Proceedings of the International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/25/20230515

Feasibility Study on China-ASEAN Cooperation in the Forewarning Mechanism Against Telecom Fraud

Ge Yinzuo[1,a,*], and Wang Qiheng[2,b]

[1]School of International Law, China Foreign Affairs University, No.24 Zhanlan Guan Road, Xicheng Area, People's Republic of China
[2]School of Foreign Language, Peking University, Beijing, People's Republic of China
a. 15723635991@163.com, b. pingyi1938@163.com
**corresponding author*

Abstract: Along with the implementation of the Belt and Road Initiative and the deepening of regional police cooperation, China and ASEAN have jointly reached remarkable achievement on cyberspace security governance, whereas facing numerous new counter-cybercrime challenges at the same time, exemplified by diversified modes and high concealment. Undeniably, China and ASEAN have accumulated abundant experience through formal conferences and informal forums, but the low institutionalization of China-ASEAN cooperation has made it hard to timely and effectively respond to the protean transborder telecom frauds. Forewarning mechanism, as an innovative method to combat telecom fraud, could significantly make up for the deficiency under the current China-ASEAN cooperative system, while enriching the Belt and Road cooperation Initiative, raising the efficiency of controlling cybercrimes, exploiting the advantage of Chinese "Internet+" strategy.

Keywords: China-ASEAN, cyberspace security governance, forewarning system, telecom fraud

1. Introduction

Along with the implementation of the Belt and Road Initiative and the deepening of regional police cooperation, China and ASEAN (Association of Southeast Asian Nations) have jointly reached remarkable achievement on cyberspace security governance, whereas facing numerous new counter-cybercrime challenges at the same time. Taking combating telecom fraud as an example, it requires massive expense and complicated procedure to make any breakthrough and gets even more costly and challenging when this happens transnationally. Hereby, this paper will demonstrate the brief discussion on the establishment of China-ASEAN forewarning system against telecom fraud.

Information era flourishing and advancing, the quick metabolism of the Internet world has made it a hotbed for breeding all kinds of illegal behaviours. Telecom fraud, as a novel fraudulent means, is gradually appearing to people's eyes, with 438 million Chinese having already get bombarded with scam messages, crime of telecom fraud accounting for about 20% of national criminal cases. According to the Law of the People's Republic of China on Anti-Telecom and Network Fraud, telecom and network fraud (for short, telecom fraud), refers to the use of telecommunication network technology under the aim of illegal possession, defrauding public and private property

DOI: 10.54254/2753-7048/25/20230515

through remote, non-contact and other ways.

Telecom fraud is characterized by the quick renovation of the modus operandi and the wide scope of the infringement. [1] Currently, the vast majority of criminals who commit fraud against China mainland are concentrated in Southeast Asia, including many ASEAN member states, especially Myanmar and Thailand. The biggest difficulty for Chinese public security organ to investigate these cases is that most of the involved websites and accounts are normally set overseas, and thus, it is extremely challenging for Chinese authority to provide help or replevy loss for people when their legitimate rights and economic interests are violated by lawbreaking telecom fraudsters. At present, the detection rate of telecom fraud is at an exceedingly low level while unfortunately fraudsters are also actively creating crime techniques, such as money laundering through multiple channels, to get more untraceable. Therefore, under the existing framework, it is of urgency to turn the prior attention to crime prevention, which could hopefully cut down the happening rate of the telecom fraud. Strengthening the construction of the forewarning mechanism against telecom fraud may be one of the most effective ways to guarantee the property security and legal rights of the citizens in both China and ASEAN member states. [2]

When Chinese government impose stricter policies, attempting to completely remove local fraudster gangs, some lawbreakers steal into neighbouring countries like Thailand, Myanmar and Laos to continue their telecom fraud crime. The powerlessness of local government and the disorder of social environment catalyse the growth of telecom frauds, drug trafficking and organ trades. The collusion between grassroot governments and criminal gangs has made it a persistent disease in the border region. Unless this disease solved, the campaign against telecom fraud will never ends. [3]

2. Inspection on the Defects of Telecom Fraud Combating under the Traditional Cooperation Framework

Cyberspace is a shared site for the humankind, with its development prospect jointly controlled by all the countries of this world. [4] Thus, inarguably, all the countries ought to enhance communication, enlarge consensus and deepen cooperation and further contribute for the cyberspace community with a shared future. [5] Traditionally speaking, there exists ASEAN Regional Forum, China-ASEAN Police Science Forum, China-ASEAN Ministerial Meeting on Transnational Crime, combinedly forming the cooperative framework of combating telecom fraud. [6] Nevertheless, even though an unenforceable institutional arrangement has already been reached among authorities of ASEAN member states after years of trying and exploring, it is nowhere near the extent of introducing a widely acknowledged convention that could act as a law document in the territory of all ASEAN members. Obviously, the full respect to national independence and state sovereignty is highly in line with the ASEAN way, but it is as well apparent that the capability of combating transnational cybercrime is severely insufficient with formalized documents and weak execution. [7] Out to their history of colonization, ASEAN member states has an innate fear and vigilance to all superpowers, inevitably making any supersovereign cooperation impossible, not to mention the counter-cybercrime cooperation might involve largescale transborder arrests.

3. Contents of China-ASEAN Cooperation on the Forewarning Mechanism Against Telecom Fraud

It has been defined by the academic community that the prewarning mechanism refers to the working mechanism that issues an alarm in advance before the economic crimes actually happens, [8] so as to prevent the occurrence of loss. [9] At present, the prewarning mechanism that China has already perfectly established is the data forewarning (monitoring and analysing users' behaviour through technical means like data analysis and artificial intelligence to timely detect potential fraud

DOI: 10.54254/2753-7048/25/20230515

and send warning signals) and multilevel anti-fraud centre forewarning (constructing a firewall to intercept or specially mark all the suspicious telephone calls). Forewarning mechanism against telecom fraud, as an advance management, has its main significance of strangling criminal acts in the cradle, relieving the pressure of grassroots police, and further maximizing social benefits with the smallest number of police force. Most importantly, this could significantly avoid most problems caused by the immature mechanism of transborder enforcement when China and ASEAN have to face together after the appearance of fraud crimes. Meanwhile, forewarning messages, naturally as nice broadcast with high social educational value, could stress the importance of Internet security among nearly all people, no matter nation, gender or age. The enrichment and popularization of the forewarning mechanism against telecom fraud is a powerful approach to raise the awareness of people's identification and prevention, safeguard people's vital interests and further promote the construction of stable and harmonious societies in both China and ASEAN member states.

The forewarning mechanism require all walks of life involved in telecom fraud to participate in the prevention and supervision in advance, especially Internet enterprises, post corporations and telecommunication industries. Telecom fraud contains a series of behaviour chains, where relevant supervisory department are responsible to detect the signals and control the situation at the very first time in the process of crime implementing or even terminate the crime procedure during the preparation period after accurate detection and prediction. [10] In many judicial practices, telecom frauds are highly targeted. The wrongdoers can obtain the victims' privacies through various channels so the departments that possess large amount of detailed personal information and organizational information, such as delivery and post, must shoulder the obligation of protecting data security. In most ASEAN member states like Thailand and Malaysia, unlike China mostly controlling relevant industries through national power, setting strict and compulsive rules for private sectors is also an indispensable step.

Noticeably, monitoring private messages and phone calls is nearly of necessity for the telecom fraud supervision, whereas this kind behaviour, long regarded as a violation of the human rights by Western mainstream, is highly disapproved by quite a few ASEAN member states. Hence, it is a trend to expand the utilization of artificial intelligence in information screening because unemotional machines will only focus on the keywords or codes related to telecom frauds with no motive to collect other privacies like identity codes, sexual orientation, or political stances. Furthermore, it will be even more fruitful if China and ASEAN could cooperatively supervise the international long-distance calls or devices in roaming service. [11]

Until now, this forewarning mechanism has already made some achievement in the practice in China. China has concluded its intelligence in combating telecom fraud into "Four Specialties and Two Resultant Forces" (Four Specialties refer to special research, special teams, special investigation and special equipment; Two Resultant Forces refers to grasping the internal resultant force and integrating the external resultant force). [12] Fact has proved that this theory is resultful. According to the statistics, a total of 232000 fraud dens have been destroyed by public security organ nationwide with 1.95 million suspects arrested. By the end of November 2022, 391000 telecom fraud cases had been solved nationwide, rising 5.7% year on year; number of suspects arrested increased by 64.4% year on year, amount of property loss caused by telecom fraud decreased by 1.3% year on year; the number of cased filed decreased by 17.3% year on year. [13] [14] Delightful results have been achieved in cracking down telecom fraud, achieving the goal of "Two Increases and Two Decreases", thanks to the change of thoughts from remedy afterward to anticipate, detect and active strike. [15]

Preventive legislation is as well a crucial part of the forewarning mechanism. Law of the People's Republic of China on Anti-Telecom and Network Fraud, as a typical example of preventive legislation, is generally taken as an experimental product of "small incision legislation",

DOI: 10.54254/2753-7048/25/20230515

where laws are published responding to the most urgent social phenomena, leaving some unimportant or undiscussed parts uninvolved, so as to shorten the legislative cycle and timely address key concerns. In contemporary society, capricious and manifold telecom frauds are emerging endlessly, and thus it is a must to promulgate a targeted law to deal with the frequent telecom frauds. The biggest highlight of this law is that it belongs to preventive legislation, emphasizing the strengthening of punishment against telecom fraud crimes, and further deterring the rampant telecom fraud gangs. The legislative success in China has evidentially demonstrated the feasibility to curb telecom frauds, providing the ASEAN member states with advanced models and Chinese experience. Notwithstanding telecom fraud has already been listed illegal in most ASEAN member states according to the local laws, a law targeted at telecom fraud, composed of both internationally acknowledged basic parts and nationally differentiated clauses could be supremely progressive for the whole counter-cybercrime campaign.

4. The Value of the Forewarning Mechanism Against Telecom Fraud under China-ASEAN Cooperative Framework

4.1. Improve the Cooperation Efficiency of Combating Telecom Frauds

ASEAN emphasizes the inviolability of the sovereignty, pursues absolute equality among countries, adheres to the principles of non-interference in each other's internal affairs and does not seek to establish a binding supranational authority. The ASEAN way, with the principle of unanimity as the core, can best safeguard the interests of all member states, reflect the common will shared by all ASEAN members and facilitate the implementation of the resolutions jointly made in ASEAN conferences. However, the ASEAN way also determines that in the context of diversification, the efficiency block is nearly unavoidable. As a matter of fact, it is precisely because of this absolute equality and absolute equivalence of dialogue mechanism that ASEAN countries lack the main guidance, coupled with the loss of confidence mechanism in recent years, which makes it particularly difficult for ASEAN to come up with a unified response to specific problems. [16]

Nevertheless, as long as a systematic resolution is concluded, the operation efficiency could dramatically improve. 2011 Mekong River Massacre as an example, the joint special operation among Thailand, Myanmar, Laos and China on this case was a complete success, with all the offenders extradited to China for trial and executed according to Chinese law. Under the negotiation of Chinese authority, police from various countries around Golden Triangle Region broke through several impossibilities without precedent, achieving one of the most successful cases of transborder police cooperation at that time. Currently, China and ASEAN are not only deepening trade cooperation but also dispatching liaison police officers to each other for police communication to facilitate transborder law enforcement. China and ASEAN, each having advantages, for shared benefits, are bound to strengthen their partnership despite the existing territorial dispute and market competition. China is responsible to offer the ASEAN member states Chinese intelligence accumulated in deduction and practice on cybercrime governance while fully respecting the option of the recipient countries, while it is suggested for ASEAN member states to absorb Chinese advanced concept on "Four Specialties and Two Resultant Forces" and further localize the extraneous theory to better utilize for themselves. Finally, only with China selflessly sharing its experience and drawing the blueprint for further action, ASEAN actively participating in the international forewarning mechanism against telecom fraud, could Southeast Asia curb the rampantness of cybercriminals and purify the world Internet environment. [17]

4.2. Enrich the Belt and Road Initiative

China has long been devoted to the construction of a community of shared future for the mankind in

DOI: 10.54254/2753-7048/25/20230515

economic development, conflict coordination and climate actions; ASEAN as well, is actively promoting the integration of the Pan-Southeast-Asia. Therefore, predictably, considering the overall policy of both sides, China and ASEAN share a strong conceptual consensus on cyberspace cooperation. The Belt and Road Initiative, as an important dialogue channel between China and ASEAN, is rich in connotation, broad in scope and mostly depoliticized in general cooperation. The practice of forewarning mechanism against telecom fraud can be displayed as an added part for the Belt and Road Initiative, so that it is much easier to reach the consensus among the contracting parties than starting a brand-new mode. [18]

Besides, as Belt and Road Initiative is nothing a political or military alliance, the criticism of the forewarning mechanism for politicizing the cybercrime governance could be basically prevented. Deeper enriching the Belt and Road Initiative to Internet field can help China and ASEAN to exchange their experience of developing online economy and better and stabilize the outcome of cyberspace governance.

4.3. Advance the Internet+ Strategy

China and ASEAN have long history and deep foundation in Internet cooperation. China-ASEAN digital ministerial conference is formerly China-ASEAN Telecommunication Minister Conference initially launched in 2006. Since 2000, in 10+1 leader summits, China have put forward initiatives in the field of information communication for 23 years, which are recognized and endorsed by ASEAN, proposing numerous documents and initiatives, inter alia, “Holding China-ASEAN Seminar on Information Communication” (Fourth 10+1 Leader Sumit, 2000), “Training 500 ASEAN information communication technology and management personnel for ASEAN countries in five years” (Sixth East Asian Leader Summit, 2002), Memorandum of Understanding on Information Communication between People’s Republic of China and Association of Southeast Asian Nations (Seventh East Asian Leader Summit, 2003), Memorandum of Understanding on Jointly Advancing the Construction of Information Superhighway in the Greater Mekong Subregion (8th East Asia Leaders' Summit, 2004). [19] China, long keeping nice relationship with ASEAN, is capable to extend advanced Internet security management experience to the cooperation mechanism with ASEAN, and promote the advancement of the Internet security technology at the same time. With plenty of experience and loads of collected data, China is expected to share its abundant case handling experience in counter-fraud management and the output of the research on fraud verbal tricks. Moreover, the police liaison officers stationed in ASEAN should also play a greater role, regularly hold local exchanges and symposiums under the fundamental purpose of promoting regional police cooperation, the behavioural guidance of “Four Specialties and Two Resultant Forces” and the ultimate goal of establishing forewarning mechanism against telecom fraud. Hereby, China is obligated to act as a leader of the cybersecurity governance in Southeast Asia as well as a major power with sense of historical mission in the global cybersecurity campaign.

5. Conclusion

The cooperation mechanism between the procuratorial organs of China and ASEAN member states in combating transnational cybercrimes still needs to be further perfected. Currently speaking, the intelligence exchange between each country’s procuratorial organs is still not unimpeded, with the cooperation channel severely limited. [20] In view of such situations, the advanced governance to establish a complete forewarning mechanism against telecom fraud is the most efficient and most beneficial but least costly and least problematic.

DOI: 10.54254/2753-7048/25/20230515

References

[1] *Zhang Wei, (2015)Research on Telecom Fraud Cases, Journal of Hebei Public Security Police Vocational College, 2015.*

[2] *Mahuya Ghosh, (2010)Telecoms Fraud , Computer Fraud & Security, Jula, 14-17.*

[3] *Telecom Fraud, (2019)A Growing Concern in Asia , Commercial Crime International, Auga, 6.*

[4] *Xi Jinping, (2015)Five Proposals on Jointly Building a Cyberspace Community with Shared Future. Retrieved from https://china.huanqiu.com/article/9CaKrnJSmtA.*

[5] *Xi Jinping, (2015)Five Proposals on Jointly Building a Cyberspace Community with Shared Future. Retrieved from https://china.huanqiu.com/article/9CaKrnJSmtA.*

[6] *Chen Weiqiang, (2018)Investigation of China-ASEAN Police Cooperation---From Basis, Form, Challenge to Perfection, Treatise on Criminal Law.*

[7] *Yang Xinmin, Zeng Fanjing, (2021)Study on China ASEAN International Cooperation on Cybercrime Governance, Journal of Hunan Police College, 1, 63.*

[8] *Li Haijun, Yang Ying, (2011)Application of Forewarning Mechanism in Ideological and Political Education for College Students, Science Consultation.*

[9] *Liu Chuanlei, Zhao Yue, (2011) Research on Construction of Forewarning Mechanism of Ideological and Political Education for College Students, Science and Technology Information.*

[10] *Cai Xian, (2014) Discussion on the Limitation of Punishment Scope for Preparatory Crime in China---Based on the Crime Types, Criminal Law Review.*

[11] *Keith A. Pequeno, Real-time Fraud Detection: Telecom's Next Big Step, Telecommunications Americas, 1997 5th, 59-60.*

[12] *Combating Fraud with the Entire Society, (2022) Guarding Peace of the Whole Nation, Wiping out Telecom Fraud with heavy punches. Retrieved from https://www.anqing.gov.cn/xwxx/zwyw/2003334141.html.*

[13] *Li Jianjun, Xiong Jun, (2020)Investigation Countermeasures of Telecom Fraud Cases related to Epidemic Situation, Journal of Jiangxi Police College.*

[14] *Central Government of the People's Republic of China, (2023)Public Security Departments Have Achieved Remarkable Results in Cracking down on Telecom Fraud Crimes. Retrieved from https://www.gov.cn/xinwen/2023-01/02/content_5734607.htm.*

[15] *Cui Jipeng, (2022)Wang Shunbing, Research on Technological Countermeasures against Telecom Frauds, Journal of Shandong Police College.*

[16] *Zhao Shaoqun, (2012) ASEAN Decision Mechanism from the Perspective of the ASEAN Charter, Legal Forum, 5, 150.*

[17] *Ali Abdullah Wibisono, (2017)ASEAN-China Security Relations: Traditional and Non-Traditional Aspects.*

[18] *Yang Xinmin, Zeng Fanjing, (2021)Study on China-ASEAN International Cooperation Cybercrime Governance , Journal of Hunan Police College, 1, 63.*

[19] *Ministry of Industry and Information Technology of the People's Republic of China, (2008)China-ASEAN (10+1) Cooperation. Retrieved from https://www.miit.gov.cn/xwdt/dwjl/art/2020/art_0afe567d524743358c265fd1008887c3.html.*

[20] *Wang Junxiang, (2008)Analysis on the Cooperation Mechanism on Combating Transborder Crimes, Hebei Law Study.*