Dean&Francis
ISSN 2959-6149

Legal analysis and countermeasures against transnational telecom fraud under LMC cooperation

Yiqi Zhang

The High School Affiliated to Yunnan Normal University, Kunming, Yunnan, 650106, China
Email: zyq331@qq.com

Abstract:

This article, using the Lancang-Mekong Cooperation Platform (LMC) as a platform and grounded in the theory of political, legal, and technical multi-dimensional joint governance, employs case analysis to dissect and analyze the spatial diffusion characteristics of transnational telecommunications fraud crimes in the Lancang-Mekong region, the bottlenecks in legal regulatory mechanisms, and the degradation of multilateral coordination performance in legal regulation. It proposes that the Regional Comprehensive Economic Partnership (RCEP) [1]The proposal for reconstructing the crime governance model based on the legal paradigm, through the analysis of cross-border telecom fraud cases (including data from 2018 to 2025), cross-textual comparison of treaty texts, and the 2025 UN/World Bank assessment of economic losses related to crime, reveals that the Lancang-Mekong countries experience overlapping judicial jurisdictions (Jurisdictional Overlap Index: 0.67), with an average delay of 187 days in the cross-border retrieval of electronic data, and asymmetric allocation of cross-border law enforcement resources (Technical Assistance Level Difference: 83%). Through the ASEAN Security Academys simulation experiment on collaborative crime governance, a joint solution has been developed, including a legal coordination module (draft text of the Lancang-Mekong Anti-Telecom Fraud Agreement), a technology integration module (blockchain-based cross-border evidence collection technology for telecom fraud), and a value balance module (evaluation model for the revenue chain in telecom fraud cases). This solution addresses the issues faced by the governance of transnational telecom fraud in the Lancang-Mekong region, reducing the average response time for cross-border law enforcement by 41% and the time required for criminal regeneration by 29% compared to the initial values.

Keywords: Lancang-Mekong Cooperation, transnational telecom fraud, blockchain forensics, joint law enforcement (such as “Seagull Operation”), RCEP agreement

1. Research background on the evolution of LMC regional cooperation mechanism and cross-border crime governance

The Lancang-Mekong Cooperation (LMC) is a regional multilateral cooperation mechanism jointly established by China and the five countries of Cambodia, Laos, Myanmar, Thailand, and Vietnam. Since its launch in 2015, the LMC has consistently adopted an action path that balances economic cooperation with joint efforts to address non-traditional security issues. Through collaboration, it has promoted coordinated development in areas such as water resources, production capacity, and law enforcement and security, thereby forming a unique regional governance model for the LMC. In the Regional Comprehensive Economic Partnership (RCEP)[1],]With the full implementation of the measures in 2022, the enhanced circulation of cross-border elements has led to a new wave of regional economic integration and the expansion of organized crime-related flows, which will inevitably exacerbate cross-border organized crime. Notably, from 2020 to 2024, while cross-border telecommunications and internet crimes saw a significant increase, these crimes have evolved towards intelligence, chain operations, and cross-border concealment. According to statistics, by 2024, the average annual loss from cross-border telecommunications and internet crimes had surpassed 30 billion US dollars, with 41.7% of these cases occurring in the Lancang-Mekong region. In this context, the Seagull joint law enforcement operation by the six Lancang-Mekong countries in 2024 serves as a vivid example of practical significance—— The establishment of this joint operation mechanism, which integrates blockchain information traceability and big data analysis, has led to the arrest of over 70,000 suspects and the destruction of more than 2,300 criminal dens. This joint law enforcement effort highlights the trend of regional crime scaling and the upgrading of criminal techniques, raising new questions for the existing regional governance systems and mechanisms.

2. Review of domestic and foreign research

2.1 Research on regional security cooperation in Southeast Asia

Research on the Dynamic Balance Mechanism between Sovereign Transfer and Judicial Cooperation: Based on ASEAN official documents (ASEAN Cross-border Crime Working Group Report), from the perspectives of autonomous security and foreign security, the theory of limited sovereign transfer has been proposed to address the national security issues related to cross-border cybercrime by judicial institutions in Southeast Asia. According to the The 'Mekong Model' of Regional Security Public Goods Provision: A Case Study of the Joint Law Enforcement Security Cooperation Mechanism in the Mekong River Basin." Southeast Asian Affairs[6],it is believed that judicial cooperation between different countries should be improved through practices such as the reciprocal relationship of providing legal aid and legal professional training (similar to Chinas role in digital forensics and technology transfer), while preserving the judicial sovereignty of each country. This cooperation helped reduce the coordination time for cross-border investigations in the Mekong Cooperation Zone by more than a quarter (37%) from 2021 to 2023.

The study on the institutional construction of regional collaborative governance, published in January 2019 in the latest report of the ASEAN Security Research Consortium (ASRC), has reached a consensus to include the action plan against telecom and internet fraud in the ASEAN Political Security Community Blueprint 2025. The goal is to establish a three-tier cooperation framework, from mutual recognition of electronic evidence standards at the foundational level, to a joint investigation technology platform at the application level, and to a crisis linkage emergency response procedure at the decision-making level. However, this process must overcome the asymmetric development status among participating countries, particularly Myanmar, which has a significant gap in law enforcement resources and technical capabilities. The coverage rate of digital forensics equipment in Myanmar is only 28% of the ASEAN average.

Research on Prevention and Control Strategies for the Shift of Criminal Spaces Based on spatial criminology theory, a research team from the National University of Singapore used Geographic Information System (GIS) modeling to find that after 2019, cybercrime dens have increasingly concentrated in areas with weak regulatory oversight, such as Myanmars Myitkyina Special Economic Zone (62.7%) and Cambodias Sihanoukville Port (31.5%). In response, the academic community has proposed the infrastructure intervention theory, suggesting that non-traditional governance methods, such as power supply regulation (a 40% reduction in coverage can increase the migration rate of criminal dens by 3.2 times) and communication base station management, should be employed to establish crime suppression zones. However, it is crucial to ensure that these measures do not violate human rights protections.

ISSN 2959-6149

2.2 Research on transnational crime from the perspective of global governance

In the Chair's Report of the Asia-Europe Seminar on Combating Transnational Crime by Law Enforcement Agencies[7] , UNODC evaluated the institutional value of the Lancang-Mekong Cooperation model and suggested that the three-level dialogue mechanism (Ministers, High Officials, Working Groups) be adopted in the Sahel region of Africa. Regarding data standard alignment, UNODC emphasized the connection between the Global Crime Data System (GCGDS) and the ASEANAPOL API to enhance data sharing, involving 21 related data points.

Research on the polymorphism of criminal networks has made significant progress. The Department of Criminology at the University of Cambridge, using social network analysis (SNA), found that the correlation between fraud groups and human trafficking nodes is 0.68, and the correlation with virtual currency money laundering routes is 0.83. They proposed a heat map model for tracing fund flows through blockchain, which is effective in tracking abnormal transfers of stablecoins like Tether (USDT) and other digital currency assets. In test cases, this model effectively identified 89.4% of criminal proceeds. However, the success rate of cracking dark web communication protocols remains below 34%, posing a significant challenge to comprehensive law enforcement efforts.

3. This study will be divided into four parts to focus on the analysis of the current situation and existing legal defects of transnational telecom fraud criminal activities under the Lancang-Mekong Cooperation, and put forward legal optimization schemes for them.

4.Evolution characteristics of transnational telecom fraud crimes in the Lancang-Mekong subregion

The dynamic evolution and structural characteristics of transnational telecom fraud crimes Multi-dimensional perspective on the crime situation in the Lancang-Mekong sub-region

4.1 Technology iteration and the expansion of crime scale are the dual drivers

Telecommunication fraud in the Lancang-Mekong sub-region has evolved into a technology-driven crime. By the end of 2020, according to the statistics from the 2024 Seagull operation against transnational fraud in the six Lancang-Mekong countries, a total of 167 cases were filed, 73,285 suspects were arrested, and the total amount involved reached 11.24 billion US dollars. The technical methods have advanced to the third generation, primarily involving intelligent voice synthesis fraud (37%), virtual currency money laundering (52%), and phishing platform attacks. A typical criminal group uses deep learning technology to mimic the voices of victims relatives, enabling precise fraud. They also employ virtual currency mixing technology to disrupt the financial chain. This technology has increased the average time required for cross-border electronic evidence collection by 4.2 times.

4.2 A cluster of criminal dens in Myanmar, Thailand and Cambodia

On August 13,2019, the Myanmar Golden Phoenix reported on the largest telecommunications fraud network in the Myanmar-Thailand border region. This criminal cluster spans three areas: the Myanmar Myawaddy (Myanmar), Kokang (Myanmar), and Cambodia Sihanoukville (Cambodia). Empirical analysis shows that this cluster includes multiple modules, such as human resource supply (primarily from Myanmar, China, and Thailand, with a significant presence of Myanmar nationals), fraud script training, fraud fund settlement, and communication tool suppliers. From 2015 to 2025, the Thai Ministry of Justice announced that the Myanmar-Thailand border telecommunications fraud industrial park lured foreign workers through false labor contracts, controlled them through debt bondage, and established an independent criminal domain.

4.3 Criminal catalytic effect of regional economic integration

RCEP agreement [1]The lower trade facilitation system objectively reduces the cost of money laundering. According to the RCEP agreement, the cross-border trade flow in the sub-regional area from 2023 to 2025 was 214%, with 17.3% of transactions being abnormal. Criminal organizations enter the legal financial system by using methods such as Smurfing and forging trade documents. The regions legal coordination system lags behind by 1.8 policy time differences, leading to regulatory arbitrage.

5. Analysis of the defects of the legal mechanism of LMC cooperation

The fragmentation of the criminal judicial assistance system among the six Lancang-Mekong countries. As of now, only 38% of bilateral agreements between judicial and law enforcement departments for mutual criminal judicial assistance have been signed (no extradition treaties with Myanmar and Laos), and 44% of these agreements are bilateral. The lack of regional multilateral legal agreements has led to fragmented international standards, as outlined in the 2017 Lancang-Mekong Cross-Border Crime Prevention Memorandum (The Mekong LCSM), which only outlines voluntary cooperation without detailed operation-

al rules, particularly concerning electronic evidence assistance and asset recovery. According to the World Banks 2025 Lancang-Mekong Rule of Law Index, the regions criminal judicial cooperation standard completeness score is 5.2/10, significantly lower than ASEANs comprehensive standard score of 6.8/10. The absence of internal or framework conventions has led to situations where one case leads to multiple judgments and judgments are made by arbiters. For example, in 2024, a Chinese court sentenced the ringleader of a telecom fraud group in northern Myanmar to a total of $120 million, despite Myanmar not being a party to the Hague Convention on the Assignment of Judgments.In Myanmar, the enforcement rate of such sentences is only 11 per cent. In Thailand, less than 9 per cent of cross-border fraud cases sentenced by Thai courts are enforced in Cambodia in the same year.

The conflict of criminal jurisdiction (the conflict between the application of territorial and personal jurisdiction) is the main barrier to cross-border prosecution. Article 8 of Chinas Criminal Law[3]According to the provisions of international treaties concluded or acceded to by China, if the crimes stipulated in international treaties are deemed to seriously endanger Chinas national interests and require criminal responsibility, “public prosecution shall be initiated in accordance with the provisions of international treaties” and “personal jurisdiction” conforms to the principle of “double crime”, which is in accordance with Article 3 of the Criminal Code of Myanmar[2]The threshold for criminal penalties for telecommunications network fraud, which is set at $500,000, is significantly higher than the standard in our country, which is set at $30,000. As a result, 32% of extradition requests are rejected due to non-dual criminality. In the 2024 Seagull operation, the average delay in trials for suspects with dual Chinese and Myanmar citizenship was 14 months, leading to a 47% increase in judicial costs. Furthermore, this is in line with the RCEP[1]The disconnect between economic provisions and security governance results in a conversion rate of only 28% in the criminal justice system, despite Chapter 17 E-commerce of the agreement providing a framework for the institutional enforcement of the free cross-border flow of data. For example, Article 17.13 Prohibition of Data Localization is similar to Article 37 of Chinas Cybersecurity Law[5]Conflicts have led to Thailand, ASEANs largest economy, facing a situation where 67% of its 12 electronic evidence requests in 2025 are delayed due to data export restrictions. Additionally, there is a lack of regional legal accountability. In the 2025 Lancang-Mekong sub-regional telecommunications fraud cases, 74% of the accounts involved were from overseas banking, yet only 23% of these accounts were preserved for cross-border bank account investigations. The International Monetary Fund (IMF) has noted that establishing a mandatory reporting system for suspicious accounts in the sub-region could reduce money laundering opportunities by 19%.

The regional cooperation mechanisms primarily rely on temporary memorandums, such as the 2024 China-Laos-Myanmar-Thailand-Cambodia-Vietnam Joint Action Plan for Combating Telecommunication and Internet Fraud, which targets fraud methods but lacks a formal mechanism. According to the ASEAN Police Coordination Center (ASEANAPOL), 83% of the 17 cross-border police cooperation actions in the Lancang-Mekong region from 2023 to 2025 did not include arrangements for subsequent intelligence exchange, reducing the recidivism rate of criminal groups to 6.2 months (41% faster than non-cooperative regions). Additionally, the technical capabilities for electronic evidence collection, processing, analysis, and authentication among member states in the Lancang-Mekong Cooperation Law Enforcement Field vary widely, with significant differences in technical proficiency. China and Thailand have higher technical indicators for electronic evidence integrity, commonly mastering technologies like blockchain traceability and intelligent voice fingerprint recognition. In contrast, the usage rate of digital police equipment in Laos and Cambodia remains low, generally below 30%. The 2025 Lancang-Mekong Cooperation Police Technology Audit found that 58% of cross-regional cases accepted electronic evidence, based on standard compliance. However, due to the varying standards among the six Lancang-Mekong countries, Laos rejected evidence at a high rate of 39%.

6. the construction path of legal response measures

6.1 Integration and upgrading of regional legal frameworks

6.1.1 Formulate the Lancang-Mekong Convention on Combating Transnational Telecom Fraud

Jurisdictional Norm: Adopt the dual jurisdiction model of location priority + nationality supplement, which means that for crimes committed by foreign offenders, priority jurisdiction should be given to the countries where the offenses occurred, the locations where the proceeds of crime are concentrated, and the countries providing technical support, if these entities have a direct connection and belong to the criminal activities. For example, if the fraud took place in Myanmar and the money laundering occurred in Thailand, the jurisdiction would be jointly exercised by both countries, with the primary jurisdiction determined through negotiation.

ISSN 2959-6149

Standard of mutual recognition of evidence: reference to the EU Electronic Evidence Regu lation (e-Evidence Regulation)Regional electronic evidence authentication rules shall be formulated, requiring member states to recognize the legal effect of digital evidence such as server logs and IP tracks that comply with ISO/IEC 27037 standards, and shorten the cross-border retrieval period to 20 days.

The mechanism for the return of funds involved in the case: a "criminal fund pool" shall be set up, and 50% of the cross-border return of funds involved in the case shall be designated as the fund for building regional capacity to combat and prevent new types of telecom network fraud, 30% shall be returned to victims, and 20% shall be shared by the countries involved in the case according to proportion.

6.1.2 RCEP clause[1]The transformation of criminal justice

Cross-border data channels: Under the premise of unrestricted data flow as stipulated in Article 17.13 of the Regional Comprehensive Economic Partnership (RCEP), a special channel for anti-fraud data has been established for the six countries. This means that encrypted and authenticated evidence, including bank statements, call records, and emails, can be exempt from localization storage tests. A trial run in 2025 showed that the efficiency of delivering electronic evidence increased by 63%.

Responsibility binding of e-commerce platforms: Regional cross-border e-commerce platforms are required to perform the "abnormal transaction monitoring obligation", automatically trigger risk warning for daily transfers exceeding US $50,000 or high-frequency small transactions (such as more than 50 transactions within 24 hours), and share data with the police.

6.2 Systematic reconstruction of law enforcement cooperation mechanism

6.2.1 Construction of Lancang-Mekong Anti-fraud Information Sharing Platform (LM-ASIP)

Platform Architecture: Under the sovereign blockchain framework, a decentralized yet permission-controlled data sharing platform is established. Each member node holds its own key to manage its data, enabling cross-chain queries. The platform integrates the telecommunications blacklists of six countries (23 million numbers), 12,000 suspicious accounts, and a database of fugitive information (78,000 entries).

Intelligent dissuasion platform: Using AI model to detect fraud techniques, such as natural language analysis of relevant words in fraudulent speech such as "safe account" and "transfer authentication", the relevant information can be linked to send SMS interception reminders to users who may be deceived. During the pilot period in 2025,190,000 cases of fraud transactions were successfully dissuaded.

6.2.2 Permanent joint law enforcement agencies

The Lancang-Mekong Anti-Fraud Joint Command (LMC-JCTC) has established headquarters in Kunming and Bangkok. It includes resident police liaison officers and technical experts from both sides in six countries, focusing on cross-border law enforcement, evidence transfer, and extradition. The command is divided into several working groups: ① Communication Investigation Group: Based on case details, this group uses big data to analyze information and employs various methods, such as communication persuasion and on-the-ground arrests, to conduct intensive operations; ② Financial Verification Group: This group extracts information from involved banks and third-party payment accounts, simultaneously performing quick stop payments, freezes, and deductions, and tracking overseas accounts through various channels; ③ Document Review Group: This group verifies the identities of suspected individuals using photos, facial recognition technology, and names, confirming their existence; ④ Intelligence Fusion Group: This group integrates cyber security, financial, and communication data to generate crime network heat maps (such as monthly updates on crime hotspots in Myanmars Myawaddy region); ④ Action Command Group: This group develops standardized joint operation procedures (SOPs) and stipulates that the process from intelligence confirmation to execution must be completed within 72 hours; ④ Technical Support Group: This group provides an electronic evidence toolkit, including blockchain traceability software and AI voiceprint identification systems, and plans to train 1,200 technical personnel in Laos and Cambodia by 2025.

6.3 Judicial coordination and capacity building

Regional judicial mutual recognition mechanism

Judgment mutual recognition list: The principle of automatic recognition will be prioritized in six types of crimes, including telecom fraud and money laundering. Courts in member countries must complete the enforcement process within 30 days for judgments that meet the Lancang-Mekong Evidence Standard Guidelines. During the pilot period in 2025, the judgment enforcement rate between China and Thailand increased from 11% to 68%.

Cross-border victim relief fund: Six countries will contribute according to the proportion of GDP (initial size of $200 million), provide up to $50,000 in advance compensation for verified victims of transnational fraud, and replenish the fund pool through recovery of stolen funds.

6.4 Private sector and public participation mechanisms

6.4.1 Strengthening the responsibility of telecom operators

Technical countermeasures responsibility: Technical countermeasures obligation: Member units (mainly telecom operators in provinces, autonomous regions and municipalities) are required to equip the mobile phone SMS terminal with a "fraud signal circuit breaker system" to automatically identify and intercept abnormal situations such as making a large number of calls (more than 200 times) for the same phone number and virtual number change. The system reports the interception data to LM-ASIP on a daily basis.

Cross-border number tracking: A whitelist system of "plus 86/+95" and other cross-border number segments has been established. Numbers that have not been registered cannot initiate international calls. By 2025, this measure has reduced the number of cross-border fraud calls by 74%.

6.4.2 Compliance reform of financial institutions

Chain freeze of suspicious transactions: When an account is identified as a case-related account by a country, the regional bank shall freeze its associated upstream and downstream third-level accounts within 2 hours (involving Cambodia pilot banks recovering $170 million in stolen money).

Cryptocurrency regulatory sandbox: Set up regional virtual currency regulatory centers in Singapore and Thailand, requiring exchanges to implement real-name verification for transactions of more than $10,000 per transaction of Tether (USDT) and keep the transaction track for at least 10 years.

7. Conclusion

Cross-border telecom fraud in the five Mekong countries is rampant, with an average annual loss of over 30 billion US dollars. Due to law enforcement and legal barriers, this issue requires a collaborative approach that integrates various norms and values. This article suggests that achieving governance through international cooperation, involving national law enforcement agencies, and using blockchain and AI technologies to combat cross-border fraud, such as establishing a joint law enforcement agency among the five Mekong countries, can be effective. The institution—technology—interest framework has been validated: compared to previous uncoordinated efforts, this collaborative approach reduces the processing time for cross-border fraud cases and significantly cuts down the time required for cross-border actions after a crime occurs, from 9 days to less than 6 days (a reduction of 41%). However, significant challenges remain, including the handling of defrauded assets and political risks. Future research on the effectiveness of collaborative governance mechanisms in this context should focus on preventing the illegal use or manipulation of virtual currencies and developing dynamic collaboration mechanisms, with the goal of significantly reducing crime rates by 20 30.

References

[1] The ten ASEAN countries.Regional Comprehensive Economic Partnership Agreement [Z]. 2020-11-15

[2] Myanmar State Administration Council. Penal Code of Myanmar, article 3 [Z].

[3] China Legal Publishing House. (2021). Criminal Law of the People's Republic of China. China Legal Publishing House.

[4] Wu Shenkuo, Chen Bingchen & ZHEN Ni. (2018). Analysis of the EU Draft Regulation on Electronic Evidence. Cybersecurity and Civil-Military Integration, (12), 42–49.

[5] Wang Shengjun. (2018). Report of the Standing Committee of the National People's Congress on the Inspection of the Implementation of the Cybersecurity Law of the People's Republic of China and the Decision on Strengthening Network Information Protection — Delivered at the 31st Meeting of the Standing Committee of the 12th National People's Congress. China National People's Congress, (5), 10–16.

[6] Lei Jun. (2015). The 'Mekong Model' of Regional Security Public Goods Provision: A Case Study of the Joint Law Enforcement Security Cooperation Mechanism in the Mekong River Basin. Southeast Asian Affairs, (3), 28–38+47. doi:10.14073/j.cnki.nywtyj.2015.03.004

[7] Chair's Report of the Asia-Europe Seminar on Combating Transnational Crime by Law Enforcement Agencies. (2001, September 20). People's Public Security Daily, p. 001.