencies in the website and platform they made. In the "10-18" mega series of telecommunication fraud case, the fraud group used dating software to recommend false gambling websites to lure victims. On October 19, 2023, a fraudster in WeChat disguised as an intermediary to provide part-time work. The commitment of the victim to complete the network brush single can be obtained after the corresponding rebate. Its brush single process falsely claimed that the abnormal data error, asking victims to deliver a certain amount of money to repair the loss of data only cheat the so-called repair fee ..... In addition, the fraud gangs also frequently change IP addresses through technical means, the use of high-tech means of crime, such as the use of malware, phishing sites and other means of obtaining information about the victim, and then carry out fraudulent activities. For example, the "211" large cross-border telecommunications network fraud case, fraud gangs have a strict management system, frequently changing the fraudulent APP during the crime, and gang members are using 'hammer' 'steel nail ' 'Steamed buns' 'crabs' and other nicknames, which caused great difficulties for the police in clarifying the organizational structure of the criminal gang, the division of labor, the division of roles, and the information of the members. Additionally, the criminal gangs are well organized and have a clear division of labor, with some being responsible for forging identities, some for luring, and some for transferring money. In short, the suspects' high degree of concealment, strong network anti-detection capabilities, high degree of professionalism in fraudulent behavior and strong organizational nature, all these factors have created significant obstacles to international cooperation in investigations and arrests.

2.4 Slow and Ineffective Recovery of Stolen Goods and Losses

Cross-border network fraud crime cost is low, high earnings, the criminals' financial chain, the speed of the stolen money is fast, the transaction channel is smooth, the upstream and downstream formation of a relatively complete black industrial chain makes the stolen money dissipate quickly, resulting in the tracking of the source of ambiguity, the screening procedure is cumbersome, the recovery of stolen goods is slow, and the effectiveness of the recovery of the loss is low. For example: "10.18" large cross-border telecommunication network fraud case, the domestic victims amounted to more than 1,500, a large number of people; from April 2019 to October 2020, "Caixin International" fraud criminal group defrauded a total of 196 victims. The total amount of fraud was more than RMB 27.96 million, and the amount of illegal profit was huge; between September 2021 and June 2022, Huang and 16 other criminals obtained victims' personal information by placing part-time advertisements on the Internet, and the "puller" pulled the victims into the designated WeChat group, and used the completion of the single-sheet task to issue red packets as a bait, leading the victims to register for a third-party APP and then to register for a third-party APP. Lead the victim to register a third-party APP, and then by the "speculation group" is responsible for issuing a small task red packets to fraudulent padding, "mentor" is responsible for luring the victim large amount of recharge fraud money, the entire flow of illegal funds mechanism is more complex; The "9-8" series of large-scale underground money laundering cases involved 68 underground money laundering criminal groups from Russia, Singapore and other countries and regions, as well as more than 20 provinces, autonomous regions and municipalities such as Fujian, Guangdong, Shandong, Liaoning, Hebei, Xinjiang, Jilin, Heilongjiang, Henan, etc., with many money laundering organizations, which made it difficult to verify quickly. In summary, the recovery and salvage of cross-border cyber-crime is affected by the following three factors, which make the relevant work slow and ineffective: firstly, the number of fraudsters is large, and the amount of money involved is particularly large; secondly, the funds involved flow through a number of domestic and foreign accounts, and are mixed in with other assets; and thirdly, money-laundering organizations such as illegal private banks are of the nature of shell companies, which are difficult for public security authorities to verify on a case-by-case basis within the statutory case handling in time.

3. Methods and Countermeasures

3.1 Prevention Level

3.1.1 Enhance Technical Means, Build a Diversified Protection System

China should comprehensively improve its network security protection capabilities, actively build a diversified protection system, and use advanced technical means to monitor, track and combat network fraud. Secondly, China has to strengthen the research and development of network security technology, promote security protection products, establish a sound network security risk assessment mechanism, and enhance the monitoring, early warning and combating of network fraud with the help of big data, artificial intelligence and other technologies. Thirdly, China can use firewalls to heighten encryption technology, use intrusion detection systems, continuously develop new security technologies and tools, strengthen technical supervision, protect the security of data, and form a tight line of defence in the field of network security, thereby effectively reducing the success rate of network fraud crimes. At the same time, accelerating the improvement of the network security protection system is also important. It can safeguard the security of personal information and reduce the occurrence of network fraud crimes.

Jointing cooperation with other countries to develop new technologies will be conducive to the prevention of cross-border telecommunication network fraud information to be shared. For instance, in recent years, an amount of China's citizens in Southeast Asian countries have carried out cross-border telecommunication network fraud, such cases are at a high incidence. Information technology means can be fully utilized to explore the sharing of cross-border information resources, so as to enhance the ability of reading the information of offenders and reduce the cost of justifying such cases.

3.1.2 Improvement of Relevant Domestic and Foreign Legal Systems

To adapt to the trend of transnationalization of network fraud crimes, China needs to continuously improve and implement relevant laws and regulations, and increase the strength of the fight against network fraud crimes. Till now, China has introduced the "Network Security Law of the People's Republic of China" and the "Anti-Telecommunication Network Fraud Law of the People's Republic of China", which strictly prevents and fights against network fraud, but with the development of society and the economy, the law needs to keep pace with the times. On this basis, the penalties for cyber fraud need to be further increased to raise the cost of crime and deter criminals. Tanzania enacted a dedicated "Cyber Crime Bill" in 2015, and Russia passed special legislation in July 2017 on the security of critical information infrastructure. The U.S. has established a broad voluntary sharing mechanism for cyber security threat intelligence between public and private entities within the U.S. territory around the "Cyber

Security Act" of 2015, while the European Union has introduced "critical service operators" and "digital service providers" for critical information security based on the "Cyber and Information Security Directive", which was adopted in July 2016. The advanced experience of these countries is worth learning from our country.

In the international arena, through the signing of extradition treaties with other countries and the strengthening of judicial assistance, a complete set of legal system has been gradually constructed to provide strong legal support for the fight against cross-border cyber fraud offence. Existing regional conventions against cyber-crime do not provide a solution to the "positive conflict" of jurisdiction. Jurisdictional disputes are serious problems in the fight against cross-border telecommunication network fraud offence. Extradition, repatriation, mutual legal assistance and other relevant systems need to be improved to provide a legal basis for combating transnational crime. In the face of inconsistencies in the network security-related laws and regulations of other countries, there is a need to expand the consensus on crime prevention between countries, and at the same time to improve the discourse power of China. For countries with relatively backward network security information technology, it is necessary to extend help in a timely manner.

3.1.3 Strengthen Financial Supervision, Cut off the Financial Channels of Network Fraud

China should strengthen the supervision of regulatory agencies or apply the thought of centralized supervision in the regulatory mechanism, letting the internet financial regulatory system have a more unified standard. This not only improves the internet financial trading environment, but also reduces the occurrence of fraud cases. Financial institutions and third-party payment institutions should strictly implement systems such as customer identification and suspicious transaction reporting, and effectively fulfil their anti-money laundering obligations. At the same time, they should strengthen the monitoring and analysis of suspicious funds, discover criminal clues, and report to the relevant departments in time. Putting the ex-ante risks under control and constantly innovating the supervision methods can cut off the source channels of network fraud funds while promoting economic development.

3.1.4 Strengthen Publicity and Education

China should focus on improving the network security awareness of the general public, strengthen the propaganda and education on preventing network fraud through various channels. Moreover, it’s good to improve the general public's awareness of prevention and self-protection ability, heighten their ability to identify true and false information, and remind the public to prevent network fraud. In addition, network security is actively promoted into schools and communities to reduce the occurrence of network fraud offence at source, thereby reducing the occurrence of network fraud offence. At the same time, the public is encouraged to actively participate in reporting network fraud crimes, forming a favourable atmosphere for the whole society to jointly combat network fraud.

3.2 Governance Level

Constructing a working mechanism for investigating cross-border co-operation platforms. First of all, in order to solve the difficulties of transnational cooperation, China, in the international cooperation of governance of cross-border network fraud, should improve the effectiveness of the use of the Interpol Platform, actively participate in and promote international law enforcement co-operation, and establish a bilateral or multilateral co-operation mechanism with the relevant countries to strengthen the exchange of intelligence and law enforcement co-operation. Multi-level communication and collaboration mechanisms should also be established with other countries, with which intelligence information is shared to jointly combat cross-border cyber fraud offence. By strengthening cooperation with the international community, China will promote the development of international criminal judicial cooperation mechanisms and enhance its status and influence in international law enforcement cooperation.

Sounding international judicial cooperation mechanism. On the one hand, China should actively participate in international organizations and regional cooperation frameworks, promote the development of international criminal judicial cooperation in the direction of greater closeness and efficiency, as well as benchmark the advanced practices of the international community regarding cross-border telecommunication network fraud crimes. On the other hand, China should heighten the bilateral cooperation with other countries, to establish more cooperation mechanisms in areas such as combating transnational crime, counter-terrorism and cyber security, to broaden the areas and levels of cooperation. In addition, China's soft power in the field of international law enforcement co-operation will be upgraded through the organisation of international seminars and the training of law enforcement officials.

Upgrading domestic law enforcement capabilities. Firstly, China has to improve the professional quality and operational level of the staff of law enforcement agencies, as well as strengthen training. Secondly, China has to improve law enforcement equipment and technical support, and provide law enforcement departments with the necessary investigative means and equipment. As a responsible country, China plays an important role role in international affairs. So, China’s should put more effort into judicial work and form a synergy with the relevant

countries to fight criminals while facing the cross-border telecommunication network fraud crime.

4. Conclusion

Thanks to the promotion of advanced in modern communications, the Internet and cloud technology, the pace of globalization is developing at an unprecedented rate. This not only brings great convenience to people, but also gives rise to loads of cross-border network telecommunication fraud criminal activities. Influenced by international politics, economy, culture and other factors, the fight against transnational network fraud crime still faces many challenges. Although in recent years China has successfully solved a number of transnational cyber-crime cases and cracked down on the arrogance of criminals through cooperation with other countries, it still fails to meet the demand for regular management of cross-border telecommunication network fraud crimes.

Oversease and internet are not illegal places, and cross-border cyber-crime shall be severely punished. Therefore, in order to cope with the many dilemmas of international co-operation in cross-border telecommunication network fraud crimes nowadays, China has to consider the prevention and governance level. For this type of crime, strengthening international cooperation is an effective method. At the prevention level, it is necessary to improve technical means and build a diversified protection system; improve the construction of domestic and foreign legal systems; strengthen financial supervision and cut off the financial channels of network fraud; and strengthen publicity and education. At the governance level, it is necessary to build a working mechanism for investigating cross-border co-operation platforms, improve international judicial co-operation mechanisms, and enhance domestic law enforcement capabilities, to curb the occurrence of related cases and effectively protect people's rights. All in all, this article addresses the difficulties of international cooperation in cross-border telecommunication network fraud and expects to provide ideas for the road of international cooperation in cross-border telecommunication network fraud crimes.

References

Chen, L. (2012). On our extradition legislation and practice. *Research on the Rule of Law, 8*, 97-104.

Diao, K. (2023). Deconstruction and countermeasure prospect of telecom network fraud crime. *Industry & Technology, 22*(17), 40-42.

Ding, C. (2019). Research on cross-border cooperation in investigation of telecom network fraud cases, People's Public Security University of China, vol.09, pp.77.

Gao, T. (2023). The dilemma of punishing cross-border telecom network fraud crime and its countermeasures. *People's Procuratorate, S1*, 88-91.

Ishida, M. (2013). Border economies in the Greater Mekong Subregion. *Macmillan, 31*(3), 489. https://doi.org/10.1355/ae31-3l

Li, X. M. (2024). Development and countermeasures of cross-border telecommunication network fraud crime. *Western Journal, 1*, 78-81.

Wang, Z. (2023). Research on the collaborative governance mechanism of cross-border telecom fraud under the background of network security cooperation. *Network Security Technology and Application, 9*, 148-149.

Weng, Y. Y., & Liu, Y. (2023). The dilemma and relief of criminal regulation of cross-border telecom network fraud. *People's Procuratorate, 22*, 25-28.

Wu, H. W., & Zhang, P. (2020). Current situation, controversy and future of international rules for combating cybercrime. *China Applied Law, 2*, 187-201.

Wu, S. K. (2017, December 14). International cooperation from the perspective of cybercrime governance. *Procuratorial Daily*.

Yu, Z. G., & Wu, S. C. (2018). Cyber-crime in our country development and legislative, judicial and theory in the face of the comb. *The History of Politics and Law, 1*, 59-78.

Zheng, Z. H. (2018). Reflections on challenges and countermeasures to cross-border police enforcement cooperation in the context of big data. *Public Security Journal, 3*, 77-82.

Acknowledgments

Not applicable.

Authors contributions

Lan Yu mainly completed the summary of the current situation and existing problems in the main part of the text,

and organized them. Meanwhile, Lan Yu summarized and analyzed the corresponding countermeasures. Qiyan Cong collected and organized relevant literature and data. In addition, Qiyan Cong was responsible for the writing of the "Introduction" section, as well as revising the current situation and existing problems in the main part of the first draft. Sixin Li was responsible for writing the "Abstract" and "Summary" sections, reviewing the data, and revising the Methods and Countermeasures in the first draft. Each author contributed equally to the study.

Funding

Not applicable.

Competing interests

Not applicable.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.