Collaborative Organization of Transnational Cyber Fraud Crimes: A Focus on Deepfake Scams

Aijia He[1], Wenyi Li[2] and Haoyu Wu[3,*]
[1]*Tianjin University of Finance and Economics, Tianjin, China*
[2]*Southwest University of Political Science and Law, Chongqing, China*
[3]*Renmin University of China, Beijing, China*

Keywords: Collaborative Organization, Transnational Cyber Fraud Crimes, Deepfake Scams.

Abstract: The abuse of deepfake technology has propelled transnational cyber fraud towards a more technologically driven and cross-border collaborative form. This paper focuses on the reconfiguration of the transnational fraud criminal ecosystem by deepfake technology and its governance challenges. By employing a comprehensive approach that includes literature review, legal hermeneutics analysis, and empirical research methods , the paper systematically explores the technical characteristics, scale of harm, and governance dilemmas associated with deepfake technology. The study reveals that deepfakes have broken through biometric identification barriers, exacerbating the autonomy and precision of fraud schemes. Meanwhile, international cooperation efforts are constrained by jurisdictional conflicts, legal disparities, and difficulties in cross-border evidence collection. In light of these findings, the paper proposes governance recommendations such as restructuring international treaties, optimizing jurisdictional coordination, and establishing a global information-sharing mechanism. It highlights China's key role in aiding international fraud governance and rule-setting.

1 INTRODUCTION

With the deep application of artificial intelligence technology, transnational cyber fraud crimes have broken through geographical limitations, forming a new type of criminal ecosystem driven by technology and cross-border collaboration. Compared with traditional models, the core difference lies in the breakthrough of biometric barriers by technological tools (such as deep fakes and voice cloning), and the evolution of the criminal process towards autonomy and precision (Zhang, 2018). Criminal organizations build transnational criminal networks through technologies such as cloud database sharing and real-time translation tools, leading to a doubling of difficulties in cross-border electronic evidence collection and judicial cooperation (Qiao, 2018).

The current cross-border network technology-based scams primarily manifest in four categories of technical crimes: Firstly, video forgery crimes, such as the fake video in March 2022 that purportedly showed Ukrainian President Volodymyr Zelenskyy "announcing surrender" which spread on Facebook (Wu, 2023). Secondly, audio forgery crimes, where voice cloning is used to mimic specific individuals' voice commands for transfers; thirdly, image forgery crimes, exemplified by the 2023 Guangzhou Metro incident where a woman was falsely portrayed using "AI one-click undressing"; and fourthly, text forgery crimes, which involve generating false financial information through natural language processing to induce transfers.

This article focuses on cross-border scams driven by deepfake technology, primarily based on three reasons: Firstly, there has been a significant increase in the penetration rate of the technology. Deepfake technology, which started in 2017 with an anonymous user u/deepfakes on Reddit synthesizing celebrity pornographic videos, has seen a surge in related research papers reaching 1,207 by 2019. The open-source nature of the technology has accelerated its global spread (Jia, 2021). Secondly, the harm caused by individual cases has dramatically increased. In 2018, a forged video of Obama attacking Trump received 2 million views and 50,000 likes, directly impacting international political security (Long,

He, A., Li, W. and Wu, H.
Collaborative Organization of Transnational Cyber Fraud Crimes: A Focus on Deepfake Scams.
DOI: 10.5220/0014293000004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 5-12
ISBN: 978-989-758-785-6

2019). Thirdly, the technology chain has matured. The emergence of tools like FakeApp and Faceswap has greatly facilitated the creation of false identities for carrying out scams (Long, 2024).

As such, deepfake technology has evolved beyond being a mere tool for criminal activities; it has become a strategic variable driving the evolution of the transnational fraud ecosystem. The strong correlation between its technical characteristics and the scale of harm it causes makes it a central research subject in the governance of cybercrime in the digital age. Based on this, this article will systematically analyze how deepfake technology is reshaping the operational paradigms and governance challenges of transnational fraud, and use this analysis as a theoretical basis to optimize the transnational cooperation organizations for combating cyber fraud crimes.

2 LITERATURE REVIEW

The rapid advancement of internet technology has led to a surge in transnational cyber fraud, with the emergence of deepfake technology presenting novel challenges to global legal frameworks and international cooperation. Scholars have investigated deepfake technology from various perspectives, including its underlying principles, application risks, legal regulation, and the jurisdictional aspects of transnational cybercrime. These studies have provided in-depth analyses of transnational cyber fraud, offering a rich theoretical foundation and practical guidance for establishing international cyber cooperation mechanisms.

Researchers have detailed the generation principles of deepfake technology, highlighting its use of autoencoders, generative adversarial networks, and other deep learning tools to create highly realistic facial and voice forgeries. The proliferation of open-source tools and commercial software has significantly lowered the barrier to entry for this technology. Despite advancements in deepfake detection technologies, significant challenges remain, such as dependence on specific datasets and generation algorithms, as well as insufficient detection capabilities for unknown types of manipulation (Li, 2021). This indicates that the misuse of deepfake technology poses substantial harm to society, while existing countermeasures are demonstrably limited, necessitating more effective solutions.

Another study delves into the role of deepfake videos in the context of the Russia-Ukraine conflict, illustrating the technology's function in the manipulation of public opinion (He et al., 2023). The research highlights the targeted nature of these videos, both in terms of their release timing and thematic content, which are often designed to counter each other. This underscores the detrimental impact of deepfake technology on public perception and international relations in transnational scenarios, emphasizing the urgency of addressing this issue.

Scholars have also examined jurisdictional conflicts in transnational cybercrime, noting that the characteristics of such crimes—their transnational nature, virtuality, and scale—challenge traditional jurisdictional rules based on territorial sovereignty. Conflicts frequently arise between territorial and personal jurisdiction in cases of transnational cyber fraud. To resolve these issues, the international community should advocate for priority jurisdiction rules, and nations must actively engage in criminal justice cooperation. China should also reconstruct its territorial jurisdiction rules and establish international collaboration mechanisms, which is crucial for resolving jurisdictional challenges in transnational cyber fraud (Su, 2020).

Scholarly analysis has also been conducted on the current state, collaborative approaches, constraints, and potential solutions concerning cross-strait telecommunications fraud. While the incidence of such crimes has decreased, significant cases persist, with increasingly sophisticated techniques and a growing professionalization of criminal activities. Despite existing cooperation between the two sides, challenges remain, including incomplete cooperation agreements and significant differences in judicial systems (Wang, 2021). Therefore, it is imperative to further refine cooperation agreements, innovate police cooperation models, resolve conflicts in criminal jurisdiction, and establish joint asset recovery mechanisms to enhance the collaborative fight against transnational cybercrime.

In conclusion, deepfake technology and transnational cyber fraud are closely linked and pose significant threats, yet current countermeasures are demonstrably insufficient. Future research on the organizational aspects of combating transnational cyber fraud should further explore the construction of more effective international cooperation frameworks. This involves, on the one hand, defining the responsibilities of cooperative organizations in terms of technical prevention, information sharing, and the

development of detection technologies, considering the characteristics and harms of deepfake technology. On the other hand, it necessitates clarifying the role of cooperative organizations in coordinating national jurisdictions and promoting judicial cooperation, based on solutions to jurisdictional conflicts in transnational cybercrime, thereby providing stronger support for combating transnational cyber fraud.

3 RESEARCH QUESTIONS

3.1 Empirical Analysis of Existing International Cooperation Organizations for the Governance of Transnational Cyber Fraud

3.1.1 The Current Situation of Transnational Cyber Fraud Involving Deepfake Technology

In recent years, deepfake technology, as a new technology based on deep learning and Generative Adversarial Networks (GAN) models, has been able to create highly realistic forgeries of videos, audio, and images. It can even replace one person's facial features and voice with those of another scene or character, thereby producing effects that are indistinguishable from reality (Jasserand,2024). This technology first gained attention through social media platforms in 2017 and quickly sparked widespread interest. It has not only altered the credibility of traditional media and personal information but also brought serious legal and ethical challenges to the fields of entertainment, politics, and personal privacy (He, 2023).

With the advancement of technology, the application scope of deepfakes is continuously expanding, and its role in fraudulent activities is becoming increasingly significant. According to a report released by Dutch company Deeptrace, as of September 2019, the number of deepfake videos globally had reached 15,000, a stark contrast to the less than 8,000 videos in December 2018, indicating a rapid growth in the application of this technology. Especially in 2017, when the anonymous online user u/deepfakes began uploading and widely disseminating related content, it enabled non-professionals to quickly produce fake videos with the help of open-source code (He, 2023). The proliferation of this technology not only poses a threat to the entertainment industry and the reputation of public figures but is also being exploited by criminals for financial fraud, political propaganda, and the spread of misinformation on social networks, gradually evolving into a new trouble that impacts cybersecurity and social order.

In this context, the three case examples presented in Table 1 vividly illustrate the application of deepfake technology in fraudulent activities and the challenges in its governance.

Table 1. The case summary.

Case Name	Time	Summary	Challenges in Governance
vZAO software incident	August 2019	China's Momo company has launched a "one-click face swap" application, which has sparked controversy due to excessive requests for personal information and data leakage risks in its user agreement. The technology could potentially be used for creating fake videos for scams. Balancing privacy protection with technological innovation is challenging; legal regulation lags behind, and there is a gap in preventing the misuse of technology.	Balancing privacy protection with technological innovation is challenging; legal supervision lags behind, and there is a gap in preventing the misuse of technology.
Ukraine-Russia conflict fake video	March 2022	Using GAN technology to forge videos of Ukrainian and Russian leaders making speeches, spreading misinformation through social media, and misleading the	The spread of misinformation is rapid and its source is difficult to trace; there is a lack of international joint governance

Case Name	Time	Summary	Challenges in Governance
		global public and policymakers' understanding of the conflict.	mechanisms, and cross-border cooperation is complex.
Deepfake pornographic video	Since 2017	Anonymous users utilize deepfake technology to replace the faces of celebrities in pornographic videos for the purpose of blackmail or illegal profit, with the content being disseminated across borders through the dark web.	Regulating anonymous networks (such as the dark web) is challenging; international law enforcement cooperation is inefficient, and technical evidence collection is complex.

These cases demonstrate that scammers, leveraging deepfake technology, significantly enhance their deceptive effectiveness by generating highly realistic audio and video content through deep learning and GANs, in conjunction with social engineering tactics and rapid dissemination channels such as social media. The target groups are both broad and specific: the general public is susceptible due to insufficient technical discernment, while high-value targets such as celebrities and public figures are prioritized due to their social status and public attention. Simultaneously, scammers often exploit the anonymity of the internet and the open-source nature of technology for international collaboration, thereby multiplying the difficulty of tracking and governance efforts.

Specifically, the challenges in governance mainly manifest in the following aspects: Firstly, the high level of realism in deepfake content makes it difficult for ordinary users and traditional detection methods to distinguish between truth and falsehood (Yang, 2024). Even when informed beforehand about the possibility of forgery, a large number of people may still misjudge its authenticity. Secondly, the current legal system lacks specific punitive measures for deepfake scams, and the differences in laws among countries and inadequate law enforcement cooperation further exacerbate the difficulty of governance. Additionally, the rapid dissemination of false information on the internet and social media means that once published, misinformation spreads quickly. For example, false videos about the Russia-Ukraine conflict have had a significant impact on global public opinion in a short time, making it difficult for regulatory authorities to respond promptly. Finally, the public's insufficient understanding of deepfake technology provides opportunities for fraudulent activities, and the risk of future scams may further increase (He, 2023).

3.1.2 Current Cooperation Organizations in Governing Transnational Cyber Fraud Crimes

The current international community's cooperation organizations in governing transnational cybercrimes primarily include INTERPOL and Europol. INTERPOL provides member states with information sharing and technical support through global police communication services, crime intelligence centers, and specialized databases, and assists in the pursuit of transnational criminals through Red Notices and Blue Notices. However, its operational effectiveness is limited by factors such as voluntary cooperation from member states, insufficient funding, and trust crises (Yang, 2024). Europol effectively combats transnational organized crime and cybercrime through information sharing systems, joint operations, and professional support, but its operations also face challenges such as resource disparities among member states, inconsistent legal systems, and political interference (Shang, 2023). Bilateral and multilateral cooperation demonstrates high efficiency in coordinating judicial resources and clarifying jurisdiction, but differences in legal systems, conflicts of national interests, and the imperfection of international criminal judicial assistance mechanisms limit its practical effects.

Overall, although these cooperation organizations have achieved certain results in combating transnational cybercrimes, further improvement in governance effectiveness is still needed by strengthening member state collaboration, improving the international legal framework, and promoting the formulation of global conventions.

3.1.3 Challenges for Cooperation Organizations Against Transnational Cyber Fraud

Jurisdictional Conflict. A primary challenge for cooperation organizations in combating transnational cyber fraud is jurisdictional conflict. This conflict manifests primarily as overlaps between national territorial jurisdictions, intersections between territorial and personal jurisdictions, and contradictions between protective jurisdiction and territorial jurisdiction. Territorial jurisdictional conflicts are particularly prominent in cyber fraud, as the location of the crime's consequences may involve multiple countries. The widespread adoption of broad territorial jurisdictional standards by various nations complicates jurisdictional claims. Although scholars have proposed limiting the scope of territorial jurisdiction by increasing the connecting factors for determining the crime's location or by referencing the "minimum contacts"，these conflicts remain difficult to fully resolve in practice. Furthermore, conflicts between territorial and personal jurisdiction are common in cyber fraud, especially when perpetrators refuse to return to their home countries. While criminal justice cooperation through extradition and repatriation can partially alleviate these conflicts, differences in substantive laws among countries still provide opportunities for perpetrators to evade legal responsibility. Protective jurisdiction, although significant in combating cybercrimes that endanger national security from abroad, has its role weakened by its intersection with territorial jurisdiction, and the coordination effects of the reasonableness principle are also relatively limited (Su, 2020).

Structural Misalignment Dilemma in Cybercrime Legislation. The structural misalignment in cybercrime legislation exacerbates the challenges in governing transnational cyber fraud. Despite the increasing transnational nature of cybercrimes, the international community has yet to establish a unified global convention. Existing regional treaties, such as the Budapest Convention, are limited by their membership scope and high entry barriers, failing to meet global demands. Some countries advocate for utilizing the United Nations Convention against Transnational Organized Crime, but its provisions are insufficient to address the specific characteristics of cybercrimes. Countries like China and Russia have called for the formulation of a global convention within the UN framework, but this has been resisted by some signatories of the Budapest Convention, leading to increased fragmentation of rules. Simultaneously, the United States, through unilateral actions like the CLOUD Act, attempts to establish a "network" for cross-border electronic evidence retrieval, further intensifying the inconsistencies in regulations. Although the UN has prioritized combating cybercrime, negotiations for a global convention are progressing slowly, and international cooperation in cybercrime governance still faces the challenge of structural misalignment in legislation (Wu, 2020).

Challenges in the Collection and Conversion of Cross-Border Evidence. First, the international judicial assistance mechanism suffers from low efficiency. Taking the "Zhang Kaimin Telecommunication Fraud Case" as an example, although Kenya transferred physical evidence to China, the extraction and identification of electronic evidence was time-consuming, increasing the risk of data tampering or loss. Furthermore, China has only signed bilateral judicial assistance treaties with 86 countries, which have limited coverage, and some treaty contents are not perfect, making it difficult to carry out effective cooperation in countries without treaties. Complex multi-agency coordination and lengthy procedures further delay case investigation, forming an "inverted U-shaped" efficiency bottleneck.

Second, the role conflict of network service providers. As shown in the "Gao's Shared Bicycle Accident Case," enterprises need to cooperate with law enforcement while also bearing the obligation of protecting user data. Due to the lack of clear legal norms, enterprises often weigh compliance risks and respond passively, even refusing to provide key evidence. This collaborative dilemma not only delays the progress of the investigation but may also lead to the inability to solve the case due to the lack of evidence.

Finally, unilateral cross-border evidence collection presents conflicts between sovereignty and privacy. In the "Hu Zijia Online Gambling Case," Chinese police were deadlocked because they could not directly obtain data from overseas servers. Although unilateral evidence collection is efficient, it may infringe on the network sovereignty of other countries and excessively collect irrelevant personal data, violating the principle of proportionality. For example, when evidence is obtained across borders through technical means, it is easy to involve the privacy of third parties other than the suspects,

triggering legal disputes (Chen, 2023).

The Dilemma Between Intelligence Sharing and Data Privacy Protection. In the governance of transnational cyber fraud, striking a balance between intelligence sharing and data privacy protection presents a significant challenge. Intelligence sharing is crucial for combating transnational cyber fraud; efficient information exchange enables law enforcement agencies to more accurately identify, track, and combat criminal activities. However, data privacy protection is equally important, especially in cross-border data flows, where personal privacy and data security face considerable risks. Existing mechanisms, such as the European Union's General Data Protection Regulation (GDPR), China's Cybersecurity Law, and India's Personal Data Protection Bill, attempt to balance intelligence sharing and privacy protection through data access controls, encryption technologies, and legal constraints. Nevertheless, these mechanisms still face serious challenges. Differences in legal systems, privacy protection standards, and technical capabilities among countries make it difficult to fully reconcile the conflicts between privacy and security in cross-border data flows. For example, some countries, based on national security or law enforcement needs, require access to data from other countries, which may conflict with the privacy protection laws of the data source country. Furthermore, technical vulnerabilities and the risk of cyberattacks exacerbate the dilemma of data security and privacy protection. Therefore, despite the achievements of existing mechanisms, further optimization of intelligence sharing mechanisms is needed through enhanced international cooperation, unified data protection standards, and improved technical security to achieve more effective governance of transnational cyber fraud (Wang, 2020).

3.2 Optimization of Cooperative Organization of Transnational Fraud Governance

3.2.1 Push for International Treaties, Legislative Systems, and Optimized Jurisdiction

Under the framework of the United Nations, international cooperation organizations should actively promote countries to reach consensus on the governance of cybercrimes, formulate a Convention on the Jurisdiction of Transnational Cybercrimes, fully take into account the interests and needs of different countries, balance the differences between developed and developing countries, lower the threshold for accession like the Budapest Convention, and expand the scope of application of the Convention. The international community should jointly resist unilateral actions, advocate bilateral cooperation and regional law enforcement, set up transnational joint investigation coordination centers, achieve efficient transfer of jurisdiction through regional mutual legal assistance agreements, strengthen coordination of legislation on cyber crimes, and strengthen the construction and refinement of extradition treaties and treaties on criminal judicial cooperation.

Secondly, efforts should be made to optimize jurisdiction on the basis of the United Nations Convention against Transnational Organized Crime. Countries should consult together at the international level to formulate unified, clear and more operational jurisdiction standards, mainly based on the principle of limited expansion of territorial jurisdiction, and apply the principle of jurisdiction of ownership and protection respectively for different transnational cyber fraud crimes, supplemented by the principle of priority admissibility (Wang&Liu, 2024).When a number of countries claim territorial jurisdiction, they should adopt the double standard of "place of main crime + place of material damage result" to reduce the uncertainty of law application. At the same time, they can learn from the asset recovery mechanism of the United Nations Convention against Corruption, establish a system of sharing the proceeds of cross-border crimes, and solve the practical contradiction between protective jurisdiction and territorial jurisdiction.

3.2.2 Innovate Cross-Border Forensics Models and Strengthen Technology Empowerment

First of all, big data policing is the foundation of modern development. China can use big data technology to analyze and mine criminal clues, build a "blockchain + smart contract" electronic evidence storage system, and solve the problem of easy tampering of electronic data. Second, establish a fast track for cross-border forensics, formulate cross-border emergency forensics rules, enable a "green channel" for cases involving major public security,

and establish a judicial big data analysis center to use AI technology to automatically convert forms of evidence in different jurisdictions, such as converting "hearsay evidence" in the common law system into "written testimony" in the civil law system. At the same time, China can provide technical support in transnational cybercrimes, share technical tools and databases related to cybercrime governance with other countries, develop new cloud control, and carry out regional cooperation by relying on computers, the Internet and cloud computing. China can also provide its self-developed network monitoring software and malicious code analysis tools to countries in need. To help them improve their ability to monitor and analyze cyber crimes, and promote a more effective governance mechanism for transnational cyber fraud crimes.

3.2.3 Establish a Privacy-Focused Intel Sharing Mech to Build a Secure Data Ecology

In terms of cross-border cooperation, the strategy of sharing threat intelligence is at the core of enhancing cooperation. Real-time information sharing enables countries and organizations to detect and respond to cyber threats more effectively. Platforms such as the European Union's Cybersecurity Agency (ENISA) and the US Cybersecurity and Infrastructure Security Agency (CISA) have demonstrated the value of collective intelligence-sharing mechanisms in reducing risk (Qudus, 2025). China can set up regional data security alliances to build a global data governance community that balances security and efficiency. At the same time, China can publicize its experience and propositions on cybercrime governance by holding international conferences and participating in international forums, encourage cooperation among countries on the basis of equality and mutual trust, and promote the establishment of a fair and reasonable international cybercrime governance system.

4 CONCLUSION

Through a systematic analysis of the application of Deepfake technology in transnational cyber fraud and its governance challenges, this study reveals the key role of deepfake technology in promoting the ecological upgrading of transnational fraud crime. The study found that the abuse of deepfake technology has evolved from a single criminal tool to a strategic variable driving the upgrade of transnational fraud ecology, and the strong correlation between its technical characteristics and the scale of harm makes it difficult for traditional legal framework and governance measures to effectively deal with it. The governance of transnational cyber fraud crimes faces multiple challenges, including jurisdictional conflicts, differences in legal systems, difficulties in cross-border forensics, and the balance between intelligence sharing and data privacy protection. Although international cooperation organizations such as Interpol and Europol have achieved some success in combating transnational cybercrimes, their operational effectiveness is still limited by factors such as voluntary cooperation among member states and the disunity of legal systems. This paper puts forward governance suggestions such as reconstructing international treaties, optimizing jurisdiction, strengthening cooperation among international organizations, and building information sharing mechanisms, and emphasizes China's positive role in promoting the Belt and Road Initiative, participating in the formulation of international rules on cybercrime governance, and providing technical assistance.

However, this study also has some limitations, such as the data source mainly relies on public literature and cases, and lacks first-hand empirical data; The legal analysis is limited by the differences in the legal systems of different countries, and it is difficult to fully cover the application of law in transnational cases; in addition, deep counterfeiting technology is developing rapidly, and this paper may not be able to fully cover the latest technological progress and criminal methods. Future studies should strengthen the collection of empirical data, deepen the comparative analysis of transnational laws, and pay close attention to the technological frontier to propose more forward-looking governance strategies.

AUTHORS CONTRIBUTION

All the authors contributed equally and their names were listed in alphabetical order.

REFERENCES

Chen, Y. 2024. Research on E-discovery of cross-border cybercrimes. *Science of Law Journal* 3(7): 1-3.

He, K., et al. 2023a. Cognitive Rashomon effect fabrication: A case study of deepfake in the Russia-Ukraine conflict. *News World* 1: 88-96.

He, K., et al. 2023b. Abuse and governance of deepfake technology. *Computer Science and Technology* 39: 123-130.

Jasserand, C. 2024. Deceptive deepfakes: Is the law coping with AI-altered representations of ourselves? 2024 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE: 1-4.

Jia, Z.F. 2021a. Legal risks and regulatory responses to deepfake technology under the Civil Code perspective. *Journal of Northeast Agricultural University (Social Science Edition)* 1: 71-78.

Jia, Z.F. 2021b. Deepfake technology and its development trends. *Network Security Technology & Application* 10: 55-61.

Jiang, Y. 2021. The orientation and limits of criminal regulation on AI deepfake technology risks. *Chinese Criminal Science* 9: 104.

Lawal, Q. 2025. Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *International Journal of Science and Research Archive* 14(1): 8.

Li, X.R., et al. 2021. A survey on deepfake and detection technologies. *Journal of Software* 32(2): 496-518.

Long, J. 2024. Legal risk prevention of AI deepfake technology. *Rule of Law Society* 3: 71.

Long, K., et al. 2019. Challenges and countermeasures of deepfake to national security. *Information Security and Communications Privacy* 10: 22.

Qiao, S.L. 2018. On law enforcement cooperation in the governance of telecom network fraud crimes. *Journal of Shandong Police College*5: 87.

Shang, F.J., et al.2023. Operational mechanisms, characteristics, and implications of Europol. *Police Education*12: 73-74.

Su, Y. 2020. Jurisdictional conflicts and solutions in transnational cybercrimes. East China University of Political Science and Law: 33-68.

Wang, N. 2020. International legal issues in cross-border data retrieval under the U.S. CLOUD Act from the perspective of cyber sovereignty. Wuhan University: 50-52.

Wang, X.W. 2021. Cross-strait cooperation in combating transnational telecom fraud crimes. *Journal of People's Public Security University of China (Social Sciences Edition)* 37(2): 71-78.

Wang, Y.Q. & Liu, H.Q. 2024. Difficulties and countermeasures in cross-border policing cooperation against telecom network fraud crimes. *Modern Business Trade Industry* 45(1): 184-186.

Wu, H.W. & Zhang, P. 2020. Current status, disputes, and future of international rules against cybercrime. *China Journal of Applied Jurisprudence* 2: 188-190.

Wu, X.D., et al. 2023. Analysis and governance of new crimes involving deepfake technology. *Journal of Political Science and Law* 6: 13.

Yang, L.Z. 2024. Strategies of INTERPOL in combating cross-border telecom network fraud crimes. *Regional Governance* (18): 13-14.

Zhang, S.P. 2018. Big data and cross-border governance of telecom network fraud. *China Legal Science* 11: 45