УДК 343.9:004.738.5

Юй Хуэйцзюань

Магистр

Казахский национальный университет

Almaty, Kazakh

МЕХАНИЗМЫ ПРАВОВОГО СОТРУДНИЧЕСТВА МЕЖДУ КИТАЕМ И КАЗАХСТАНОМ В БОРЬБЕ С ТРАНСНАЦИОНАЛЬНОЙ КИБЕРПРЕСТУПНОСТЬЮ

Аннотации: В данной статье рассматриваются правовые механизмы сотрудничества между Китаем и Казахстаном в борьбе с транснациональной киберпреступностью. В статье анализируется правовая основа сотрудничества между двумя сторонами, включая международные конвенции, двусторонние договоры и внутреннее законодательство, а также подробно рассматриваются ключевые элементы сотрудничества, такие как обмен разведданными, совместные расследования, взаимная правовая помощь и наращивание потенциала. Несмотря на значительный прогресс в борьбе с киберпреступностью, обе страны по-прежнему сталкиваются с такими препятствиями, как правовые различия, технологические проблемы и политические факторы. В связи с этим в статье предлагаются рекомендации по укреплению правовой координации, углублению технического сотрудничества и расширению международного взаимодействия в целях дальнейшего совершенствования механизма сотрудничества для противодействия развивающимся киберугрозам.

Ключевые слова: Транснациональная Киберпреступность, Китайско-Казахстанское Сотрудничество, Правовая Гармонизация, Обмен Разведданными, Кибербезопасность

Yu Huijuan

Master

Kazakh National University

Almaty, Kazakh

LEGAL COOPERATION MECHANISMS BETWEEN CHINA AND KAZAKHSTAN IN COMBATING TRANSNATIONAL CYBERCRIME

Abstracts: This article discusses the legal cooperation mechanisms between China and Kazakhstan in combating transnational cybercrime. The article analyzes the legal basis for cooperation between the two sides, including international conventions, bilateral treaties and domestic legislation, and elaborates on the key elements of cooperation, such as intelligence sharing, joint investigations, mutual legal assistance and capacity-building. Despite significant progress in combating cybercrime, the two countries still face obstacles such as legal differences, technological challenges and political factors. In this regard, the article puts forward recommendations to strengthen legal coordination, deepen technical cooperation and expand international collaboration in order to further improve the cooperation mechanism to cope with evolving cyber threats.

Keywords: Transnational Cybercrime, China-Kazakhstan Cooperation, Legal Harmonization, Intelligence Sharing, Cybersecurity

Introduction

The rapid development of information technology has brought unprecedented challenges to global security, with transnational cybercrime emerging as a significant threat to national sovereignty, social stability, and individual rights. Characterized by its cross-border nature, high concealment, and severe harmfulness, transnational cybercrime has become a pressing issue that no single nation can address alone. The interconnectedness of cyberspace allows criminals to operate across jurisdictions, exploiting legal loopholes and technological barriers to evade detection and prosecution.[1] This phenomenon necessitates robust international cooperation, particularly among neighboring countries that share common security concerns and geopolitical interests.

China and Kazakhstan, as close neighbors and strategic partners, face similar threats from transnational cybercrime, including cyber terrorism, financial fraud, and

data breaches. The shared border and extensive economic ties between the two nations make them vulnerable to coordinated cyber-attacks and criminal activities that transcend national boundaries. Recognizing the mutual benefits of collaboration, both countries have demonstrated a strong commitment to combating cybercrime through bilateral agreements and multilateral frameworks. However, the evolving nature of cyber threats and the inherent complexities of legal and technical coordination pose significant challenges to their cooperative efforts.

This study aims to explore the legal cooperation mechanisms between China and Kazakhstan in combating transnational cybercrime, analyzing their current status, identifying existing challenges, and proposing future directions for enhancement. By examining the legal foundations, operational frameworks, and institutional practices of their collaboration, this research seeks to contribute to the broader discourse on international cybercrime governance. The findings will not only provide insights into the Sino-Kazakh partnership but also offer valuable lessons for other nations seeking to strengthen cross-border legal cooperation in the digital age.

Legal Foundations of China-Kazakhstan Cooperation in Combating Transnational Cybercrime

The legal framework underpinning the cooperation between China and Kazakhstan in combating transnational cybercrime is rooted in a multi-layered structure encompassing international law, bilateral agreements, and domestic legislation. This comprehensive legal foundation not only legitimizes their collaborative efforts but also provides a structured pathway for addressing the complex and evolving nature of cyber threats. At the international level, both countries are bound by a series of conventions and treaties that emphasize the necessity of cross-border cooperation in tackling cybercrime. The United Nations Convention against Transnational Organized Crime (UNTOC), for instance, serves as a cornerstone for international efforts to combat organized crime, including cyber-enabled offenses. By ratifying this convention, China and Kazakhstan have committed to enhancing mutual legal assistance, extradition, and law enforcement

cooperation, thereby creating a robust framework for addressing transnational cybercrime.Similarly, the Budapest Convention on Cybercrime, although not ratified by China, represents a significant international instrument that Kazakhstan has adopted.[2] This convention provides a detailed legal framework for harmonizing national laws, improving investigative techniques, and facilitating international cooperation in cybercrime cases. While China's absence from the Budapest Convention poses certain challenges, the shared principles of international cooperation and the mutual recognition of cybercrime as a global threat have enabled both nations to engage in practical collaboration. The alignment of their efforts with these international instruments underscores their commitment to a rules-based approach in combating cybercrime, even as they navigate the complexities of differing legal systems and priorities.

At the bilateral level, China and Kazakhstan have established a series of agreements that specifically address the challenges posed by transnational cybercrime. The Agreement on Cooperation in Combating Terrorism, Separatism, and Extremism between China and Kazakhstan, for example, explicitly includes provisions for combating cyber-enabled terrorism and related activities. This agreement not only reflects the shared security concerns of both nations but also provides a legal basis for joint operations, intelligence sharing, and capacity-building initiatives. Furthermore, the China-Kazakhstan Treaty on Mutual Legal Assistance in Criminal Matters facilitates the exchange of evidence, the execution of requests for investigative measures, and the coordination of judicial proceedings. These bilateral instruments collectively form a specialized legal framework that complements broader international commitments and addresses the unique challenges of cybercrime in the context of their bilateral relations.

Domestically, both China and Kazakhstan have enacted comprehensive legislation to address cybercrime, thereby providing the necessary legal support for their international and bilateral cooperation. China's Cybersecurity Law, enacted in 2017, establishes a legal framework for network security, data protection, and the

prevention of cybercrime. The law mandates cooperation with international partners in addressing cyber threats and provides a basis for cross-border investigations and information sharing. Similarly, Kazakhstan's Law on Information, Informatization, and Information Protection outlines the legal principles for combating cybercrime, including provisions for international cooperation and the protection of critical information infrastructure. These domestic laws not only align with international standards but also create a legal environment conducive to collaborative efforts in addressing transnational cybercrime.The interplay between international, bilateral, and domestic legal frameworks forms the bedrock of China-Kazakhstan cooperation in combating transnational cybercrime. While international conventions provide a broad normative foundation, bilateral agreements offer tailored mechanisms for addressing specific challenges, and domestic legislation ensures the practical implementation of cooperative measures. This multi-layered approach reflects a nuanced understanding of the complexities of cybercrime and underscores the importance of a coordinated and legally grounded response. As both nations continue to refine their legal frameworks and deepen their collaborative efforts, this foundation will remain critical to their ability to effectively address the evolving threats posed by transnational cybercrime.

Key Components of the Legal Cooperation Mechanism between China and Kazakhstan in Combating Transnational Cybercrime

The legal cooperation mechanism between China and Kazakhstan in combating transnational cybercrime is characterized by a multifaceted approach that integrates intelligence sharing, joint investigative efforts, judicial assistance, and capacity-building initiatives. This comprehensive framework is designed to address the complex and dynamic nature of cyber threats, ensuring that both nations can effectively respond to incidents that transcend their borders. At the core of this mechanism lies the establishment of robust platforms for intelligence and information exchange. Recognizing the critical role of timely and accurate information in combating cybercrime, China and Kazakhstan have developed dedicated channels for

sharing intelligence related to cyber threats, criminal networks, and emerging trends. These platforms facilitate real-time communication between law enforcement agencies, enabling proactive measures to prevent and mitigate cyber-attacks. Regular high-level meetings and technical exchanges further strengthen this aspect of cooperation, fostering a culture of trust and mutual understanding.

In the realm of investigative collaboration, China and Kazakhstan have demonstrated a commitment to joint operations and cross-border coordination. The transnational nature of cybercrime often necessitates coordinated efforts to trace criminal activities, gather evidence, and apprehend suspects. To this end, both countries have established protocols for joint investigations, allowing their law enforcement agencies to work in tandem on complex cases. Cross-border evidence collection, a critical component of such investigations, is facilitated through bilateral agreements that streamline legal procedures and ensure the admissibility of evidence in court. Additionally, the extradition of suspects, governed by mutual legal assistance treaties, ensures that individuals involved in cybercrime cannot evade justice by exploiting jurisdictional boundaries.[3] These collaborative efforts underscore the importance of a unified approach to dismantling cybercriminal networks.Judicial cooperation forms another pillar of the China-Kazakhstan mechanism, providing the legal infrastructure necessary to support cross-border investigations and prosecutions. Mechanisms for mutual legal assistance, such as the serving of legal documents, the collection of evidence, and the freezing or seizure of assets, are essential for addressing the financial dimensions of cybercrime. By aligning their judicial processes and adhering to internationally recognized standards, both nations ensure that cybercriminals are held accountable, regardless of where they operate. This aspect of cooperation also includes the harmonization of legal frameworks to address discrepancies in the definition and prosecution of cyber offenses, thereby reducing potential obstacles to effective collaboration.

Capacity-building initiatives represent a forward-looking dimension of the China-Kazakhstan cooperation mechanism, aimed at enhancing the technical and

operational capabilities of both nations in combating cybercrime. Recognizing the rapid evolution of cyber threats, both countries have prioritized the training of law enforcement personnel, the sharing of best practices, and the development of advanced technological tools. Joint training programs and workshops provide opportunities for professionals to acquire specialized skills in areas such as digital forensics, cyber intelligence analysis, and incident response. Furthermore, the exchange of technological expertise and the co-development of cybersecurity solutions contribute to the creation of a resilient and adaptive defense against cyber threats. These initiatives not only strengthen the individual capacities of China and Kazakhstan but also foster a collaborative ecosystem that is better equipped to address future challenges.The integration of intelligence sharing, investigative collaboration, judicial assistance, and capacity-building initiatives forms the backbone of the China-Kazakhstan legal cooperation mechanism in combating transnational cybercrime. This holistic approach reflects a deep understanding of the multifaceted nature of cyber threats and the necessity of a coordinated response. By leveraging their respective strengths and fostering a spirit of collaboration, China and Kazakhstan have established a model for regional cooperation in addressing one of the most pressing security challenges of the digital age. As cyber threats continue to evolve, this mechanism will remain vital to ensuring the security and stability of both nations and the broader international community.

Challenges Facing the Legal Cooperation Mechanism between China and Kazakhstan in Combating Transnational Cybercrime

Despite the robust framework of cooperation between China and Kazakhstan in combating transnational cybercrime, several significant challenges hinder the full realization of their collaborative potential. One of the most pressing issues stems from the legal differences between the two nations. Variations in the definition of cybercrime, sentencing standards, and evidentiary rules create substantial obstacles to seamless cooperation. For instance, actions classified as criminal offenses in one country may not be similarly recognized in the other, leading to discrepancies in legal

proceedings and enforcement. These differences complicate the process of mutual legal assistance, extradition, and the admissibility of evidence in cross-border cases, thereby undermining the effectiveness of joint efforts.

Technical challenges further exacerbate the difficulties faced by China and Kazakhstan in addressing transnational cybercrime. The inherently complex and rapidly evolving nature of cyber threats requires advanced technological capabilities for the collection, preservation, and analysis of electronic evidence. However, disparities in technological infrastructure and expertise between the two nations can impede the efficient handling of cyber incidents.[4] The anonymity and cross-border nature of cybercriminal activities often necessitate sophisticated tools and methodologies for tracking and attribution, which may not always be readily available or harmonized across jurisdictions. These technical limitations highlight the need for continuous investment in cybersecurity technologies and the development of standardized protocols for digital forensics.

Political factors also play a critical role in shaping the dynamics of China-Kazakhstan cooperation in combating cybercrime. The broader international political environment, including geopolitical tensions and shifting alliances, can influence the willingness and ability of both nations to collaborate effectively. Additionally, domestic political considerations, such as differing priorities in national security strategies or concerns over sovereignty, may impact the implementation of joint initiatives. These political dimensions underscore the importance of fostering a stable and trusting bilateral relationship, as well as aligning their respective interests in the realm of cybersecurity. Addressing these challenges requires a nuanced understanding of the interplay between legal, technical, and political factors, as well as a commitment to overcoming these barriers through sustained dialogue and cooperation.

Recommendations for Enhancing the Legal Cooperation Mechanism between China and Kazakhstan in Combating Transnational Cybercrime

To address the challenges facing the legal cooperation mechanism between China

and Kazakhstan in combating transnational cybercrime, a series of targeted measures must be implemented to strengthen their collaborative framework. Central to these efforts is the need for enhanced legal coordination between the two nations. The existing legal disparities, particularly in the definition of cybercrime, evidentiary standards, and procedural requirements, necessitate the development of harmonized legal instruments. Signing a specialized bilateral agreement focused exclusively on combating transnational cybercrime would provide a clear and cohesive legal foundation for cooperation. Such an agreement should include provisions for the mutual recognition of cyber offenses, standardized procedures for evidence collection and sharing, and streamlined mechanisms for extradition and mutual legal assistance. By aligning their legal frameworks, China and Kazakhstan can reduce jurisdictional conflicts and enhance the efficiency of their joint efforts.Deepening technical cooperation is equally critical to overcoming the challenges posed by the sophisticated and evolving nature of cyber threats. Establishing joint laboratories dedicated to cybersecurity research and development would enable both nations to pool their resources and expertise, fostering innovation in areas such as digital forensics, threat intelligence, and incident response.[5] Collaborative projects aimed at developing advanced technological tools, including artificial intelligence-driven analytics and blockchain-based traceability systems, could significantly enhance their capacity to detect, prevent, and respond to cyber incidents. Furthermore, regular technical exchanges and joint training programs would ensure that law enforcement personnel in both countries are equipped with the latest skills and knowledge, thereby strengthening their operational effectiveness.

Expanding international collaboration is another essential component of a robust strategy to combat transnational cybercrime. While bilateral efforts between China and Kazakhstan are crucial, the global nature of cyber threats necessitates a broader approach. Active participation in international organizations such as INTERPOL and the United Nations Office on Drugs and Crime (UNODC) would provide access to a wider network of resources, intelligence, and best practices. Engaging in multilateral

initiatives, such as the Budapest Convention on Cybercrime or regional cybersecurity forums, would further enhance their ability to address cross-border cyber threats. Additionally, forging bilateral and multilateral agreements with other nations, particularly those in the Central Asian region, would create a more comprehensive and interconnected cybersecurity ecosystem.

By prioritizing legal harmonization, technological innovation, and international engagement, China and Kazakhstan can significantly enhance their legal cooperation mechanism for combating transnational cybercrime. These measures not only address the immediate challenges but also lay the groundwork for a more resilient and adaptive approach to cybersecurity. As cyber threats continue to evolve, sustained commitment to these recommendations will be essential to safeguarding the security and stability of both nations and the broader international community.

Conclusion

The legal cooperation mechanism between China and Kazakhstan in combating transnational cybercrime represents a critical framework for addressing one of the most pressing security challenges of the digital age. By integrating intelligence sharing, joint investigations, judicial assistance, and capacity-building initiatives, this mechanism has demonstrated its effectiveness in mitigating the threats posed by cybercriminals who exploit the borderless nature of the internet. The collaboration between the two nations not only strengthens their individual cybersecurity postures but also contributes to regional and global stability by setting a precedent for cross-border cooperation in a highly complex and evolving domain. The significance of this partnership lies in its ability to bridge legal, technical, and political differences, fostering a unified approach to safeguarding national sovereignty, economic interests, and the rights of citizens in the digital realm.

Looking ahead, the dynamic and ever-changing nature of cyber threats necessitates a sustained and proactive commitment from both China and Kazakhstan. Continued efforts to harmonize legal frameworks, enhance technological capabilities, and expand international collaboration will be essential to maintaining the relevance

and effectiveness of their cooperation mechanism. As cybercriminals increasingly employ sophisticated tactics, the two nations must remain vigilant and adaptive, leveraging their shared experiences and mutual trust to innovate and refine their strategies. By deepening their partnership and embracing a forward-looking perspective, China and Kazakhstan can not only address current challenges but also anticipate and mitigate future risks, ensuring the long-term security and resilience of their digital ecosystems.

Reference

1. Kreminskyi O., Kuzmenko O., Antoniuk A., et al. International cooperation in the investigation of economic crimes related to cryptocurrency circulation // Studies of Applied Economics. 2021. T. 39, № 6.
2. Saifullah R., Shah S. S. R. Transnational Law and Criminal Justice System: Highlighting Legislative and Procedural Challenges to Combat Cyber Crime in the Wake of CPEC // JISR Management and Social Sciences & Economics (JISR-MSSE). 2023. T. 21, № 4. Pp. 73-92.
3. Nukusheva A., Zhamiyeva R., Shestak V., et al. RETRACTED ARTICLE: Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development // Security Journal. 2022. T. 35, № 3. Pp. 893-912.
4. Zhaparalina B., Sheryazdanova K., Kakenova G., et al. The Influence of Information Cooperation in Central Asia on the Interests and Foreign Policy of the Republic of Kazakhstan // Journal of Information Policy. 2024. T. 14.
5. Bolatbek M., Baispay G., Mussiraliyeva S., et al. A framework for detection and mitigation of cyber criminal activities using university networks in Kazakhstan // Radioelectronic and Computer Systems. 2024. T. 2024, № 2. Pp. 186-202.