Al Ushuliy: Jurnal Mahasiswa Syariah dan Hukum
Vol. 5 No. 1, 2026, 39 - 54
P-ISSN: 3025-1060; E-ISSN: 3025-1001
DOI: 10.31958/alushuliy.v5i1.16871

Law Enforcement Barriers to Cross-Border Cybercrime in Indonesia: A Comparative Study with the Philippines

Fadhli Muhaimin Ishaq[1*]

[1] Universitas Pamulang

*Corresponding Author: dosen03505@unpam.ac.id

Abstract: Cross-border cybercrime poses significant challenges to national law enforcement because digital offenses transcend territorial jurisdictions and rely on volatile electronic evidence. In Indonesia, enforcement remains hindered by fragmented jurisdiction, limited digital forensic capacity, weak mutual legal assistance mechanisms, constrained extradition arrangements, and incomplete harmonization of domestic law with international standards. This article examines these challenges through Lawrence Friedman's Legal System Theory, focusing on the dimensions of legal structure, legal substance, and legal culture. Employing normative legal research with statute and comparative approaches, the study analyzes primary legal materials, including Law No. 1 of 2024 amending the Electronic Information and Transactions Law, Law No. 27 of 2022 on Personal Data Protection, Law No. 1 of 2023 on the Criminal Code, and the 2001 Budapest Convention on Cybercrime, supported by relevant secondary sources. The findings reveal that Indonesia's enforcement difficulties arise not only from incomplete legal harmonization but also from weak procedural mechanisms for cross-border electronic evidence, limited institutional capacity, inadequate digital forensic resources, and ineffective international cooperation. A comparison with the Philippines, the only ASEAN member state to have ratified the Budapest Convention, shows that ratification facilitates access to international cooperation and capacity-building programs but does not automatically ensure effective enforcement, as significant implementation gaps remain. The study therefore recommends Indonesia's conditional ratification of the Budapest Convention through reservation mechanisms that safeguard digital sovereignty, particularly regarding Article 32, accompanied by targeted amendments to the Electronic Information and Transactions Law and the Personal Data Protection Law to strengthen domestic enforcement capacity.

Abstrak: Kejahatan siber lintas negara menimbulkan tantangan yang signifikan bagi penegakan hukum nasional karena tindak pidana digital melampaui batas yurisdiksi teritorial dan bergantung pada alat bukti elektronik yang bersifat dinamis. Di Indonesia, penegakan hukum terhadap kejahatan siber lintas negara masih menghadapi berbagai kendala, antara lain fragmentasi yurisdiksi, keterbatasan kapasitas forensik digital, lemahnya mekanisme bantuan hukum timbal balik, terbatasnya pengaturan ekstradisi, serta belum optimalnya harmonisasi hukum nasional dengan standar internasional. Artikel ini mengkaji tantangan tersebut menggunakan Teori Sistem Hukum Lawrence Friedman dengan menitikberatkan pada dimensi struktur hukum, substansi hukum, dan budaya hukum. Penelitian ini merupakan penelitian hukum normatif yang menggunakan pendekatan peraturan perundang-undangan dan pendekatan komparatif. Bahan hukum primer meliputi Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta Konvensi Budapest 2001 tentang Kejahatan Siber, yang didukung oleh berbagai sumber hukum sekunder. Hasil penelitian menunjukkan bahwa kendala penegakan hukum di Indonesia tidak hanya disebabkan oleh belum optimalnya harmonisasi hukum, tetapi juga oleh lemahnya mekanisme pembuktian elektronik lintas negara, keterbatasan kapasitas kelembagaan, minimnya sumber daya forensik digital, dan belum efektifnya kerja sama internasional. Perbandingan dengan Filipina menunjukkan bahwa ratifikasi Konvensi Budapest

memperluas akses terhadap jaringan kerja sama internasional dan program penguatan kapasitas, namun belum menjamin efektivitas penegakan hukum karena masih terdapat kesenjangan implementasi. Oleh karena itu, penelitian ini merekomendasikan ratifikasi Konvensi Budapest secara bersyarat melalui mekanisme reservasi untuk menjaga kedaulatan digital, khususnya terhadap Pasal 32, disertai perubahan yang terarah terhadap Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pelindungan Data Pribadi guna memperkuat kapasitas penegakan hukum nasional.

Keywords: Cross-border cybercrime; Budapest Convention; Legal System Theory

‖ *Recieved: 29-04-2026* ‖ *Revised: 25-06-2026* ‖ *Accepted: 29-06-2026*

Introduction

The exponential advancement of information and communication technologies has transformed social interaction, economic activity, and public governance on a global scale. At the same time, digitalization has created new opportunities for criminal conduct committed through or against computer systems, commonly referred to as cybercrime. Unlike conventional offences, cybercrime is characterized by its technological dependence, borderless operation, and the volatility of electronic evidence, all of which complicate its detection, investigation, and prosecution (Yiu-Chung Lau, 2025). In this respect, cybercrime has become one of the most pressing challenges for contemporary criminal justice systems, particularly because legal institutions remain territorially structured while cyber offences frequently transcend national borders. The adagium het recht hinkt achter de feiten aan is therefore especially relevant in the digital era, as law often lags behind the rapid and dynamic development of technology

Within the academic literature, cybercrime is increasingly discussed not merely as a question of criminalization, but as a problem of transnational law enforcement. Existing studies identify at least three central issues in this debate. First, scholars have emphasized the jurisdictional problem arising from the fact that perpetrators, victims, servers, financial flows, and harmful effects may be located in different jurisdictions, thereby challenging conventional approaches to locus delicti and territorial criminal jurisdiction (Nicholas L Tobing & Fitria, 2025; Situmeang et al., 2026). Second, the literature highlights the problem of electronic evidence and procedural law, particularly because digital evidence is fragile, easily altered, and often stored abroad, while cross-border access to such evidence remains dependent on slow and fragmented cooperation mechanisms (Casino et al., 2022; Davies & Kennedy-Mayo, 2026). Third, a growing body of scholarship underscores the institutional and cooperative dimension of cybercrime enforcement, arguing that even where domestic criminal provisions already exist, effective enforcement remains difficult without harmonized procedural standards, technical capacity, and operational international cooperation(Billow, 2024). These debates demonstrate that the challenge of cybercrime lies not only in defining cyber offences under domestic law, but also in building a legal and institutional architecture capable of responding to offences that operate across jurisdictions.

This broader debate is highly relevant to Indonesia. Empirically, the threat of cybercrime in Indonesia has shown a significant upward trend. Reports from national and international institutions indicate that Indonesia remains one of the countries in Southeast Asia with a high level of exposure to cyberattacks(Sari, 2024). This trend is reflected not only in the increasing number of incidents, but also in the growing sophistication of cybercrime modalities, including ransomware attacks, phishing schemes, and the exploitation of digital systems in both public institutions and the private sector (Velázquez, 2025). The Badan Siber dan Sandi Negara (2025), for example, recorded

approximately 3.64 billion anomalous cyberattack activities in Indonesia between January and July 2025. A notable example was the 2024 ransomware attack on the Pusat Data Nasional Sementara (PDNS), which disrupted hundreds of public services and exposed the continuing vulnerability of Indonesia's digital infrastructure. Yet, as recent scholarship suggests, the significance of these incidents lies not merely in the fact that cyberattacks are increasing, but in what they reveal about the structural limits of Indonesia's legal and institutional readiness to respond to cybercrime with transnational dimensions (Moise, 2024).

In the Indonesian context, prior studies have indeed examined cybercrime from different perspectives, but they remain relatively fragmented. Some scholars focus on the problem of jurisdiction and locus delicti, arguing that Indonesia's legal framework still lacks a sufficiently coherent basis for addressing cyber offences whose conduct and effects are dispersed across several states (Situmeang et al., 2026). Other studies emphasize electronic evidence and cross-border investigation, showing that the effectiveness of cybercrime enforcement depends on the availability of rapid preservation, access, and disclosure mechanisms for data stored in foreign jurisdictions, something that Indonesian law and practice still struggle to provide (Davies & Kennedy-Mayo, 2026). Another strand of literature stresses the importance of international cooperation and institutional capacity, noting that Indonesia's cybercrime enforcement is hindered by limited technical expertise, fragmented coordination among institutions, and the absence of fully operational cooperation channels for transnational investigations (Efendi Tanjung et al., 2026). Taken together, these studies suggest that Indonesia's cybercrime problem cannot be reduced to the existence of cyber threats alone; rather, it concerns the adequacy of the country's legal framework, procedural mechanisms, and cooperative capacity for enforcing the law against transnational cybercrime.

One of the most important issues emerging from this literature is Indonesia's non-ratification of the Convention on Cybercrime (Budapest Convention). The Budapest Convention is widely regarded as the principal international legal instrument governing the criminalization of cyber offences, procedural powers relating to electronic evidence, and mechanisms for international cooperation in cybercrime investigations (Wicki-Birchler, 2020). It has become a global reference point because it does not merely define substantive cyber offences, but also provides a framework for expedited preservation of data, mutual legal assistance, and 24/7 points of contact that are crucial for transnational investigations(Moeso Novianto & Nur Arfiani, 2025). In Southeast Asia, this issue is particularly significant because the Philippines remains the only ASEAN member state to have ratified the Budapest Convention, having done so in 2018, whereas Indonesia and other regional states remain outside this legal regime. For that reason, the Indonesian case raises a broader legal question: to what extent does the absence of treaty-based integration into the Budapest framework affect Indonesia's ability to investigate, prosecute, and cooperate in addressing transnational cybercrime?

Despite the growing literature on cybercrime in Indonesia, at least two gaps remain apparent. First, existing studies tend to discuss jurisdiction, electronic evidence, institutional challenges, and the Budapest Convention in a separate and fragmented manner, rather than integrating them into a single analytical framework for understanding the structural obstacles to transnational cybercrime enforcement in Indonesia. Second, there remains limited research that systematically compares Indonesia and the Philippines in order to assess the practical implications of Indonesia's non-ratification of the Budapest Convention, particularly in relation to jurisdiction, procedural powers, and international cooperation. Most existing Indonesian studies stop at the normative argument that Budapest ratification is important, but do not sufficiently examine how treaty participation may affect domestic legal preparedness when compared with a regional state that has already ratified the Convention.

Based on these considerations, this article seeks to fill that gap by examining the structural obstacles faced by Indonesia in enforcing the law against transnational cybercrime and by comparing Indonesia's legal framework with that of the Philippines as a Budapest Convention state party. Accordingly, this study addresses two main research questions. First, what structural obstacles does Indonesia face in the enforcement of law against transnational cybercrime? Second, how does Indonesia's legal framework compare with that of the Philippines in addressing transnational cybercrime, and what are the implications of Indonesia's non-ratification of the Budapest Convention? By positioning Indonesia's cybercrime enforcement problem within the broader debates on jurisdiction, electronic evidence, and international cooperation, this article aims not only to explain the limitations of the current legal framework, but also to provide a more analytically grounded basis for policy reform in strengthening Indonesia's response to increasingly complex cyber threats.

Method

This study employs normative legal research (penelitian hukum normatif), focusing on the analysis of written legal norms, statutory regulations, and international legal instruments. The theoretical foundation of the study is Lawrence Friedman's Legal System Theory, which conceptualizes any legal system as operating across three interconnected dimensions: structure (the institutional architecture of law enforcement, including courts, police, and agencies), substance (the written norms, rules, and legislation), and culture (the attitudes, values, and practices of legal actors and the public toward the law). This theoretical framework is selected because it enables a multi-dimensional diagnosis of Indonesia's cybercrime enforcement barriers beyond the purely normative revealing that deficits exist not only in legislative texts (substance) but equally in institutional capacity (structure) and enforcement behavior (culture). This theoretical lens is applied consistently throughout the discussion to prevent the analysis from collapsing into descriptive narration.

Two research approaches are employed in combination. The statute approach examines the internal coherence of Indonesia's cyber legal framework and the gap between this framework and international standards established by the Budapest Convention. The comparative approach systematically contrasts Indonesia's legal framework and enforcement practice with that of the Philippines. The Philippines is selected as the comparator on the basis of structural equivalence: both states share archipelagic geography, comparable digital infrastructure development trajectories, civil law-influenced legal traditions, and analogous institutional challenges in transnational law enforcement. This equivalence justifies the comparison as analytically meaningful rather than administratively convenient.

The data used in this research consists of secondary data, comprising primary and secondary legal materials. Primary legal materials include national legislation such as Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 27 of 2022 on Personal Data Protection, Law No. 1 of 2023 on the Criminal Code, and Law No. 1 of 1979 on Extradition. In addition, the study also draws on international legal instruments such as the Budapest Convention on Cybercrime (2001), as well as Philippine national legislation, namely Republic Act No. 10175 (Cybercrime Prevention Act of 2012). Secondary legal materials consist of academic literature, including books, peer-reviewed journal articles, and reports from relevant official institutions concerning cybercrime and international cooperation.

The analytical technique employed is qualitative analysis using descriptive-analytical and comparative methods. Descriptive analysis is used to systematically outline the applicable legal framework, while comparative analysis is employed to identify differences and gaps

between the Indonesian and Philippine legal systems in the context of transnational cybercrime enforcement. Through this approach, the study is expected to provide a comprehensive understanding of structural weaknesses in the national legal system and to formulate recommendations based on international best practices.

Results and Discussion

Legal Framework of Cybercrime in the Indonesian Legal System

Cybercrime constitutes a criminal act committed through or against computer systems, networks, or electronic data, carried out by individuals or organized groups with the use of information technology as both the instrument and the target of the offense (Brenners, 2010). Satjipto Rahardjo observed that the development of cybercrime is causally linked to advances in information technology that have restructured social order (Hamzah, 2013). Within Friedman's Legal System Theory, the Indonesian response to cybercrime can be assessed across three dimensions simultaneously: the substantive dimension (the content and coherence of legislation), the structural dimension (the institutional capacity to enforce it), and the cultural dimension (the behavioral attitudes of enforcement actors). This tri-dimensional framework reveals that Indonesia's cybercrime enforcement deficit is not reducible to any single legislative gap.

At the substantive level, Indonesia's cyber legal framework is distributed across three principal instruments: UU ITE (Law No. 1 of 2024), UU PDP (Law No. 27 of 2022), and KUHP (Law No. 1 of 2023). Table 1 summarizes the distribution of relevant offenses across these instruments. Collectively, these instruments represent significant legislative progress. However, their coexistence without a unified overarching cyber law framework produces synchronization deficits that constitute a structural weakness in the substantive dimension of Indonesia's legal system. Four substantive gaps are identifiable through horizontal synchronization analysis

Table 1. Legal Framework of Cybercrime in the Indonesian Legal System

KUHP (Undang-Undang Nomor 1 Tahun 2023)	UU ITE	UU PDP
Forgery (Articles 391–400)	Distributing or disseminating, transmitting, or making illegal content accessible (Articles 27–29)	Obtaining or collecting personal data that does not belong to oneself with the intent to benefit oneself or another party, which may result in harm to the data subject (Article 67)
Theft (Articles 476–481)	Accessing another person's computer and/or electronic system by any means (Article 30)	Creating false personal data or falsifying personal data with the intent to benefit oneself or

		another party, which may result in harm to others (Article 68)
Fraud (Articles 492–510)	Illegal interception of electronic information and/or documents and other people's electronic systems (Article 31)	
Property Damage (Articles 521–526)	Altering, adding, reducing, damaging, deleting, transferring, or concealing (data interference) electronic information and/or electronic documents (Article 32)	
	Interference with electronic systems (system interference), causing them to function improperly (Article 33)	
	Facilitating prohibited acts, such as producing, selling, procuring for use, importing, distributing, providing, or possessing hardware or computer passwords (Article 35)	

Sources: Author's Compilation

From the perspective of Lawrence M. Friedman's legal system theory, the effectiveness of cybercrime enforcement cannot be assessed solely by the existence of criminal provisions. Rather, it depends on the interaction between legal substance, legal structure, and legal culture. This framework is particularly useful for examining Indonesia's response to transnational cybercrime because the principal challenge does not lie merely in whether cyber-related conduct has been criminalized, but in whether the substantive norms are sufficiently harmonized, whether the institutional and procedural framework is capable of operationalizing cross-border enforcement, and whether the legal culture of enforcement is adequately equipped to deal with the technologically sophisticated and transnational nature of cybercrime (Flora et al., 2023; Friedman, 1975). On this basis, the Indonesian cybercrime regime—primarily embodied in the Electronic Information and Transactions Law (UU ITE), the 2023 Criminal Code (KUHP 2023), and the Personal Data Protection Law (UU PDP) should not be read as a mere collection of statutory instruments, but as components of a broader legal system whose effectiveness depends on the coherence of norms, institutional readiness, and enforcement capacity.

At the level of legal substance, Indonesia has indeed established a normative basis for addressing cybercrime. UU ITE criminalizes a range of cyber-related conduct, including unauthorized access, illegal interception, interference with electronic systems, and unlawful content dissemination. It also adopts an extraterritorial orientation through Article 37, which allows Indonesian law to apply to conduct committed outside the national territory insofar as such conduct produces legal consequences for electronic systems under Indonesian jurisdiction (Suseno et al., 2025; Tobing & Fitria, 2026). However, from a Friedmanian

perspective, the issue is not simply whether cyber offences have been codified, but whether the substantive framework is sufficiently coherent and harmonized to support effective enforcement.

In this respect, Indonesia's substantive regulation of cybercrime remains only partially aligned with internationally recognized standards, particularly the Budapest Convention on Cybercrime. The Convention provides a more systematic taxonomy of cybercrime by distinguishing offences against the confidentiality, integrity, and availability of computer data and systems, computer-related offences, content-related offences, and copyright-related offences (Clough, 2014). By contrast, UU ITE adopts several cybercrime-related concepts in a dispersed and functionally fragmented manner, without constructing a comprehensive and internally coherent taxonomy. This lack of harmonization is not merely a drafting concern. The classificatory architecture of cybercrime matters because it determines the scope of criminalization, the clarity of enforcement mandates, and the extent to which domestic law can interoperate with international legal cooperation frameworks. Consequently, the Indonesian framework may appear normatively broad, yet it still produces substantive uncertainty regarding the treatment of attack vectors that are already clearly recognized in international cybercrime governance (Auliaurrahman et al., 2025). In Friedman's terms, this reflects a weakness in legal substance: the law has criminalized cyber-related conduct, but it has not yet done so through a sufficiently integrated normative structure capable of responding to evolving forms of transnational cyber offending.

A related problem concerns the incomplete synchronization between UU ITE and KUHP 2023. The issue is not simply the coexistence of multiple legislative instruments, but the absence of a clearly articulated doctrinal relationship between cyber-specific offences under UU ITE and the general principles codified in the new Criminal Code. Several cybercrime provisions remain insufficiently integrated with the broader framework of KUHP 2023, particularly in relation to sentencing principles, attempt, participation, and corporate criminal liability. This lack of normative coherence risks producing interpretive inconsistency in practice, especially where cybercrime involves collective actors, corporate entities, or transnational conduct requiring the simultaneous application of special and general criminal law regimes. Thus, the problem extends beyond legislative overlap; it reflects a deeper fragmentation in the substantive architecture of Indonesian criminal law, where cybercrime has not yet been fully situated within the broader framework of penal reform (Flora et al., 2023).

The more acute weakness of Indonesia's cybercrime regime lies in legal structure, particularly in the procedural and institutional mechanisms required to investigate and prosecute transnational cybercrime. While UU ITE recognizes electronic information and electronic documents as legally admissible evidence, this formal recognition has not been matched by sufficiently operational procedures for obtaining, preserving, and transferring digital evidence located outside Indonesian territory. In transnational cybercrime cases, the decisive issue is not merely whether electronic evidence is legally valid in abstracto, but whether law enforcement authorities possess the procedural tools necessary to secure that evidence before it is altered, deleted, or rendered inaccessible across borders.

Here, Indonesian law still lacks clear equivalents to several mechanisms central to the Budapest Convention framework, including expedited preservation of stored computer data, expedited disclosure of preserved traffic data, and regulated transborder access to stored computer data(Adinda et al., 2025). This creates a structural disconnect between the formal admissibility of electronic evidence and the practical evidentiary capacity required in

cybercrime enforcement. In other words, the weakness does not lie in the absence of recognition of digital evidence, but in the absence of a procedural architecture capable of transforming that recognition into effective investigative and prosecutorial action. Studies on digital evidence in Indonesia have similarly noted the absence of a comprehensive chain of custody framework, disparities in technical competence among law enforcement agencies, and the underdevelopment of digital forensic protocols within criminal proceedings. From Friedman's perspective, this demonstrates a structural deficiency: the law exists, but the institutions and procedures necessary to implement it remain underdeveloped.

A similar structural problem is evident in the implementation of the Personal Data Protection Law (UU PDP). Normatively, UU PDP represents a significant step toward strengthening privacy protection and regulating data governance, while also introducing criminal sanctions for certain forms of unlawful data processing. Yet, the effectiveness of this regime cannot be assessed solely in terms of statutory enactment. Under Friedman's framework, the critical question is whether a functioning institutional structure exists to enforce those norms. At the time of writing, the personal data protection supervisory authority had not yet become fully operational. This is not a merely administrative delay; it constitutes a structural impediment with direct consequences for Indonesia's capacity to engage in cross-border data governance and enforcement cooperation. In transnational cybercrime cases involving data breaches, identity theft, or unlawful cross-border data processing, a supervisory authority should function as an institutional interlocutor for information exchange, investigative coordination, and mutual legal assistance. In the absence of such an operational body, Indonesia's data protection regime lacks one of the institutional preconditions for effective cybercrime governance (Auliaurrahman et al., 2025). Accordingly, the weakness of the Indonesian cybercrime regime is not confined to normative incompleteness; it also stems from the limited institutional infrastructure available to operationalize the law.

Although discussions of cybercrime regulation in Indonesia often focus on legislative reform, Friedman's third element—legal culture—suggests that enforcement effectiveness also depends on the values, practices, and professional orientations of the actors who implement the law. In the cybercrime context, legal culture encompasses the degree to which law enforcement agencies, prosecutors, judges, and regulatory authorities are prepared to treat digital evidence, forensic analysis, and cross-border technological coordination as integral components of criminal justice practice. This dimension is particularly relevant because cybercrime enforcement requires not only legal authority, but also a culture of technological literacy, inter-agency coordination, evidentiary discipline, and responsiveness to rapidly evolving modes of offending.

In Indonesia, the persistence of procedural uncertainty and institutional fragmentation indicates that legal reform has not yet been accompanied by a sufficiently adaptive enforcement culture. The uneven capacity of investigators to handle digital evidence, the absence of standardized forensic practices, and the limited operationalization of cross-border cooperation mechanisms all suggest that cybercrime is still not treated through a fully consolidated enforcement paradigm. This means that the challenge is not only one of statutory design or institutional architecture, but also of legal culture: a criminal justice system that remains largely oriented toward conventional offences will struggle to respond effectively to crimes that are technologically mediated, evidentially volatile, and jurisdictionally dispersed. In this sense, the Indonesian cybercrime regime illustrates one of Friedman's central insights—namely, that legal reform cannot be reduced to legislation alone, because the practical force of

law depends on whether institutions and legal actors internalize, operationalize, and consistently reproduce the norms embedded in the formal legal order.

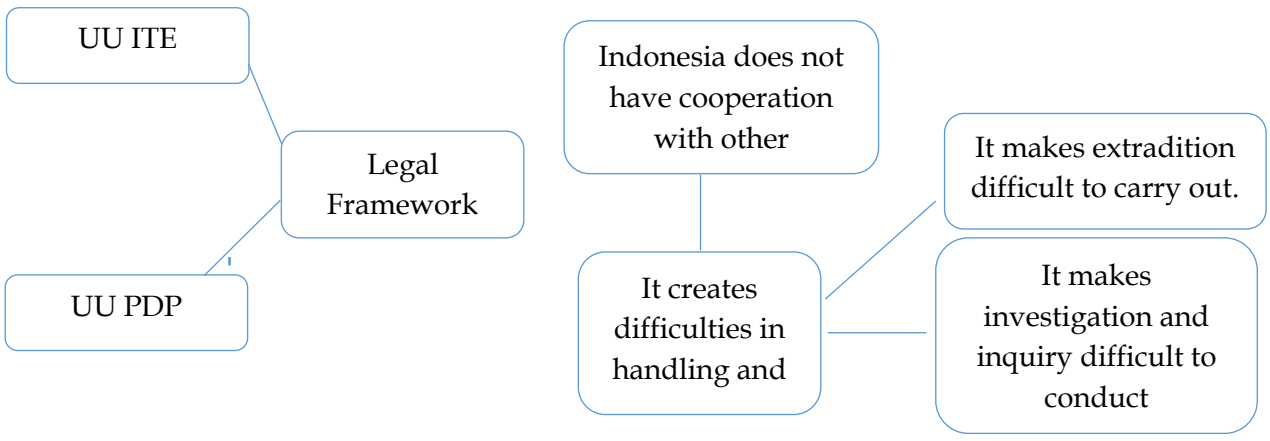
Taken together, these observations indicate that the main barriers to cybercrime enforcement in Indonesia cannot be reduced to the question of whether the country already criminalizes cyber-related conduct. The more fundamental issue is that Indonesia's response remains uneven across the three dimensions of Friedman's legal system. At the level of legal substance, the cybercrime framework remains only partially harmonized with international standards and insufficiently synchronized with the broader architecture of criminal law reform. At the level of legal structure, significant deficiencies persist in the procedural management of cross-border electronic evidence, the institutionalization of data protection oversight, and the technical capacity of enforcement bodies. At the level of legal culture, the transition toward a technologically responsive and internationally coordinated model of cybercrime enforcement remains incomplete.

Accordingly, cybercrime enforcement in Indonesia should be understood not merely as a matter of criminalization, but as a problem of systemic legal capacity. Future reform should therefore move beyond the expansion of offence provisions and focus instead on four interrelated agendas: (i) harmonizing substantive cybercrime regulation with internationally recognized standards; (ii) developing operational procedural mechanisms for cross-border electronic evidence; (iii) strengthening institutional structures, including the full operationalization of the personal data protection authority and digital forensic capacity; and (iv) fostering an enforcement culture capable of responding to technologically sophisticated and transnational forms of criminality. Only by addressing cybercrime through these interlocking dimensions of substance, structure, and legal culture can Indonesia move toward a more coherent and effective framework for transnational cybercrime enforcement.

Structural Challenges and Obstacles in the Enforcement of Transnational Cybercrime Law

Law enforcement against cybercrime as a transnational offense in Indonesia faces various complex structural obstacles, both from juridical, technological, and institutional aspects. The borderless nature of cybercrime means that its handling cannot rely solely on a national legal approach, but also requires regulatory harmonization and effective international cooperation. In practice, the UNODC (2013) notes that these various limitations indicate a gap between the complexity of cybercrime and the capacity of national legal systems to respond to it.

Image 1



Use of evidence

Sources: Author's Compilation

First, jurisdictional issues constitute the most fundamental challenge. Although Article 37 of UU ITE adopts the principle of extraterritorial jurisdiction, its implementation faces obstacles in determining locus delicti in cyberspace. Tobing and Fitria (2025; 2026) demonstrate that when perpetrators, victims, servers, and transit infrastructure are distributed across multiple jurisdictions, the territorial premise of Article 37 becomes legally indeterminate. This fragmentation is compounded by Indonesia's exclusion from the Budapest Convention's Article 29–35 mechanisms for expedited cross-border evidence preservation(Abdelkarim, 2025). Second, technological capability and digital forensic capacity limitations constitute significant investigative obstacles ENISA Threat Landscape (2023). Cybercriminals increasingly exploit VPNs, anonymous networks, and encrypted communications that require specialized forensic tools and trained personnel. This deficit is partially addressable through Budapest Convention capacity-building programs (GLACY+), but cannot be resolved by ratification alone as the Philippine experience demonstrates.

Third obstacles in extradition mechanisms further complicate law enforcement processes. Law No. 1 of 1979 on Extradition requires the existence of bilateral treaties as a basis for extradition implementation. In the context of cybercrime, the limited number of extradition treaties held by Indonesia—particularly with countries that serve as sources of cyberattacks—hinders the process of transferring offenders. This situation reduces the effectiveness of transnational law enforcement efforts, including coordination through Interpol (Bassiouni, 2014). The suboptimal state of international cooperation represents a systemic structural constraint. Although Indonesia has ratified the United Nations Convention against Transnational Organized Crime (UNTOC) through Law No. 5 of 2009, this convention does not specifically address cybercrime. On the other hand, Indonesia has not acceded to the Budapest Convention on Cybercrime (2001), which is the most comprehensive international instrument governing criminalization, procedural law, and international cooperation in the field of cybercrime (Sitompul, 2020). The absence of participation in this regime limits Indonesia's ability to access more effective international cooperation mechanisms, particularly in the exchange of electronic evidence and the coordination of cross-jurisdictional investigations (Ramadanti, 2024). Overall, these obstacles reflect a structural gap between the nature of cybercrime as a transnational offense and the readiness of Indonesia's national legal system. Therefore, comprehensive reform is required, not only in regulatory aspects but also in strengthening technological capacity, improving the quality of human resources, and fostering closer integration with international legal regimes.

The Budapest Convention: The Urgency of Ratification

Indonesia has not yet ratified the Budapest Convention, which has several strategic implications. In general, non-ratification limits Indonesia's access to standardized cooperation mechanisms, particularly the 24/7 network under Article 35, standardized evidentiary frameworks, and legal harmonization benchmarks (Marcén, 2024; N. A. Luhina & O. M. Paliukh, 2025; Velázquez, 2025). However, the ratification debate cannot be reduced to a

binary choice between accession and abstention. Article 32 of the Budapest Convention — which permits member states to access stored computer data in another state's territory without authorization under specified conditions (transborder access) — poses a genuine sovereignty risk. This provision effectively allows foreign law enforcement to access data stored on Indonesian servers without prior Indonesian authorization. The PDNS ransomware incident of 2024 has rendered this concern politically acute rather than merely theoretical, and its dismissal as a pretext for inaction reflects the analytical naivety this article seeks to correct.

Nevertheless, the ratification process is not without policy dilemmas. Several provisions, particularly those related to cross-border data access, may be perceived as potentially conflicting with Indonesia's digital sovereignty. Critically, Article 42 of the Budapest Convention provides a reservation mechanism that allows states to decline application of specific provisions — including Article 32. Indonesia should treat this mechanism not as insufficient justification for wholesale non-ratification, but as the principal instrument for reconciling Convention accession with sovereignty preservation. Developments in international law also demonstrate new dynamics through the United Nations. In 2020, the UN General Assembly established an Ad Hoc Committee to formulate a UN Convention on Cybercrime with a more inclusive scope. This Convention, adopted in 2024, includes stronger data sovereignty provisions and more explicit human rights safeguards than the Budapest Convention (Malikzada, 2026; Sarkar & Shukla, 2026). For Indonesia, the UN Convention represents a complementary — not alternative — accession pathway that should be pursued concurrently with, not instead of, Budapest Convention ratification.

The Philippines as a Comparative Lens for Assessing Indonesia's Cross-Border Cybercrime Enforcement Barriers

A comparison with the Philippines offers a particularly relevant lens for assessing Indonesia's readiness to address cybercrime as a transnational offence. The Philippines is the only ASEAN member state that has ratified the Budapest Convention on Cybercrime, having acceded in March 2018, and therefore provides a useful regional benchmark for examining how participation in an international cybercrime regime may shape domestic legal development and cross-border enforcement capacity. The comparison is analytically justified not merely by regional proximity, but by a degree of structural equivalence between the two jurisdictions: both are archipelagic states, have experienced rapid digitalization amid uneven infrastructure development, operate within legal systems influenced by civil law traditions, and face comparable institutional challenges in policing technologically mediated crime. These similarities make the Philippines an appropriate comparator for evaluating not only the potential advantages of accession to the Budapest Convention, but also the practical limits of treaty-based cybercrime governance in Southeast Asia.

From a normative and institutional perspective, the Philippines appears to have moved further than Indonesia in aligning its domestic cybercrime regime with international standards. This development is anchored in Republic Act No. 10175 (Cybercrime Prevention Act of 2012), which criminalizes a range of conduct broadly consistent with the Budapest Convention framework, including illegal access, illegal interception, data interference, system interference, and misuse of devices (Clough, 2014). More importantly, accession to the Budapest Convention has provided the Philippines with at least three concrete institutional advantages. First, it has gained access to the 24/7 cooperation network under Article 35, which facilitates expedited contact and coordination in cybercrime investigations involving cross-

border electronic evidence. Second, ratification has strengthened the harmonization of domestic cybercrime law with internationally recognized classifications and procedural expectations, thereby improving interoperability with foreign law enforcement and prosecutorial authorities. Third, membership has enabled the Philippines to participate in international capacity-building initiatives such as GLACY+, which provide technical training in digital forensics, cyber investigations, and the handling of electronic evidence for law enforcement personnel(Boudermine, 2025; Peters & Jordan, 2022; Sari, 2024). In contrast, Indonesia, as a non-party to the Convention, remains outside these institutional mechanisms and must rely more heavily on bilateral cooperation, Interpol channels, or ad hoc diplomatic arrangements, which are often slower and less effective in cases involving volatile digital evidence and rapidly moving cross-border data flows (Abdelkarim, 2025; N. A. Luhina & O. M. Paliukh, 2025).

Yet a comparative analysis that stops at these formal advantages would be incomplete. A more critical assessment reveals that the Philippine experience also illustrates the limits of equating treaty accession with enforcement effectiveness. Despite six years of Budapest Convention membership and the availability of international cooperation and capacity-building mechanisms, the Philippines has remained one of Southeast Asia's major hubs for cyber-enabled fraud and scam operations. Large-scale scam compounds operating from Philippine territory have reportedly targeted victims across Asia and generated substantial illicit proceeds, indicating that formal legal alignment and access to international mechanisms have not automatically translated into effective domestic suppression of organized cybercrime (Yiu-Chung Lau, 2025). This gap between formal legal advancement and enforcement outcomes is analytically significant because it exposes the limits of a purely normative reading of ratification. In other words, the Philippine case should not be treated as straightforward evidence that joining the Budapest Convention necessarily produces effective cybercrime governance; rather, it demonstrates that the value of ratification depends on the extent to which international legal commitments are supported by adequate prosecutorial resources, institutional integrity, and sustained political willingness to dismantle cybercriminal networks.

This point is particularly important when viewed through Lawrence M. Friedman's legal system theory. Ratification of the Budapest Convention may improve legal substance by encouraging the harmonization of domestic criminalization and procedural rules with international standards, and it may strengthen aspects of legal structure by expanding access to cooperation networks, mutual legal assistance channels, and capacity-building programs. However, treaty accession alone does not resolve the third dimension of Friedman's framework, namely legal culture—the attitudes, priorities, enforcement practices, and institutional integrity that determine whether the law is actually implemented effectively. The Philippine experience suggests that the central obstacle in cybercrime governance may lie less in the formal absence of legal instruments than in the persistent gap between law in the books and law in action. Where enforcement institutions remain under-resourced, vulnerable to corruption, or politically constrained in confronting organized cybercrime, the benefits of formal accession may be significantly diluted. Accordingly, the Philippine case should be read not as unqualified evidence in favour of ratification, but as a cautionary illustration that international legal integration, while important, does not by itself overcome deeper structural and cultural constraints within domestic law enforcement systems.

For Indonesia, this comparison yields at least three policy implications. First, ratification of the Budapest Convention should be understood as a necessary but not sufficient step in strengthening cybercrime enforcement. Accession may improve Indonesia's access to

cross-border cooperation mechanisms, procedural models for electronic evidence, and technical assistance frameworks, but these advantages will remain limited unless accompanied by domestic reforms in investigative capacity, prosecutorial coordination, and institutional accountability. Second, concerns regarding sovereignty particularly in relation to cross-border access to electronic evidence under the Convention—should not be used as a blanket justification for non-ratification. Rather, such concerns should be addressed through the Convention's reservation mechanisms and through careful domestic calibration of implementing legislation. Third, the Philippine experience confirms that the ultimate challenge in cybercrime governance lies not only in legal substance or legal structure, but also in legal culture. Enforcement attitudes, political commitment, inter-agency trust, and institutional integrity remain decisive variables in determining whether a state can translate formal legal integration into effective action against transnational cybercrime (Bunga, 2019).For that reason, Indonesia's debate on the Budapest Convention should move beyond the narrow question of whether ratification is desirable, and instead confront the broader issue of whether Indonesia's legal system—across the dimensions of substance, structure, and culture—is prepared to operationalize the obligations and opportunities that such ratification would entail.

Conclusion

This article has argued that the barriers to enforcing cross-border cybercrime in Indonesia cannot be understood solely as a problem of insufficient criminalization. Using Lawrence M. Friedman's legal system theory, the study demonstrates that Indonesia's enforcement deficits operate simultaneously across the dimensions of legal substance, legal structure, and legal culture. The persistence of jurisdictional complexity, limitations in digital forensic capacity, shortages of technically competent personnel, weaknesses in cross-border evidentiary mechanisms, and uneven international cooperation indicates that the problem is not merely legislative, but systemic. In this respect, the article contributes to the cybercrime literature by shifting the analysis away from a purely normative reading of Indonesia's legal framework toward a broader assessment of the institutional and cultural conditions that shape enforcement effectiveness.

The comparative analysis with the Philippines further refines this conclusion. The Philippine experience shows that accession to the Budapest Convention can generate meaningful formal advantages, including access to expedited cooperation networks, procedural harmonization, and international capacity-building mechanisms. At the same time, it also demonstrates that ratification does not automatically translate into effective enforcement outcomes. The continued prominence of the Philippines as a regional hub for cyber-enabled fraud underscores a central finding of this study: formal legal integration is important, but it is not self-executing. Without parallel improvements in institutional capacity, inter-agency coordination, and enforcement integrity, treaty accession alone is unlikely to resolve the deeper constraints of cross-border cybercrime governance.

On that basis, this study suggests that Indonesia's response to cross-border cybercrime should not be framed as a binary choice between ratification and non-ratification. Rather, ratification of the Budapest Convention should be approached as part of a broader reform agenda that includes harmonizing substantive cybercrime provisions with international standards, strengthening procedural mechanisms for cross-border electronic evidence, operationalizing the personal data protection supervisory authority, and investing in sustainable digital forensic and prosecutorial capacity. In policy terms, the value of ratification

lies less in symbolic alignment with global norms than in whether Indonesia is institutionally prepared to convert that alignment into effective enforcement practice.

At the same time, the article also recognizes its own boundaries. This study focuses on the legal and institutional barriers to cross-border cybercrime enforcement in Indonesia through a doctrinal-comparative approach, with the Philippines serving as a regional comparator. It does not examine the day-to-day implementation of cybercrime investigations through fieldwork, nor does it provide a quantitative assessment of case handling, prosecutorial outcomes, or the operational performance of Indonesian cybercrime units. Likewise, while the article addresses the implications of Budapest Convention ratification, it does not undertake a clause-by-clause analysis of the Convention's implementation requirements or a technical assessment of Indonesia's digital sovereignty architecture.

These limitations open several directions for future research. First, further studies should examine the implementation gap between cybercrime law in the books and cybercrime law in action through empirical research involving investigators, prosecutors, judges, and digital forensic practitioners in Indonesia. Second, comparative work should move beyond formal legal comparison and investigate how cybercrime cases are actually managed in practice in Convention member states such as the Philippines, particularly with respect to electronic evidence preservation, mutual legal assistance, and inter-agency coordination. Third, future scholarship should explore the interaction between cybercrime enforcement and data governance, including the institutional role of Indonesia's personal data protection authority in cross-border investigations. Finally, more focused doctrinal research is needed on the design of reservation clauses, procedural safeguards, and sovereignty protections that would allow Indonesia to engage with the Budapest Convention framework without compromising constitutional commitments to data control and legal oversight. By situating legal reform within these broader empirical and comparative agendas, cyber law scholarship can move beyond the question of whether Indonesia should ratify the Budapest Convention and toward the more important question of how Indonesia can build an enforcement system capable of making such ratification effective in practice.

References

Abdelkarim, Ya. A. (2025). UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age. *Journal of Digital Technologies and Law*, *3*(4), 543–569. https://doi.org/10.21202/jdtl.2025.22

Adinda, F. A., Rahmawati, E., Suparman, E., Arifin, R., & Ezzerouali, S. (2025). The Challenge of Admitting Electronic Evidence in Civil Procedure Law. *Jurnal IUS Kajian Hukum Dan Keadilan*, *13*(3), 656–680. https://doi.org/10.29303/ius.v13i3.1873

Auliaurrahman, A., Anshari, N., & Firdaus, S. U. (2025). The Existence and Regulation of Cyber Law: The Government's Role in Combating Digital Crime in Indonesia. *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan Dan Ekonomi Islam*, *17*(1), 206–223. https://doi.org/10.32505/jurisprudensi.v17i1.10612

Bassiouni, C. (2014). *International Extradition: United States Law and Practice. Oxford University Press.* Oxford University PressNew York.

Billow, J. (2024). No country is an island: Embracing international law enforcement cooperation to reduce the impact of cybercrime. *Journal of Cyber Policy*, *9*(2), 149–158. https://doi.org/10.1080/23738871.2023.2245417

Boudermine, M. (2025). *Finalization Of The United Nations Convention On Combating Cybercrime – Challenges And Opportunities Of Overcoming Them*. *62*, 156–173.

Brenners, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

Bunga, D. (2019). Legal Response to Cybercrime in Global and National Dimensions. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, *06*(01), 69–89. https://doi.org/10.22304/pjih.v6n1.a4

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). *SoK: Cross-border Criminal Investigations and Digital Evidence* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2205.12911

Clough, J. (2014). A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. *Monash University Law Review*, *40*, 698.

Davies, G., & Kennedy-Mayo, D. (2026). The promise and pitfalls of the Second Protocol to the Budapest Convention: Assessing its impact on EU and UK cross-border criminal investigations. *New Journal of European Criminal Law*, *17*(1), 101–123. https://doi.org/10.1177/20322844261419413

Efendi Tanjung, R., Ansyari Siregar, A., & Siahaan, N. (2026). Legal Analysis of Police Challenges in Facing Transnational Cyber Crime. *International Journal of Science and Environment (IJSE)*, *6*(1), 1217–1223. https://doi.org/10.51601/ijse.v6i1.392

ENISA. (2023). *Enisa Threat Landscape*. European Union Agency For Cybersecurity.

Flora, H. S., Thuong, M. T. H., & Erawati, R. D. (2023). The Orientation and Implications of New Criminal Code: An Analysis of Lawrence Friedman's Legal System. *Jurnal IUS Kajian Hukum Dan Keadilan*, *11*(1), 113–125. https://doi.org/10.29303/ius.v11i1.1169

Friedman, L. M. (1975). *Legal System, The: A Social Science Perspective*. Russell Sage Foundation. JSTOR. http://www.jstor.org/stable/10.7758/9781610442282

Hamzah, A. (2013). *Aspek-aspek Pidana di Bidang Komputer.* Sinar Grafika.

Malikzada, T. (2026). Assessing the Role of International Law in Regulating the Fight Against Cybercrime in the Digital Environment. *Futurity Economics&Law*, *6*(1). https://doi.org/10.57125/FEL.2026.03.25.01

Marcén, A. G. (2024). The Budapest Convention and the UN Cybercrime Convention negotiations. In A. Segura Serrano, *Global Cybersecurity and International Law* (1st ed., pp. 174–192). Routledge. https://doi.org/10.4324/9781003344124-10

Moeso Novianto & Nur Arfiani. (2025). KEJAHATAN SIBER DAN PERDAGANGAN DATA GELAP (DARK WEB): TANTANGAN HUKUM INDONESIA DALAM KONTEKS BUDAPEST CONVENTION. *Journal of Innovation Research and Knowledge*, *5*(7), 8249–8268. https://doi.org/10.53625/jirk.v5i7.11929

Moise, A. C. (2024). Procedural Aspects of the Second Additional Protocol to the Council of Europe Convention on Cybercrime. *Bulletin of the Transilvania University of Braşov. Series VII: Social Sciences • Law*, 189–196. https://doi.org/10.31926/but.ssl.2023.16.65.3.23

N. A. Luhina, & O. M. Paliukh. (2025). *Legal Challenges of International Cooperation in Combating Cybercrime: Prospects for Improving the Regulatory Framework*. https://doi.org/10.5281/ZENODO.15080178

Nicholas L Tobing, A., & Fitria, A. (2025). Jurisdiction and Locus Delicti of Transnational Cybercrime: A Normative Study Of International Law and Indonesian Telematics Law. *Interdisciplinary Social Studies*, *5*(1), 27–36. https://doi.org/10.55324/iss.v5i1.951

Peters, A., & Jordan, A. (2022). Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. *Center On National Security*.

Ramadanti, N. K. (2024). Strategi Pemberantasan Cybercrime Lintas Batas: Implementasi Mekanisme Mutual Legal Assistance berdasarkan Permenkumham Nomor 12 Tahun 2022. *Padjadjaran Law Review*, *12*(2), 184–195. https://doi.org/10.56895/plr.v12i2.1829

Sari, M. N. (2024). Cybercrime in Association of Southeast Asian Nations. *Journal of Information Policy*, *14*, 568–598. https://doi.org/10.5325/jinfopoli.14.2024.0016

Sarkar, G., & Shukla, S. K. (2026). *Policing Transnational Cybercrime: A Critical Assessment of the Anticipated Impact of the United Nations Convention against Cybercrime in India and Worldwide*. SSRN. https://doi.org/10.2139/ssrn.5899223

Sitompul, J. (2020). *Cross-border Access to Electronic Evidence: Improving Indonesian Law and Practice in Investigating Cybercrime*. Eleven International Publishing.

Situmeang, S. M. T., Kamilia, E. R., Lutfiyah, N., & Aurora, D. M. (2026). Enforcement of the universality principle in combating cybercrime as a transnational crime. *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*, *16*(1), 70–88. https://doi.org/10.35295/sz.iisl.2411

Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Aurellia Nathania Tiarma, B. (2025). Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences*, *11*(1), 2439543. https://doi.org/10.1080/23311886.2024.2439543

Tobing, A. N. L., & Fitria, A. (2026). LEGAL JURISDICTION AND PLACE OF OCCURENCE IN TRANSNATIONAL CYBERCRIME: A NORMATIVE ANALYSIS OF GLOBAL LAW AND INDONESIAN TELECOMMUNICATIONS REGULATIONS. *Awang Long Law Review*, *8*(2), 530–538. https://doi.org/10.56301/awl.v8i2.1894

UNODC. (2013). *Comprehensive Study on Cybercrime*. UNITED NATIONS OFFICE ON DRUGS AND CRIME.

Velázquez, H. L. C. (2025). *Strengthening Global Cooperation: International Legal Frameworks for Combatting Emerging Cyber Threats and Cybercrime*. Unpublished. https://doi.org/10.13140/RG.2.2.33288.94720

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*(1–2), 63–72. https://doi.org/10.1365/s43439-020-00012-5

Yiu-Chung Lau, L. (2025). *Cybercrime in Asia: Policing, Technological Environment, and Cyber-Governance in China and Vietnam*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-80213-3