Scientific Research Publishing

Beijing Law Review, 2026, 17(3), 827-837
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Mechanism Dilemmas and Innovative Paths of China-ASEAN Police Law Enforcement Cooperation from the Perspective of the Holistic Approach to National Security: Focusing on the Intelligentization of Cross-Border Crime and Digital Policing Governance

Yi Lei

Yunnan Police College, Kunming, China
Email: 240208567@qq.com

How to cite this paper: Lei, Y. (2026). Mechanism Dilemmas and Innovative Paths of China-ASEAN Police Law Enforcement Cooperation from the Perspective of the Holistic Approach to National Security: Focusing on the Intelligentization of Cross-Border Crime and Digital Policing Governance. *Beijing Law Review, 17,* 827-837.
https://doi.org/10.4236/blr.2026.173043

Received: July 18, 2026
Accepted: September 4, 2026
Published: September 7, 2026

Abstract

The intelligent iteration of cross-border crime and the regional penetration of digital policing are profoundly reshaping the governance logic of border security between China and ASEAN. Traditional police cooperation models, dominated by case-by-case consultation and ad hoc operations, can neither adapt to new forms of crime empowered by algorithms and virtual circulation, nor respond to governance demands amid growing awareness of data sovereignty. Grounded in the four-dimensional connotation of the holistic approach to national security—common, comprehensive, cooperative, and sustainable security—this paper incorporates frontier variables such as cross-border data flow rules and digital policing governance into its analytical scope, and constructs a framework of *conceptual guidance-mechanism operation-rule constraint-effectiveness output*. The study finds that current cooperation faces three structural dilemmas: informal institutional supply, misalignment of digital rules, and a weak trust foundation. Among these, the inherent tension between the sovereign attribute of police data and law enforcement effectiveness constitutes the core contradiction restricting the deepening of cooperation in the digital era. Accordingly, this paper proposes a four-dimensional innovative path of *consensus building*, *field expansion*, *rule improvement*, *and joint capacity building*. It focuses on exploring graded and classified data flow rules, the ap-

plication of privacy computing technology, and the construction of a collaborative algorithm governance framework to bridge the gap between technical feasibility and regulatory compliance. This research aims to provide theoretical support and practical solutions for the institutional and intelligent collaborative transformation of China-ASEAN police cooperation.

Keywords

Holistic Approach to National Security, China-ASEAN Police Law Enforcement Cooperation, Cross-Border Data Flow, Digital Policing Governance

1. Introduction

1.1. Research Background and Problem Formulation

The deep integration of digital technology and cross-border crime is driving a paradigmatic shift in crime patterns along the China-ASEAN border. In recent years, telecom fraud syndicates in northern Myanmar and along the Myanmar-Thailand border have completed intelligent upgrades: they rely on generative AI to customize scam scripts, use encrypted communications to coordinate division of labor, and launder funds via virtual currencies, exhibiting typical characteristics of corporate operation, chain-based layout, and technical anti-investigation. Since 2023, joint China-Myanmar crackdown operations have transferred over 10,000 suspects, which not only demonstrates law enforcement effectiveness but also exposes structural shortcomings of traditional policing models in responding to intelligent crime.

Traditional China-ASEAN police cooperation centers on traditional security issues such as drug control and counter-terrorism, advanced through bilateral meetings and case-by-case assistance, and has achieved remarkable results in physical space governance. However, in the face of instantaneous, decentralized, and cross-domain linked intelligent crime, the limitations of the original framework have become increasingly prominent: intelligence exchange lags behind operational needs, data flow is hindered by sovereignty barriers, and joint law enforcement lacks rigid constraints. The deeper bottleneck lies in the fact that cooperation has extended from the technical level to the institutional and regulatory levels. As countries strengthen their awareness of data sovereignty and tighten data localization legislation, the long-term absence of cross-border flow rules for police data has plunged digital police collaboration into the dilemma of being *technically feasible but non-compliant with rules*.

Against this backdrop, how to break through sovereignty concerns and regulatory dilemmas under the guidance of the holistic approach to national security, and build a new cooperation system adapted to intelligent crime governance, has become an important proposition for maintaining regional security. The systematic thinking and global security vision inherent in the holistic approach to na-

tional security provide a theoretical foundation and value guidance for transcending zero-sum games and coordinating data sovereignty with law enforcement effectiveness.

1.2. Definition of Core Concepts

Intelligentization of cross-border crime: An evolutionary trend in which criminal organizations use digital technology to restructure their offense processes, achieving precise target screening, covert implementation of behaviors, and cross-border transfer of proceeds. Its core is a cross-regional division of labor and upgraded anti-investigation capabilities empowered by technology.

Cross-border digital police collaboration: Cooperation among police authorities of various countries relying on digital technology in areas such as data sharing and algorithmic analysis, aiming to improve effectiveness on the premise of safeguarding sovereignty.

Cross-border flow of police data: The cross-border transmission and processing of case clues, personnel information, and other data, which have the dual attributes of law enforcement tool and national sovereignty, and belong to a highly sensitive governance field.

1.3. Research Design and Methodology

This paper follows the logic of "theoretical construction–mechanism analysis–dilemma interpretation–path optimization". Guided by the four-dimensional connotation of the holistic approach to national security, it combines digital governance dimensions to construct an analytical framework, explains the operation mechanism of cooperation, analyzes the causes of dilemmas, and proposes innovative paths. This paper adopts the normative analysis method to sort out theoretical connotations, the case study method to analyze practices such as Mekong River patrols and China-Myanmar anti-fraud operations, and the comparative analysis method to compare differences in national data legislation.

2. Literature Review and Theoretical Foundation

2.1. Maintaining the Integrity of the Specifications

Domestic research has gone through two stages. In the initial stage, studies focused on traditional security issues such as drug control and counter-terrorism. Scholars such as Li (2024) and Wu (2024) summarized the *problem-oriented*, *project-driven* model and the effectiveness of bilateral cooperation, but most of them emphasized empirical induction with insufficient theoretical construction. With the spread of new types of crime, research has turned to intelligent transformation. Zhang et al. (2024) proposed a collaborative pattern of data sharing and joint algorithm construction, and Cui (2024) pointed out that the lack of rigid constraints on flexible document carriers is a bottleneck for effectiveness.

Research on the application of the holistic approach to national security falls into two categories: one is value-oriented research, such as Xiao (2018) and Cen

& Wu (2021), who emphasized its guiding significance for international cooperation but mostly focused on conceptual interpretation; the other is practical application research, which focuses on institutional design but has the problem of 'conceptual labeling', failing to transform the concept into analyzable variables. In terms of digital governance research, Li (2025) pointed out that the flow of police data needs to balance law enforcement and sovereignty, and Huang (2024) analyzed national security exception rules, but did not form a theoretical connection combined with regional practice.

Existing research has the following gaps: first, theoretical application is fragmented, with insufficient interpretation of the digital dimension; second, the response to issues lags behind, failing to delve into the core contradiction between data flow and algorithm governance; third, the adaptability of countermeasures is insufficient, without fully considering the sovereignty sensitivity and development differences of ASEAN countries. This paper attempts to fill the above gaps and construct a systematic analytical framework.

2.2. Theoretical Foundation: Connotation Expansion and Digital Dimension of the Holistic Approach to National Security

The holistic approach to national security is the fundamental guideline for national security governance in the new era. Its connotation for international security governance extends to the concepts of *common*, *comprehensive*, *cooperative*, *and sustainable security*. Common security emphasizes interest symbiosis and risk sharing; comprehensive security emphasizes coordinating multi-dimensional threats; cooperative security emphasizes replacing zero-sum games with equal consultation; sustainable security emphasizes the long-term effectiveness of institutional and capacity building.

In the digital era, its connotation expands to cyberspace: data security becomes a component of the security system, and data sovereignty becomes an extension of political security. This requires cross-border police cooperation to adhere to the bottom line of data security and sovereign equality. Under the guidance of the four-dimensional connotation, countries should jointly respond to digital crime threats, coordinate traditional border and cyberspace security, negotiate to build data flow rules, and simultaneously promote technological and governance capacity building. Different from the Western logic of *sovereignty transfer*, China-ASEAN cooperation needs to adhere to the bottom line of political security and explore a path of *resilient mutual embedding and gradual upgrading*.

2.3. Analytical Framework: The Logic of Concept-Rule-Effectiveness

Based on the holistic approach to national security, this paper constructs a research framework of "conceptual guidance-rule intermediation-effectiveness output". Common security constitutes the driving mechanism, reshaping interest perception to drive mutual trust; comprehensive security constitutes the expan-

sion mechanism, identifying threat correlations to promote field extension; cooperative security constitutes the guarantee mechanism, standardizing law enforcement links through procedural design; sustainable security constitutes the supporting mechanism, ensuring long-term operation through institutional construction. Cross-border data flow rules are the core intermediary connecting concepts and effectiveness: concepts guide the direction of rules, rules determine the boundaries of technology, and together they affect cooperation effectiveness.

3. Operational Mechanisms of Police Law Enforcement Cooperation under the Guidance of the Holistic Approach to National Security

3.1. Common Security: Generation Mechanism of Political Mutual Trust and Willingness to Cooperate

Common security regards the region as an indivisible whole and promotes the shift from *unilateral defense* to *collaborative governance* by reconstructing interest calculation. In terms of cognitive reshaping, the rapid consensus reached by China, Laos, Myanmar, and Thailand after the Mekong River tragedy stemmed from all parties recognizing the common harm of spreading crime and that collaborative governance has the lowest cost and optimal effectiveness. In terms of interest binding, Lancang-Mekong cooperation coordinates drug control law enforcement with alternative planting and livelihood assistance. The *security + development* model increases willingness to invest and reduces the risk of single-issue fluctuations. Of course, geopolitical and external discourse factors still pose challenges to strategic mutual trust, requiring continuous expansion of interest convergence points.

3.2. Comprehensive Security: Transmission Mechanism of Field Expansion and Resource Integration

Comprehensive security advocates systematic governance to address intertwined chain-based crime patterns. Its transmission effect is reflected in horizontal field expansion: cooperation extends from drug control to digital crimes such as counter-terrorism, telecom fraud, and money laundering, avoiding governance blind spots. It is also reflected in vertical resource integration: the Lancang-Mekong Integrated Law Enforcement and Security Cooperation Center (LMLECC) builds a platform to integrate multi-departmental resources of various countries, enabling cross-departmental circulation and joint disposal. Although limited by differences in national systems and the depth of integration, the concept of comprehensive security provides a cognitive foundation for whole-chain governance.

3.3. Cooperative Security: Guarantee Mechanism of Intelligence Sharing and Joint Operations

Cooperative security provides guarantees for sensitive collaboration through procedural design and mutual trust accumulation. At the level of intelligence sharing,

the rule of *graded classification and on-demand sharing* has been established. Mekong River joint patrols prioritize sharing early warning information while retaining the right to handle core secrets, reducing sovereignty risks through *separable sharing*. In the digital era, the China-Thailand Memorandum of Understanding on Digital Police Cooperation clarifies three levels of sharing standards: regular sharing of early warning data, approved sharing of clue data, and result feedback of sensitive data. This mechanism transforms political judgment into technical judgment and realizes the implementation of concepts. At the level of joint operations, following the principle of *low starting point and step-by-step* to accumulate mutual trust, cooperation gradually advances from patrol notification to joint crackdowns.

3.4. Dual-Dimensional Empowerment Mechanism Innovation: Institutional Construction of Physical Platforms and Technological Upgrading of Smart Policing

Sustainable security focuses on governance resilience and promotes the transformation of cooperation from *passive response* to *active defense*. Institutional evolution is reflected in normalization and substantiation. The establishment of substantive institutions such as the LMLECC has shifted cooperation to *platform-driven* mode, ensuring timeliness. Technological evolution is reflected in smart police collaboration, such as the Youyi Pass smart customs clearance system and cross-border crime algorithm research and development, which improve accuracy and response speed to adapt to the evolution of crime patterns.

4. Structural Dilemmas of China-ASEAN Police Law Enforcement Cooperation

4.1. Insufficient Institutional Supply: Informality and Fragmentation of Cooperation Mechanisms

The mismatch between institutional supply and governance demand is a prominent dilemma. In terms of institutional carriers, most existing documents are declarations and memoranda of understanding, lacking legal binding force. Cooperation relies on *political consensus-driven* advancement, and case-by-case collaboration is greatly affected by leaders' mutual visits and special operations, lacking stable expectations. While this flexible arrangement conforms to the ASEAN *consensus* principle, it also leads to insufficient execution, and core links tend to become formalistic. In terms of organizational carriers, permanent institutions have a low degree of substantiation, lack independent action scheduling authority, and have long intelligence transmission chains and slow responses, making it difficult to cope with the iteration of intelligent crime. At the current stage, the institutional foundation for regional police cooperation mostly takes the form of "soft law" such as political declarations, memorandums of understanding, and consensus reached at annual meetings, including foundational documents like the Joint Declaration on Cooperation in the Field of Non-Traditional Security between

China and ASEAN and the Memorandum of Understanding on Cooperation in the Field of Non-Traditional Security. Such cooperation frameworks only carry political guiding value and lack binding force under international law, making it difficult to establish a unified, stable, and enforceable system of regional law enforcement rules. The imbalance in the supply of regional institutions is particularly prominent in the fields of extradition and judicial assistance. To date, China has concluded bilateral extradition treaties with only a small number of ASEAN countries including Thailand, Laos, Cambodia, and the Philippines. No stable extradition cooperation mechanisms have been established with key countries plagued by frequent cross-border crimes such as Myanmar, Vietnam, and Malaysia. The transfer of involved persons mostly relies on informal channels including ad hoc repatriation and friendly assistance, which feature arbitrary procedures and poor stability. Meanwhile, some ASEAN countries have formed special judicial barriers based on their domestic legal systems. For instance, Cambodia has abolished the death penalty and generally applies the principle of non-extradition of persons facing the death penalty. This directly prevents the lawful extradition of core ringleaders in major cases such as cross-border telecom fraud and transnational drug trafficking, seriously undermining the effectiveness of regional crackdowns on serious crimes.

4.2. Misalignment of Digital Rules: Tension of Data Sovereignty and Gap in Algorithm Governance

Data and algorithms have become core elements, but the absence of rules constitutes a barrier.

First, legislative fragmentation leads to docking dilemmas. Data governance within ASEAN is divergent, with large differences in standards among Singapore, Thailand, Indonesia, and other countries, and the ASEAN Digital Data Governance Agreement does not include special provisions for police data. China incorporates police data into strict management as *important data*, and dual compliance requirements expose regular sharing to legal risks. Second, the *dual attribute* of data leads to sovereignty tension. Full-volume sharing is conducive to law enforcement effectiveness, but data is related to national governance fundamentals, and excessive openness will damage sovereign security. Some ASEAN countries seek technical support while fearing sovereignty transfer, and this tension needs to be resolved through rule design. Third, there is a gap in algorithm governance. Cross-border predictive policing algorithms have three gaps: jurisdiction, ethics, and standards. The responsibility for misjudgment is unclear; models may produce discrimination due to data bias; and inconsistent data standards among countries lead to high adaptation costs. This results in cooperation mostly staying at the level of equipment assistance, making it difficult to enter deep collaboration. The digital legislation and data governance systems of ASEAN member states currently exhibit a distinct tiered fragmented pattern. Singapore, Malaysia, and Thailand have established comprehensive legislative frameworks for personal data

protection and cybersecurity with stringent data regulatory standards. Vietnam enforces strict data localization requirements that restrict the free flow of cross-border data. In contrast, Myanmar, Laos, Cambodia, and other countries have yet to introduce dedicated unified data protection legislation, leaving gaps in digital governance rules and ambiguous law enforcement standards. In terms of unified regional regulations, the ASEAN Model Contract Clauses for Cross-Border Data Flows serve merely as voluntary reference norms without binding force. There exist substantial discrepancies among member states regarding standards for cross-border transmission of classified police data and case-related electronic data, forensic procedures, confidentiality requirements, and the recognition of evidentiary validity. This impedes the formation of unified regional rules for police data collaboration.

4.3. Weak Trust Foundation: Geopolitical Cognitive Bias and Cultural Differences Barriers

Political mutual trust and cultural identity are the foundation of cooperation, but trust deficits still exist. At the geopolitical level, influenced by external discourses, some countries regard cooperation as *strategic expansion*, are highly vigilant about intelligence sharing involving sovereignty, and even regard technology export as *digital penetration*. At the law enforcement culture level, China emphasizes systematic governance and active prevention, while some countries focus on procedural justice. Differences in concepts lead to cognitive bias and psychological resistance. Cross-border ethnic issues also increase the complexity of border law enforcement. From the perspective of cooperative practice, the current police mutual trust between China and ASEAN is typically "ad hoc mutual trust", and a long-term security mutual trust system has not yet taken shape. For instance, cross-border special joint operations against telecom fraud such as Operation Seagull carried out in the region can concentrate law enforcement resources in a short period and achieve remarkable governance outcomes. Nevertheless, upon the conclusion of such special operations, regular coordination mechanisms weaken immediately, and the intensity of intelligence sharing, joint control, and risk joint prevention keeps declining. Meanwhile, current regional police exchange and cooperation adopt limited forms and lack carriers for fostering mutual trust, making it difficult to support in-depth digital police cooperation. Existing cooperation mostly stays at superficial exchange models, including short-term police training, one-off joint drills, and annual work meetings. Long-term platforms such as regular secondment of police officers, joint laboratories for digital forensics, special working groups for cross-border crime research and judgment, and coordination mechanisms for law enforcement disputes have not been established. When confronted with emerging conflicts such as differing standards for digital law enforcement, divergences over the admissibility of electronic evidence, and disputes concerning cross-border data flows, mature consultation and mitigation mechanisms are absent, which hinders the formation of stable and sustainable governance synergy.

5. Innovative Upgrading of Cooperation Paths from the Perspective of the Holistic Approach to National Security

The innovative model of intelligent cross-border crime governance and digital police management for China-ASEAN cooperation is not a marginal technical upgrade of conventional regional police cooperation. Instead, it responds to cross-border security governance transformations in the digital era and achieves a dual theoretical iteration and boundary expansion of international police cooperation theory and global digital security governance theory. Traditional China-ASEAN police cooperation, which relies on offline assistance, case-by-case disposal, and sovereign equal cooperation, is inherently limited by conservative security perceptions, fragmented institutional arrangements, and passive governance paradigms. By reshaping security values, restructuring institutional cooperation mechanisms, and realizing leaps in governance effectiveness, the digital policing and intelligent governance model proposed in this study forms a complete causal loop of "concept innovation - mechanism upgrading - performance advancement." It addresses the theoretical adaptability dilemmas embedded in traditional regional police cooperation and enriches the theoretical system of cross-border public security governance in the digital age. To solve the above dilemmas, we must take the holistic approach to national security as the fundamental guide and make coordinated efforts from four dimensions: *consensus building*, *field expansion*, *rule improvement*, *and joint capacity building*.

5.1. Building Consensus on Common Security: Deepening Strategic Mutual Trust and Interest Binding

Common security is the prerequisite. First, strengthen high-level strategic docking, explain security concepts through multilateral platforms, convey goodwill for cooperation, dispel the cognitive bias of *digital hegemony*, and carry out differentiated communication in response to different concerns. Second, deepen the *security* + *development* interest binding, embed police cooperation into regional economic and livelihood projects, so that security cooperation becomes a guarantee for development rather than a burden, and enhance the willingness of all countries to invest. Third, expand law enforcement, cultural, and people-to-people exchanges, enhance professional identity and conceptual consensus through joint training, and reduce the interference of cultural barriers.

5.2. Practicing the Concept of Comprehensive Security: Expanding Governance Fields and Resource Integration

Comprehensive security is the path. Promote the extension of fields to the whole chain of digital crime. On the basis of consolidating traditional cooperation, focus on deepening the governance of new types of crimes such as telecom fraud and money laundering, and establish special mechanisms to study and judge trends. Build a cross-departmental and cross-level collaborative system, break the single dominance of police affairs, integrate resources from multiple departments such

as cyberspace administration, finance, and customs, grant border areas greater autonomy in collaboration, and form governance synergy.

5.3. Improving Cooperative Security Rules: Constructing an Institutional Framework for Digital Police Collaboration

Cooperative security is the guarantee. In response to the absence of rules, first, establish graded and classified data flow rules. Promote the *whitelist* mechanism to simplify the exit of early warning data; establish mutual recognition of security assessments to avoid repeated reviews; promote the *data localization* + *cross-border results* model, where core data does not leave the country and only conclusions are shared to safeguard sovereignty. Second, implement privacy computing technology. With the core principle of *data stays*, *model moves*, *value flows*, build a privacy computing platform, and jointly train models through federated learning to realize data availability without visibility, balancing effectiveness and sovereignty. Third, establish an algorithm governance mechanism. Build a collaborative algorithm governance framework, formulate ethical guidelines, establish a mutual recognition mechanism for security assessments to prevent bias risks; promote the joint construction of data standards, unify formats and interfaces, and reduce adaptation costs.

5.4. Anchoring Sustainable Security Goals: Promoting Institutional Substantiation and Joint Capacity Building

Sustainable security is the support. First, promote the substantiation of mechanisms. Build permanent cooperation institutions and endow them with intelligence, research and judgment, and action coordination functions; promote the upgrading of agreements to legal treaties, improve clauses in emerging fields, and enhance rigidity.

Second, deepen joint capacity building. Shift to a two-way model of *technical assistance* + *standard co-construction* + *talent training* to make up for the technical shortcomings of less developed countries; establish a normalized talent training mechanism to improve comprehensive capabilities. Third, establish a dynamic iteration mechanism. Regularly evaluate and adjust cooperation fields and rules, encourage border areas to pilot first, and maintain the adaptability and vitality of the system.

6. Conclusion and Future Work

Guided by the holistic approach to national security, this paper analyzes the mechanisms, dilemmas, and paths of China-ASEAN police law enforcement cooperation. The study finds that the four-dimensional connotation of the holistic approach to national security guides cooperation through four mechanisms: driving, expansion, guarantee, and support, and that data sovereignty and rule supply have become key variables in the digital era. Current cooperation faces three dilemmas: informal institutions, misaligned digital rules, and a weak trust foundation, and

the tension between data sovereignty and law enforcement effectiveness is the core contradiction. The solution lies in following the four-dimensional concepts, adopting a layered and gradual path, focusing on building data flow rules, applying privacy computing, and constructing a collaborative algorithm governance framework, so as to achieve a balance between effectiveness and security.

This paper constructs an analytical framework for the holistic approach to national security guiding cross-border police cooperation, expanding theoretical horizons; it introduces cross-border data flow rules into research, revealing the contradiction of *technically feasible but rules lag behind*. The limitations are that most empirical materials are derived from public documents, lack front-line research, and the analysis of ASEAN country differences is insufficient. Future research should carry out empirical investigations, deepen country-specific comparative studies, and continuously track the impact of new technologies such as generative AI on cooperation.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Cen, S. J., & Wu, F. (2021). Counter-Terrorism Police Cooperation between China and ASEAN from the Perspective of the Holistic Approach to National Security. *Journal of Sichuan Police College, 33,* 97-104. (In Chinese)

Cui, Y. T. (2024). The Construction of Permanent Police Cooperation Agency in the "China-ASEAN" Region: Necessity, Feasibility, and Basic Framework. *Journal of Jiangsu Police Institute, 39,* 87-97. (In Chinese)

Huang, Z. X. (2024). National Security Exception Rules in Cross-Border Data Flow and Their Application in Law Enforcement Cooperation. *Chinese Journal of Law, No. 3,* 128-146. (In Chinese)

Li, S. Q. (2025). Balance between Law Enforcement Effectiveness and Data Sovereignty in Cross-Border Police Cooperation. *Journal of Criminal Investigation Police University of China, No. 2,* 33-41. (In Chinese)

Li, Y. Z. (2024). Expansion and Deepening of Regional International Police Law Enforcement Cooperation under the Framework of the China-ASEAN Community with a Shared Future. *Legal Vision, No. 35,* 10-13. (In Chinese)

Wu, P. (2024). Research on Police Cooperation in Combating Transnational Crimes under the Background of Building a China-Vietnam Community with a Shared Future. *Journal of Railway Police College, 34,* 28-32. (In Chinese)

Xiao, J. (2018). International Police Cooperation from the Perspective of the Holistic Approach to National Security. *Journal of Criminal Investigation Police University of China, No. 4,* 19-25. (In Chinese)

Zhang, T. et al. (2024). Collaborative Pattern of Data Sharing and Algorithm Co-Construction in China-ASEAN Intelligent Police Cooperation. *Journal of Public Security, No. 4,* 72-80. (In Chinese)