Begawan Abioso
(Volume 17, Nomor 2, December 2026)
P-ISSN: 1858-2990 I E-ISSN: 2810-0727
Open access at: https://ejournal.hukumunkris.id/index.php/abioso

Combating Digital Transnational Organized Crime: Assessing the Effectiveness of Mutual Legal Assistance for Indonesia

[a] Gusti Rafi Muhammad*, [a] Siti Marwiyah, [a] Vallencia Nandya Paramitha, [a] Fathul Hamdani

[a] Faculty of Law, Universitas Dr. Soetomo, Surabaya, Indonesia

Submitted: 16-06-2026 | Revised: 04-08-2026 | Accepted: 09-08-2026 | Published: 10-08-2026

Abstract

Transnational Organized Crime (TOC) in the digital era has evolved into an increasingly complex global threat, characterized by the convergence of cyber fraud, underground banking, and virtual asset-based money laundering. In Indonesia, such criminal activities have resulted in substantial economic losses by exploiting cross-border jurisdictional gaps and weaknesses in domestic regulatory frameworks. This study examines the effectiveness of Mutual Legal Assistance (MLA) mechanisms under Law Number 1 of 2006 in addressing transnational cybercrime and evaluates the urgency of international legal harmonization. The novelty of this study lies in its specific examination of the structural incompatibility between Indonesia's traditional MLA mechanisms and the ontological characteristics of contemporary cybercrime involving cloud computing ecosystems, virtual asset-based underground banking, and the malware-as-a-service phenomenon. Employing a normative juridical method based on statutory and conceptual approaches, the study finds that conventional MLA mechanisms are no longer effective. This ineffectiveness fundamentally stems from a temporal asymmetry between lengthy MLA bureaucratic procedures, which may take months to complete, and the operational speed of digital crime, which can occur within seconds. Moreover, the rigidity of the dual criminality principle and the volatility of electronic evidence across jurisdictions further impede effective law enforcement. At the regional level, the ASEAN Mutual Legal Assistance Treaty is similarly constrained by the principle of non-interference and the absence of mechanisms for the immediate preservation of digital data. The study concludes that Indonesia urgently needs to accede to the *Budapest Convention on Cybercrime*. Such accession is crucial for overcoming jurisdictional barriers, facilitating the immediate exchange of digital evidence through the 24/7 Network, and curbing jurisdictional arbitrage by transnational criminal syndicates.

Keywords: *Budapest Convention*; Cybercrime; Jurisdiction; Mutual Legal Assistance; Transnational Organized Crime.

A. Introduction

The massive digital transformation that has unfolded since the beginning of the twenty-first century has created a highly interconnected and digitalized global order. At the same time, however, it has introduced new structural vulnerabilities that are increasingly being exploited in a systematic and organized manner by transnational criminal actors (Farhan et al., 2022). Transnational Organized Crime (TOC) is no longer confined to conventional physical activities, such as the smuggling of goods or traditional forms of human trafficking, but has increasingly expanded into the borderless realm of cyberspace (Rampadio et al., 2022). This emerging criminal architecture has adopted business models resembling those of global corporations, centered on the provision of criminal services, a phenomenon widely referred to in the cybersecurity literature as Crime-as-a-Service (CaaS) (Ashalirrohman, 2024).

* ✉ **Corresponding author:** gustirm04@gmail.com

Recent strategic reports issued by the United Nations Office on Drugs and Crime (UNODC) in 2024 and 2025 explicitly highlight a significant shift in the global threat landscape, in which cybercrime has increasingly converged with underground banking and technological innovations such as Artificial Intelligence (AI), deepfakes, and mass-produced social engineering schemes. Southeast Asia, particularly the Mekong region, has been identified by various international organizations as a major epicenter of this global "criminal service economy." In this region, organized criminal syndicates exploit illegal online gambling platforms, shell companies, and unregulated Virtual Asset Service Providers (VASPs) to generate and launder billions of dollars in proceeds derived from cybercrime while largely evading effective law enforcement (UNODC, 2024).

The consequences of this convergence of transnational cybercrime are particularly severe for developing countries with large digital populations, with Indonesia being at the forefront of such vulnerabilities. In Indonesia, the proliferation of cross-border cybercrimes—including online fraud, online gambling, exploitation of banking data, identity theft, and cryptocurrency-based money laundering—has reached an alarming level of penetration and poses a potential threat to the stability of the national financial system (Fauzia & Hamdani, 2021). Based on an analysis of empirical data from the first half of 2025 alone, transnational cybercrime syndicates are estimated to have caused direct economic losses to Indonesian citizens amounting to approximately IDR 3.2 trillion (Harahap et al., 2025).

The principal actors behind these crimes are located beyond the territorial jurisdiction of the Republic of Indonesia. They operate strategically through servers and from Special Economic Zones (SEZs) situated in foreign jurisdictions, such as Cambodia, the Philippines, and even the United Arab Emirates, deliberately exploiting jurisdictional gaps in Indonesia's domestic legal framework to evade local criminal prosecution (Martono et al., 2025). This jurisdictional asymmetry requires Indonesian law enforcement authorities, particularly the Indonesian National Police (*Kepolisian Negara Republik Indonesia* or Polri) and the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* or BSSN), to rely heavily on international cooperation mechanisms. Historically and doctrinally, the established legal mechanism for obtaining evidence and pursuing perpetrators located abroad has been Mutual Legal Assistance (MLA).

Within the discourse of international criminal law, the relationship between domestic law and global legal instruments can be assessed through the alignment between normative expectations (*das Sollen*) and empirical realities (*das Sein*) (Fachuda & Risma, 2025). At the level of *das Sollen*, international and domestic legal instruments have, in principle, established a formal operational framework for combating transnational organized crime (TOC). Indonesia ratified the United Nations Convention against Transnational Organized Crime (UNTOC) through Law Number 5 of 2009 and, more specifically, enacted Law Number 1 of 2006 concerning Mutual Legal Assistance in Criminal Matters (Martono et al., 2025). At the regional level, Indonesia is also a State Party to the 2004 *Treaty on Mutual Legal Assistance in Criminal Matters* (ASEAN MLAT), which doctrinally establishes a framework for interstate legal cooperation in Southeast Asia in addressing transnational crime (Jackson, 2016).

Under the prevailing principles of international law, the MLA mechanism is specifically designed to overcome territorial jurisdictional barriers, enabling law enforcement authorities to exchange critical evidence, trace and freeze proceeds of crime, and facilitate cooperation concerning the extradition of offenders between the requesting and requested States (Hamdani et al., 2023). From a normative standpoint, this legal framework appears sufficient

to provide a basis for cross-border cooperation involving the exercise of extraterritorial jurisdiction.

However, a closer examination of empirical realities (*das Sein*) reveals a profound and debilitating gap between the normative framework established by law and the actual effectiveness of law enforcement in cyberspace (Setiawan et al., 2026). Investigations into cross-border cybercrime frequently reach an impasse, ultimately resulting in the discontinuation of criminal investigations (Orias, 2019). The conventional MLA mechanism governed by Law Number 1 of 2006 remains burdened by bureaucratic obstacles, complex multilayered diplomatic procedures, and the absence of emergency communication channels. Globally, conventional MLA requests may take an average of 10 to 11 months merely to obtain access to a single piece of cryptocurrency transaction data or a server log held in a foreign jurisdiction (Busser, 2017).

In contrast, digital evidence is inherently volatile: it can be altered, overwritten, permanently deleted, or transferred across multiple cloud servers located on different continents within a matter of seconds (Martono et al., 2025). Furthermore, cross-border cybercrime enforcement initiated by Indonesian authorities frequently encounters the rigid application of the doctrine of state sovereignty by requested States, where requests for forensic assistance may be rejected outright due to the failure to satisfy the dual criminality requirement, particularly because not all jurisdictions have criminalized cryptocurrency-related fraud (Spicer, 2020). Consequently, even the most extensive measures available to Indonesian law enforcement authorities are often reduced to unilateral and largely passive administrative actions, such as blocking access to website content through the relevant communications authority or freezing domestic bank accounts. Such measures, however, do not provide Indonesian authorities with the capacity to apprehend and prosecute the principal actors behind these criminal operations who remain beyond Indonesia's territorial jurisdiction (Harahap et al., 2025).

This critical divergence between the expectations of *das Sollen* and the shortcomings of *das Sein* underscores the compelling need for the present study. Existing scholarship on transnational crime and the effectiveness of Mutual Legal Assistance (MLA) in Indonesia has generally been limited to conventional crimes involving a predominantly physical dimension. For comparative purposes, (Azizurrahman et al., 2023) examined the effectiveness of MLA in addressing human trafficking and migrant smuggling in geographical border areas. Similarly, (Apriansyah et al., 2024) evaluated the effectiveness of the ASEAN MLAT in combating conventional transnational crimes in general, without addressing the technical dimensions of digital forensics.

A normative study by (Qohirunnisa et al., 2026), meanwhile, examined jurisdictional sovereignty from a philosophical perspective, while other scholarship has explored MLA in relation to digital evidence at the global level without contextualizing it within Indonesia's legal architecture. More recent research by (Situmeang et al., 2026) has focused primarily on the dynamics of personal data protection and the transformation of normative pluralism within the Indonesian judicial system.

The distinctiveness, positioning, and novelty of this study lie in its specific focus on the structural incompatibility between Indonesia's traditional MLA mechanism, which is rooted in twentieth-century law enforcement paradigms, and the ontological characteristics of contemporary cybercrime involving cloud computing ecosystems, virtual asset-based underground banking, and the malware-as-a-service phenomenon. This study not only

critically examines the conceptual limitations of Law Number 1 of 2006 in addressing the spatial and temporal dimensions of the digital environment, but also compares Indonesia's current legal framework with the *Budapest Convention on Cybercrime* (2001), a global legal instrument specifically developed to address cybercrime and facilitate international cooperation in this field. Through this comparative analysis, the study seeks to formulate a concrete and actionable roadmap for reforming Indonesia's international legal cooperation framework, which may assist the Government of the Republic of Indonesia in addressing jurisdictional arbitrage in the enforcement of transnational cybercrime.

To achieve the intended depth of analysis, this study employs an integrated theoretical framework comprising three principal doctrines and concepts in international law and cyber law. First, the Theory of Extraterritorial Jurisdiction is employed to assess the extent to which a State may exercise its legal authority beyond geographical boundaries in pursuing intangible evidence located in cyberspace. Second, the doctrine of *aut dedere aut judicare*, a fundamental principle of international criminal law, establishes an obligation for a sovereign State to extradite an alleged perpetrator of an international crime present within its territory or, alternatively, to prosecute that individual under its domestic law (Harahap et al., 2025). Third, the concept of Digital Sovereignty represents an ambivalent framework: on the one hand, it is invoked by developing countries to protect their citizens' data from foreign intervention; on the other hand, it may serve as a legal shield for States functioning as safe havens to reject extradition requests (Fidler, 2025). These three theoretical perspectives are integrated into a unified analytical framework to examine the underlying factors contributing to failures in cross-border cybercrime enforcement, as further elaborated in the Results and Discussion section.

Building on the factual and theoretical gaps identified above, this study is guided by three primary research objectives. First, it seeks to critically examine the operational effectiveness of the existing Mutual Legal Assistance (MLA) mechanism and identify the structural barriers to its implementation under the current national legal framework, particularly Law Number 1 of 2006, and relevant regional instruments in addressing transnational cybercrime. Second, it aims to establish the urgency of international legal harmonization by specifically evaluating the prospects, implications for State sovereignty, and strategic benefits of Indonesia's accession to the *Budapest Convention on Cybercrime* as a means of strengthening the prevention and enforcement of transnational organized crime in the digital era. Third, the study seeks to formulate an appropriate framework or model for reconstructing Indonesia's MLA mechanism.

Accordingly, this study addresses the following research questions: (1) What are the structural and operational challenges associated with the implementation of Mutual Legal Assistance in the context of cyber jurisdiction in Indonesia? (2) How urgent is international legal harmonization for optimizing the ASEAN MLAT, and what are the prospects for Indonesia's accession to the *Budapest Convention on Cybercrime*? (3) What reconstruction model should be developed for Indonesia's MLA mechanism to support the reform of Law Number 1 of 2006 and accelerate the preservation of digital evidence?

B. Research Methodology

This study employs a normative legal research approach, which is primarily based on library-based legal research, the systematic examination of positive legal norms and doctrinal principles, and the synchronization of national and international legal instruments (Marzuki,

2014). The selection of this methodology is grounded in the identified disharmony and normative void between existing criminal procedural law and conventional Mutual Legal Assistance (MLA) mechanisms, on the one hand, and the demands associated with the rapid handling and preservation of digital evidence, on the other (Martono et al., 2025). It is important to emphasize that this study does not seek to assess empirical effectiveness in practice, given the inherent limitations of normative legal research in measuring sociological variables. Rather, the analysis is specifically directed toward assessing the normative adequacy of Indonesia's Mutual Legal Assistance (MLA) framework under Law Number 1 of 2006 and the regional ASEAN MLAT in responding to the distinctive ontological characteristics of transnational cybercrime.

To provide a comprehensive analysis of the research problems, this study combines three principal approaches: the statute approach, the conceptual approach, and comparative legal analysis (Muhaimin, 2020). Through the statute approach, the study examines the adequacy, completeness, and consistency of the legal norms contained in Law Number 1 of 2006, the Electronic Information and Transactions Law (ITE Law), and the law ratifying the United Nations Convention against Transnational Organized Crime (UNTOC). The conceptual approach is employed to examine relevant doctrines and concepts of international criminal law, including extraterritorial jurisdiction, the principle of *aut dedere aut judicare*, digital sovereignty, the volatile nature of electronic evidence, and cloud forensics (Aksa et al., 2024). Meanwhile, comparative legal analysis is employed to compare the legal norms and operational mechanisms embodied in Indonesia's MLA framework, the ASEAN MLAT, and the *Budapest Convention on Cybercrime* (2001).

To assess the normative adequacy of the legal instruments under examination, this study employs four qualitative-doctrinal parameters: temporal adaptability, jurisdictional flexibility, digital evidence accessibility, and international interoperability. Temporal adaptability assesses the availability of legal provisions that enable immediate emergency measures, particularly expedited preservation, to address the volatility of digital evidence and prevent data loss through overwriting. Jurisdictional flexibility evaluates the adaptability of legal norms to distributed cloud computing environments without being constrained by differences in the legal characterization of offenses under the dual criminality requirement or by physical territorial boundaries. Digital evidence accessibility examines the existence of a legal basis for distinguishing between procedures governing access to or seizure of content data and those applicable to non-content data, including subscriber and traffic data, as well as the delegation of authority for direct access to Cloud Service Providers (CSPs). Finally, international interoperability assesses the extent to which domestic legal norms are harmonized with established international standards for cybercrime cooperation, including the requirement to maintain a 24/7 network of designated points of contact. Collectively, these four parameters provide the analytical framework for evaluating the capacity of Indonesia's existing MLA regime to address the distinctive characteristics of transnational cybercrime and cross-border digital evidence.

All primary and secondary legal materials are analyzed using a qualitative-prescriptive method through three complementary modes of legal reasoning: statutory interpretation, conceptual analysis, and comparative legal analysis. Statutory interpretation is conducted through grammatical, systematic, and teleological approaches to examine the explicit meaning of the provisions contained in Law Number 1 of 2006, particularly Article 7 concerning the dual criminality requirement, and to determine whether this legal framework remains fit for purpose in the contemporary ecosystem of crypto-assets and cloud

computing. Conceptual analysis is employed to examine the normative tension between the traditional doctrine of Westphalian sovereignty and the demands of borderless law enforcement in addressing transnational cybercrime. Comparative legal analysis is subsequently undertaken through a side-by-side mapping of the provisions of Chapter III of the *Budapest Convention on Cybercrime*, particularly Articles 29, 30, and 35, against the corresponding provisions of Law Number 1 of 2006 and the ASEAN MLAT. This comparative analysis is intended to identify normative gaps and formulate an appropriate model for the transferability of international best practices to support the reform of Indonesia's legal framework.

C. Results

The normative analysis, systematic interpretation, and comparative mapping of Law Number 1 of 2006, the 2004 ASEAN MLAT, and the 2001 *Budapest Convention on Cybercrime* reveal a significant deficiency in the normative adequacy of Indonesia's Mutual Legal Assistance (MLA) framework in responding to the ontological characteristics of transnational organized cybercrime. Based on the parameter of temporal adaptability, this study identifies a normative void in Law Number 1 of 2006, which contains no provisions governing expedited data preservation or the immediate preservation of digital evidence. In the absence of such a provisional preservation mechanism, requests for legal assistance must proceed through multilayered government-to-government (G2G) bureaucratic channels, with the process taking an average of 10 to 11 months. This temporal delay stands in stark contrast to the volatile nature of digital evidence within cloud computing ecosystems and Virtual Asset Service Providers (VASPs), where data may be automatically deleted or overwritten within a matter of days. Consequently, the integrity and continuity of the chain of custody may be compromised before a formal MLA request reaches the requested State.

From the perspective of jurisdictional flexibility and digital evidence accessibility, Law Number 1 of 2006 continues to apply the dual criminality principle rigidly under Article 7(a), requiring equivalence in the legal characterization of criminal offenses rather than focusing on the substance of the underlying conduct. This normative rigidity may provide a legal basis for authorities in requested States, including jurisdictions functioning as safe havens, to refuse MLA requests involving cryptocurrency fraud or malware-as-a-service schemes that have not been uniformly criminalized under their respective domestic laws. Furthermore, Indonesia's domestic legal framework does not yet establish distinct procedural rules for the handling of content data and non-content data, including subscriber and traffic data. Nor does it provide a clear legal basis for domestic investigators to employ a Direct-to-CSP Request mechanism, whereby non-content data could be requested directly from foreign Cloud Service Providers (CSPs) without having to navigate the complexities of the formal MLA process.

At the comparative level, the analysis of the 2004 ASEAN MLAT reveals similar structural limitations within the regional legal framework. The treaty does not provide a specific protocol for the emergency preservation of digital evidence and, in practice, its implementation is frequently constrained by the principle of non-interference and the requirement for political consensus among ASEAN Member States. These constraints ultimately impede the timely handling of cross-border online fraud cases in Southeast Asia. By contrast, an examination of the 2001 *Budapest Convention on Cybercrime* demonstrates the existence of more developed operational mechanisms under Chapter III that could address several normative gaps in Indonesia's domestic legal framework. The Convention provides

for expedited preservation mechanisms under Articles 29 and 30, including the expeditious preservation and disclosure of stored computer data and traffic data; permits limited forms of trans-border access to stored computer data under Article 32; and mandates the establishment of a 24/7 Network under Article 35, requiring designated points of contact to remain continuously available to provide immediate assistance in cybercrime investigations and the collection of electronic evidence. Collectively, these mechanisms provide an accelerated channel for international cooperation that can reduce reliance on traditional diplomatic procedures when responding to urgent cybercrime-related requests.

D. Discussion

D.1 Structural and Operational Challenges in Implementing Mutual Legal Assistance within Indonesia's Cyber Jurisdiction

The emergence of the digital era and the expansion of the Internet as a global domain of interaction have fundamentally challenged the classical legal understanding of the locus of crime, or *locus delicti* (Anggara et al., 2025). Within the conventional paradigm of international criminal law grounded in the Westphalian conception of sovereignty, the principle of territorial jurisdiction recognizes a State's sovereign authority to investigate, prosecute, and punish offenses committed within its physical territory (Qohirunnisa et al., 2026). Cloud computing architecture and cyber networks, however, operate across and increasingly blur conventional geographical boundaries.

Transnational cybercrime consequently creates complex jurisdictional anomalies that complicate the determination of *locus delicti*. A perpetrator may, for example, be physically located in a hotel room in Dubai, within the jurisdiction of the United Arab Emirates, while deploying a botnet or malware rented from a criminal syndicate operating along the Myanmar border, routing data anonymously through temporary proxy servers located in Ireland, and ultimately siphoning billions of Indonesian rupiah from the bank accounts of customers in Jakarta. Such a scenario simultaneously implicates multiple jurisdictions based on the physical location of the perpetrator, the technological infrastructure employed, and the location where the harmful effects of the offense materialize.

In circumstances characterized by such extreme territorial fragmentation, international legal discourse, including the Tallinn Manual 2.0, recognizes the possibility of concurrent or overlapping jurisdiction based on multiple jurisdictional connecting factors, including the location of relevant infrastructure, the physical location of the perpetrator, and the place where the effects of the criminal conduct occur under the principle of objective territoriality (Tobing & Fitria, 2026).

Irrespective of the academic debate over the allocation of jurisdiction, operational realities indicate that transnational organized crime (TOC) syndicates are acutely aware of these overlapping regulatory frameworks. They strategically exploit such inconsistencies through a form of legal evasion commonly referred to as jurisdictional arbitrage. In this context, jurisdictional arbitrage refers to a deliberate strategy whereby cybercriminals locate their command centers and operational infrastructure, including command-and-control (C2) servers, in jurisdictions characterized by weak cybercrime legislation, the absence of bilateral extradition treaties, or governmental regimes unwilling to cooperate in providing international legal assistance (Tanjung et al., 2026). This criminal landscape renders cross-border cybercrime enforcement heavily—and, in certain circumstances, almost exclusively—dependent on the effectiveness of Mutual Legal Assistance (MLA) mechanisms.

For Indonesia, the principal legal framework and procedural foundation governing the transmission of requests for international legal cooperation are established under Law Number 1 of 2006 concerning Mutual Legal Assistance in Criminal Matters (Suharyo, 2010). Administratively and institutionally, this legislation designates the Ministry of Law and Human Rights of the Republic of Indonesia (*Kementerian Hukum dan Hak Asasi Manusia* or Kemenkumham) as the Central Authority. In this capacity, the Central Authority is responsible for verifying, approving, and transmitting requests for legal assistance submitted by domestic investigative authorities, including the Cybercrime Directorate of the Criminal Investigation Agency of the Indonesian National Police (Bareskrim Polri), to requested States, as well as processing incoming requests from foreign jurisdictions (Secretariat, 2014).

Although, in principle, this statutory framework is intended to facilitate cross-border cooperation in identifying perpetrators, searching or obtaining evidence from servers, freezing crypto-assets, and securing and repatriating electronic evidence relevant to criminal proceedings, its practical implementation in the contemporary global cybercrime landscape encounters a series of structural constraints that substantially impede effective law enforcement. Three major systemic anomalies and challenges illustrate the growing inadequacy of Indonesia's conventional MLA mechanism in responding to the operational dynamics of contemporary transnational organized cybercrime.

First, a fundamental weakness of the MLA framework in the cyber era lies in temporal asymmetry, namely the substantial disparity between the slow pace of bureaucratic procedures and the time required to transmit formal legal documents, on the one hand, and the speed at which digital transactions can be executed, on the other. Traditional MLA procedures were designed in the analog era, when requests primarily concerned the seizure of physical evidence, such as paper documents, or the apprehension of fugitives whose movements occurred within a considerably slower operational environment.

In Indonesia, an MLA request must be initiated by the police and subsequently submitted to the Central Authority at the Ministry of Law and Human Rights (Kemenkumham) for formal and substantive review. It is then transmitted through formal government-to-government (G2G) diplomatic channels via the Ministry of Foreign Affairs, generally by means of a diplomatic note, before being forwarded to the embassy of the requested State. The request is subsequently received by the foreign ministry of the requested State, reviewed by its competent judicial authority, and ultimately transmitted to the relevant local law enforcement authority for execution (UNODC, 2023).

This lengthy and multilayered bureaucratic process creates substantial delays that can severely undermine digital investigations. Based on compiled intelligence data and reports issued by international organizations across multiple regions, the average time required to execute and complete a conventional MLA request merely to obtain electronic communication logs or subscriber registration data from a service provider, such as a social media company or digital asset platform, ranges from approximately 10 to 11 months (Busser, 2017).

A striking contrast emerges in the operational dynamics of TOC syndicates, which increasingly employ algorithmic automation, botnets, smart contracts, and anonymity-enhancing technologies to facilitate their criminal activities. As comprehensively highlighted in the UNODC threat assessment published in October 2024 on the convergence of threats across Southeast Asia, multibillion-dollar criminal activities, including cyber-enabled fraud and technology-facilitated money laundering, increasingly rely on cryptocurrency transfers,

particularly stablecoins such as Tether (USDT), which offer substantial liquidity, channeled through high-risk Virtual Asset Service Providers (VASPs) with inadequate Know Your Customer (KYC) controls. Within this technological environment, the transfer of funds and the movement of crypto-asset ownership records can occur at extremely high speeds.

Moreover, by exploiting cryptographic obfuscation services such as crypto-mixers and techniques involving the transfer of assets across different blockchain protocols, commonly referred to as cross-chain hopping, perpetrators can rapidly launder and redistribute proceeds of crime in ways that substantially complicate manual transaction tracing, often within minutes of the underlying fraudulent activity (Rogers, 2024). By the time an Indonesian MLA request reaches the competent judicial authority of a requested State approximately ten months later, digital traces stored on temporary servers, in random-access memory (RAM), or in cache data may already have been automatically overwritten by service providers pursuant to relatively short data-retention policies. As a result, the critical investigative window—often characterized as the "golden hour" of digital forensics—may have already elapsed, significantly diminishing the possibility of preserving and reconstructing relevant digital evidence (Busser, 2017).

The substantial disparity between the lengthy bureaucratic response cycle of conventional MLA mechanisms and the rapid operational cycle of cybercrime can be systematically illustrated through the structural comparison presented in Table 1.

Table 1. Comparison of the Operational Characteristics of Conventional MLA and the Dynamics of Transnational Cybercrime

Operational Aspect	Conventional MLA Characteristics (Under Law Number 1 of 2006)	Characteristics of Transnational Cybercrime (TOC) Operations	Critical Implications for Law Enforcement
Execution Cycle Duration	The completion cycle is relatively lengthy, ranging from approximately 10 to 11 months and remaining highly dependent on bilateral diplomatic relations and cooperation.	Operations may occur at extremely high speeds, ranging from near-instantaneous execution to several minutes, particularly in crypto-asset transfers, cross-chain hopping, and cross-border data transmission.	The temporal disparity creates a substantial asymmetry between investigative procedures and criminal operations. Critical digital evidence may already have been deleted, manipulated, or automatically overwritten before the relevant legal assistance can be executed (Busser, 2017).
Communication Channels and Bureaucratic Procedures	Centralized and hierarchical, primarily operating through government-to-government (G2G) channels involving the Ministry of Foreign Affairs and formal diplomatic notes (UNODC, 2023).	Highly decentralized, involving end-to-end encrypted communications, no-log VPN services, and globally distributed cloud computing infrastructure (Martono et al., 2025).	The procedural structure significantly delays investigative responses, increasing the risk that Indonesian investigators will lose the critical window for identifying perpetrators, tracing IP-related evidence, and undertaking other time-sensitive investigative

			measures during the "golden hour" of digital forensics (Yasir, 2025).
Nature and Ontology of Evidence	The legislative framework was originally oriented toward procedures for obtaining, seizing, and transferring tangible physical evidence or authenticated documentary evidence.	Digital evidence is highly volatile, can be remotely altered without physical access, and may exist as ephemeral data in volatile memory or other forms of live data (Qohirunnisa et al., 2026).	Procedural integrity and the continuity of the chain of custody become increasingly vulnerable to disruption as delays increase, potentially undermining the admissibility and evidentiary reliability of digital evidence in judicial proceedings (Yasir, 2025).

Second, the effectiveness of cross-border cybercrime enforcement is significantly constrained by the rigidity of the dual criminality principle. As a long-established principle within extradition and mutual legal assistance regimes, dual criminality has also been incorporated into Indonesia's MLA framework, as expressly stipulated in Article 7(a) of Law Number 1 of 2006 (UNODC, 2023). This requirement operates as a mandatory precondition whereby the conduct under investigation in Indonesia must also constitute a criminal offense punishable under the law of the requested State (Spicer, 2020). In determining whether this requirement is satisfied, foreign authorities may assess dual criminality either in *abstracto* or *in concreto* by reference to their respective domestic criminal laws.

Within the fragmented architecture of global cybercrime law, the legal definitions of illegal access, misuse of devices, interference with electronic systems, and money laundering conducted through cryptocurrency proxies remain insufficiently harmonized and vary considerably across jurisdictions. In some jurisdictions, for example, disputes involving financial losses arising from fraud conducted through anonymous crypto-assets may be treated primarily as matters of civil liability or commercial contractual disputes rather than as serious criminal fraud. This divergence in legal interpretation can be strategically exploited by cybercriminals as part of broader jurisdictional arbitrage.

When Indonesia's Central Authority ultimately transmits a formal MLA request to a State identified as a cyber safe haven in which the perpetrators' command-and-control (C2) servers are located, the requested State may invoke its domestic legal framework and sovereign authority to refuse the request on the ground that the underlying conduct does not satisfy the dual criminality requirement. Analytical studies have further indicated that substantive differences among domestic legal frameworks, as well as difficulties in establishing equivalent elements of criminal intent (mens rea) across jurisdictions, may constitute significant grounds for refusing the execution of MLA requests. Such refusals can abruptly disrupt an international investigation that may already have required months of procedural coordination (UNODC, 2025).

The continuing requirement to establish compliance with dual criminality may therefore create a substantial structural obstacle to cross-border cybercrime enforcement. In practice, this constraint may provide transnational organized cybercrime actors with a degree of jurisdictional protection, particularly where they deliberately locate their network

infrastructure in jurisdictions characterized by underdeveloped technological regulation, institutional corruption, or permissive approaches to the movement and concealment of illicit capital (Qohirunnisa et al., 2026).

Third, another significant challenge undermining the effectiveness of transnational cybercrime enforcement within Indonesia's jurisdiction arises from the jurisdictional fragmentation of digital evidence and the complexities of cloud forensics. Modern data-storage systems relying on cloud computing architecture inherently involve the fragmentation, replication, and distribution of data across infrastructure located in multiple legal jurisdictions, primarily to enhance data security, availability, and redundancy. This technological architecture substantially complicates the identification of the jurisdiction in which particular digital evidence is legally or physically located.

In practice, user identification data, connection traffic records, or end-to-end communication records associated with a hacker located in Central Asia and targeting the banking systems of victims in Indonesia may not necessarily be stored within a single country or even on a single continent. Such data may be managed and processed by a multinational Cloud Service Provider (CSP) legally incorporated and headquartered in the United States, while portions or replicas of the underlying data may be simultaneously backed up on servers located in Ireland or stored in high-performance data centers in Singapore. Such geographically distributed infrastructure may be employed to optimize operational efficiency, reduce cooling-related energy consumption, enhance data redundancy, and minimize server transmission latency (Akilal & Kechadi, 2025).

At the level of legal enforcement, the Indonesian National Police lack the sovereign authority and extraterritorial jurisdiction necessary to compel multinational Cloud Service Providers (CSPs) operating in foreign jurisdictions to disclose sensitive user data. Such disclosure generally requires a legally recognized cross-border production or seizure order executed through formal and reciprocal MLA mechanisms (Martono et al., 2025). In contrast to the lengthy nature of conventional MLA procedures, cloud forensic investigations are highly time-sensitive and may require coordinated, confidential, and expedited access to digital evidence without prior notification to the account holder, consistent with a no-tip-off approach.

By the time Indonesian investigators have completed the multilayered MLA process and obtained authorization requiring a CSP to provide access to critical datasets—such as network traffic data, other forms of non-content transmission data, or Internet Protocol (IP) logs—the requested data may already have been removed from the relevant storage infrastructure. Such loss of evidence may occur not only because perpetrators affiliated with criminal syndicates actively erase traces of their activities using advanced secure data-erasure techniques, but also because CSPs may automatically and lawfully delete or overwrite data pursuant to their established data-retention policies. Consequently, the temporal mismatch between formal cross-border legal procedures and automated data-retention cycles may result in the irreversible loss of potentially critical digital evidence before investigators are legally authorized to obtain it (Hamid & Rasyid, 2025).

This series of interconnected constraints provides an important explanation for the persistently low and unsatisfactory prosecution and conviction rates in complex transnational cybercrime cases brought before Indonesian courts. In many cybercrime enforcement operations, the measures available to domestic authorities are ultimately limited to administrative interventions that are largely passive, defensive, and temporary in nature. Such

measures may include requesting the blocking of websites used to promote fraudulent investment schemes through the competent communications authority or ordering the freezing of domestic bank accounts suspected of being used to launder criminal proceeds through the Financial Services Authority (*Otoritas Jasa Keuangan* or OJK).

While these interventions may mitigate immediate harm, they remain limited in their capacity to achieve the broader objectives of criminal enforcement. This limitation reflects a more fundamental enforcement deficit, as Indonesian authorities continue to face significant jurisdictional constraints in tracing, apprehending, prosecuting, and ultimately seeking the extradition of the principal actors who organize and direct cybercriminal operations from foreign jurisdictions. Consequently, the individuals exercising strategic control over such operations may remain beyond the effective reach of Indonesia's domestic criminal justice system by exploiting the territorial sovereignty and jurisdictional protections of other States. (Harahap et al., 2025).

D.2 The Urgency of International Legal Harmonization: Optimizing the ASEAN MLAT and the Prospects of Accession to the *Budapest Convention*

Building on the preceding analysis of the effectiveness and enforcement capacity of Indonesia's domestic legal instruments, it is evident that a cybercrime enforcement strategy relying predominantly on domestic jurisdiction and conventional mutual legal assistance mechanisms is increasingly inadequate to address the inherently transnational and technologically dynamic nature of contemporary cybercrime. Substantial government investment in advanced technological infrastructure for cybercrime prevention and response, the enhancement of sophisticated cyber-forensic capabilities within the Criminal Investigation Agency of the Indonesian National Police (Bareskrim Polri), and the institutional development of the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* or BSSN) may yield suboptimal outcomes unless such measures are accompanied by corresponding reforms to Indonesia's international legal cooperation framework (Martono et al., 2025).

Accordingly, legal reform aimed at reducing bureaucratic constraints and overcoming jurisdictionally fragmented approaches to cross-border cybercrime enforcement should be structured around two complementary strategic pillars. The first involves optimizing the existing regional cooperation architecture under the ASEAN MLAT to facilitate more effective and timely legal assistance among ASEAN Member States. The second requires sustained political commitment to advancing Indonesia's accession to the *Budapest Convention on Cybercrime* as a global framework for cybercrime cooperation and electronic evidence. Together, these two pillars could strengthen the interoperability of Indonesia's domestic legal framework with regional and international mechanisms, thereby enhancing its capacity to respond to the increasingly complex and borderless nature of cybercrime.

At the regional level in Southeast Asia, Indonesia is a State Party to the *Treaty on Mutual Legal Assistance in Criminal Matters* (ASEAN MLAT), signed in late 2004. This multilateral instrument has been regarded by scholars and policymakers as an important milestone in establishing a regional framework for formal law enforcement cooperation and facilitating the exchange of information among Southeast Asian States. Over the course of its implementation, the ASEAN MLAT has contributed to cooperation in several strategic areas of transnational criminal enforcement, including counterterrorism, investigations into human trafficking networks, and efforts to disrupt cross-border narcotics trafficking (Apriansyah et al., 2024).

Nevertheless, extending the operational scope of the 2004 ASEAN MLAT to address the distinctive complexities of cybercrime investigations and digital forensics reveals significant structural and functional limitations. These limitations constrain the Treaty's capacity to respond effectively to the technological, temporal, and jurisdictional characteristics of contemporary transnational cybercrime.

The first fundamental limitation stems from the original design of the 2004 ASEAN MLAT, whose substantive provisions do not specifically establish an emergency mechanism for the immediate preservation and protection of volatile digital traffic data. In particular, the Treaty does not provide an expedited preservation protocol capable of securing vulnerable digital evidence before it is altered, overwritten, or deleted. This normative gap significantly limits the responsiveness of the regional MLA framework when dealing with time-sensitive electronic evidence in transnational cybercrime investigations.

The regional instrument was primarily designed as a general framework for mutual legal assistance in criminal matters and remains substantially dependent on the domestic substantive and procedural laws of the respective States Parties for the execution of requests. This dependence creates particular difficulties in the context of cybercrime enforcement because Southeast Asian States exhibit considerable differences in levels of cyber capacity, the development and architecture of domestic cybercrime legislation, and the underlying approaches to personal data and privacy protection. These regulatory disparities may complicate the timely and interoperable execution of cross-border requests involving digital evidence (Jackson, 2016).

Second, regional cooperation in Southeast Asia has historically operated within a political and institutional framework strongly influenced by the principle of non-interference, which emphasizes respect for the sovereignty and domestic affairs of individual Member States (Jackson, 2016). This principle has become deeply embedded in ASEAN's institutional culture and has reinforced a cautious approach to external intervention in matters falling within domestic jurisdiction. In addition, ASEAN's consensus-oriented decision-making practices may further constrain the speed and flexibility of regional responses when cross-border law enforcement operations require urgent coordination among multiple national authorities.

These constraints become particularly significant when Indonesian cyber intelligence and law enforcement authorities are required to respond rapidly to transnational online fraud networks operating across multiple jurisdictions. A prominent example concerns large-scale online romance and investment fraud schemes, including so-called *pig-butchering scams*, which have increasingly been associated with organized criminal networks operating from casino complexes, large-scale scam compounds, and Special Economic Zones (SEZs) in parts of the Mekong region. When Indonesian victims suffer substantial financial losses from such operations, effective investigation may require immediate coordination with authorities in the jurisdictions where the perpetrators, digital infrastructure, and financial assets are located. However, the procedural and bureaucratic structure of regional mutual legal assistance may delay such coordination, particularly where requests implicate politically sensitive issues of territorial sovereignty and domestic jurisdiction. Under these circumstances, the interaction between procedural requirements, consensus-oriented regional cooperation, and the principle of non-interference may constitute a significant legal and institutional obstacle to the timely enforcement of transnational cybercrime cases (U.S Department of State, 2025).

In light of these operational limitations, a roadmap for optimizing the ASEAN MLAT within the context of accelerating digital transformation should prioritize the development of a cyber-specific regional cooperation mechanism. Such reform could be pursued through an additional protocol or supplementary instrument to the existing ASEAN MLAT, or, at a minimum, through the establishment of a binding cyber-specific emergency cooperation framework coordinated within the relevant ASEAN cybersecurity institutional architecture, including the ASEAN Ministerial Conference on Cybersecurity (AMCC). This framework should be specifically designed to facilitate rapid and secure cross-border cooperation in cybercrime investigations and the preservation and exchange of electronic evidence.

A central component of this initiative would be the establishment of a trusted regional cooperation ecosystem capable of facilitating secure and expedited exchanges of digital evidence among competent law enforcement authorities in Southeast Asia. Such an arrangement could provide a specialized law-enforcement-to-law-enforcement (LE-to-LE) cooperation channel through which designated national authorities could communicate directly and securely in urgent cybercrime cases. By reducing dependence on multilayered diplomatic transmission procedures while maintaining appropriate legal safeguards and State sovereignty, this mechanism could strengthen the speed, interoperability, and operational effectiveness of regional cooperation in responding to transnational cybercrime.

This proposed emergency fast-track channel is expected to streamline the procedural complexities associated with the hierarchical and multilayered diplomatic transmission of conventional MLA requests. Rather than replacing the formal MLA framework in its entirety, the mechanism could function as an expedited channel specifically designed to facilitate emergency rapid preservation requests, enabling competent authorities to secure critical server metadata and other volatile electronic records immediately after a cyber incident is detected and before such data are altered, overwritten, or deleted (Harahap et al., 2025). The preserved data could subsequently be obtained through the applicable formal legal procedures, thereby reconciling the need for investigative speed with procedural safeguards and respect for State sovereignty.

Without a cohesive commitment among ASEAN Member States to reduce regional response times and institutionalize such expedited cooperation, Southeast Asia may remain particularly vulnerable to exploitation by transnational cybercriminal networks. Persistent procedural delays and fragmented legal frameworks may enable the region to function as an attractive operational and testing environment for professional hacking syndicates, cyber-enabled financial crime networks, ransomware operators, and organized groups engaged in cryptocurrency-related fraud and money laundering. Strengthening rapid preservation capabilities is therefore essential not only for improving the effectiveness of individual investigations but also for preventing regulatory and jurisdictional fragmentation from reinforcing the region's attractiveness to transnational organized cybercrime (UNODC, 2024).

Turning to the second strategic pillar, meaningful progress toward comprehensive international legal harmonization requires States to consider aligning their domestic legal frameworks and cross-border cooperation mechanisms with established global standards for combating cybercrime. In this context, particular attention should be given to the *Convention on Cybercrime*, developed under the auspices of the Council of Europe and opened for signature in Budapest in 2001, which has subsequently become widely known as the *Budapest Convention on Cybercrime* (Tropina, 2024). The Convention has developed into an influential

international legal framework for addressing cybercrime and facilitating cooperation concerning electronic evidence across jurisdictions.

The expanding geographical reach of the Convention also demonstrates its significance beyond the European regional context. By mid-2025, more than 80 States worldwide had become Parties to the Convention, reflecting its increasing acceptance across different legal systems and geographical regions. This broad participation underscores the Convention's role as an important reference point for the harmonization of substantive cybercrime legislation, procedural powers concerning electronic evidence, and mechanisms for international cooperation in cybercrime investigations.

The Convention's expanding membership extends beyond Europe and includes a substantial number of States with significant roles in the global economy and digital technology sector, including members of the G7 and the European Union. Its geographical reach has also expanded within Southeast Asia, with ASEAN Member States such as the Philippines becoming Parties to the Convention, while other regional States have progressively engaged with the *Budapest Convention* framework (Harahap et al., 2025). This broader participation illustrates the Convention's increasing relevance as a mechanism for facilitating cross-border cooperation on cybercrime and electronic evidence beyond its original European context.

In contrast, as of mid-2025, Indonesia had not become a Party to the *Budapest Convention on Cybercrime*. Indonesia's position therefore remained outside the Convention's formal treaty framework, despite the increasing importance of cross-border access to electronic evidence and international cooperation in addressing transnational cybercrime. This position highlights an important policy question concerning whether Indonesia should maintain its existing reliance on bilateral and regional cooperation mechanisms or move toward accession to the Convention as part of a broader strategy for harmonizing its domestic cybercrime framework with international cooperation standards (Harahap et al., 2025).

One of the most significant features of the *Budapest Convention on Cybercrime* lies in its framework for international cooperation, as established under Chapter III, particularly Articles 23 to 35. These provisions establish a structured legal framework for cross-border cooperation in cybercrime investigations and the collection and preservation of electronic evidence. Rather than merely reproducing conventional and often time-consuming channels of mutual legal assistance, Chapter III introduces mechanisms specifically designed to enhance the speed, responsiveness, and operational effectiveness of international cooperation in cases involving volatile digital evidence (Harahap et al., 2025).

A systematic interpretation of these provisions reveals several procedural mechanisms that could address important normative and operational gaps in Indonesia's existing MLA framework. These mechanisms are particularly relevant to the challenges identified in this study, including temporal asymmetry, jurisdictional fragmentation, limited access to electronic evidence, and the absence of expedited channels for urgent cross-border cooperation. If Indonesia were to accede to the Convention and incorporate the relevant procedural standards into its domestic legal framework, these mechanisms could strengthen the capacity of Indonesian law enforcement authorities to preserve, obtain, and exchange electronic evidence across jurisdictions in a more timely and interoperable manner. The principal mechanisms relevant to the reconstruction of Indonesia's MLA framework are examined below:

First, the establishment of the 24/7 Network under Article 35 of the *Budapest Convention* constitutes a key mechanism for facilitating expedited international cooperation in cybercrime investigations. Article 35 requires each Party to designate a point of contact that is available twenty-four hours a day, seven days a week, to ensure the provision of immediate assistance for investigations or proceedings concerning offenses related to computer systems and data, as well as for the collection of electronic evidence (Harahap et al., 2025). The designated contact point must possess the capacity to facilitate or directly provide urgent assistance within the scope of its domestic legal authority, thereby establishing a continuously available channel for time-sensitive cross-border cooperation.

For Indonesia, participation in such a network could substantially reduce the delays associated with reliance on conventional diplomatic communication channels. A designated Indonesian contact point could communicate rapidly with its counterpart in another Party when urgent assistance is required to identify the location of relevant digital infrastructure, preserve server logs, secure volatile electronic evidence, or facilitate other time-sensitive investigative measures. In this context, competent Indonesian cybercrime authorities, including the Cybercrime Directorate of the Criminal Investigation Agency of the Indonesian National Police (Bareskrim Polri), could use the 24/7 Network to initiate direct and expedited communication with designated foreign counterparts in jurisdictions where relevant perpetrators, service providers, servers, or electronic evidence are believed to be located. This mechanism would not eliminate formal MLA requirements where they remain legally necessary, but it could provide an essential preliminary channel for preserving evidence and coordinating urgent investigative assistance before conventional procedures are completed.

Such rapid cross-border coordination could enable Indonesian authorities to request the immediate preservation of critical digital evidence located in a foreign jurisdiction before volatile data are altered, transferred, overwritten, or permanently deleted. Through an expedited communication channel, competent authorities could promptly request their foreign counterparts to secure relevant server logs, traffic data, subscriber information, and other time-sensitive electronic records while the applicable formal legal procedures are being initiated or completed. This mechanism could substantially reduce the risk of evidentiary loss arising from the weeks or months otherwise required for multilayered verification, diplomatic transmission, and administrative processing through conventional MLA channels. Accordingly, the principal value of such expedited cooperation lies in its capacity to preserve the availability and integrity of digital evidence during the critical period between the detection of a cyber incident and the completion of formal cross-border legal assistance procedures.

Second, Articles 29 and 30 of the *Budapest Convention* provide an expedited framework for the preservation and disclosure of stored computer data and associated traffic data across jurisdictions. Article 29 establishes a mechanism through which a Party may request another Party to expeditiously preserve specified computer data stored within the latter's territory, particularly where there are grounds to believe that the data are especially vulnerable to loss or modification. This mechanism enables relevant electronic evidence to be secured while the requesting State undertakes the procedures necessary to obtain its subsequent disclosure through the applicable mutual assistance framework. Article 30 complements this mechanism by providing for the expedited disclosure of sufficient traffic data where necessary to identify another service provider and the State through which the relevant communication was transmitted.

These provisions represent an important procedural adaptation to the volatile nature of digital evidence. By separating the urgent preservation of data from its subsequent disclosure or production, the Convention enables competent authorities to secure potentially critical electronic evidence before it is altered, overwritten, transferred, or deleted, while preserving the legal safeguards applicable to access and disclosure. This approach is particularly relevant to stored computer data, server logs, subscriber-related records, and associated traffic data distributed across multiple jurisdictions. It therefore provides a mechanism for maintaining the availability and evidentiary integrity of digital records during the period required to complete formal cross-border legal procedures.

For Indonesia, the incorporation of comparable expedited preservation mechanisms could substantially mitigate the temporal asymmetry identified in the existing MLA framework. Rather than allowing volatile electronic evidence to disappear while formal requests proceed through lengthy bureaucratic and diplomatic channels, investigators could first seek its immediate preservation and subsequently pursue disclosure through the legally prescribed procedure. Such a framework could reduce the risk of evidentiary degradation and strengthen the continuity and reliability of the chain of custody in transnational cybercrime investigations (Busser, 2017).

Third, the harmonization of jurisdictional principles and the reinforcement of the doctrine of *aut dedere aut judicare* constitute an important dimension of international cooperation in addressing transnational cybercrime. Greater harmonization is required to establish a more consistent understanding of the scope and limits of jurisdictional authority in cross-border cybercrime enforcement, particularly where perpetrators, digital infrastructure, electronic evidence, and the harmful effects of criminal conduct are dispersed across multiple States. Such harmonization could reduce jurisdictional uncertainty and facilitate more coherent cooperation among States in determining their respective authority and responsibilities in investigating and prosecuting transnational cybercrime.

Within this framework, the doctrine of *aut dedere aut judicare* provides a relevant conceptual basis for strengthening accountability where alleged offenders are located outside the jurisdiction of the State primarily affected by the criminal conduct. The principle emphasizes that, where applicable under the relevant international legal framework, a State in whose territory an alleged offender is present should either extradite the individual to a competent requesting State or submit the case to its own competent authorities for prosecution. In the context of transnational cybercrime, reinforcing this principle could contribute to reducing jurisdictional safe havens by limiting opportunities for perpetrators to exploit territorial boundaries and differences among domestic legal systems to evade criminal accountability.

D.3 Reconstruction of Indonesia's MLA Framework: Reforming Law Number 1 of 2006 and Accelerating Digital Evidence Preservation

Building on the preceding analysis, this study proposes a Hybrid Fast-Track System for Indonesia's MLA Reform. The proposed model seeks to reconstruct the conventional mutual legal assistance framework by incorporating cyber-specific procedural mechanisms into the reform of Law Number 1 of 2006 while simultaneously establishing a domestic legal foundation for Indonesia's prospective accession to the *Budapest Convention on Cybercrime*. The model is designed to address the principal normative and operational deficiencies identified in the existing framework, particularly those concerning temporal asymmetry, expedited

preservation of digital evidence, cross-border access to electronic evidence, and international interoperability.

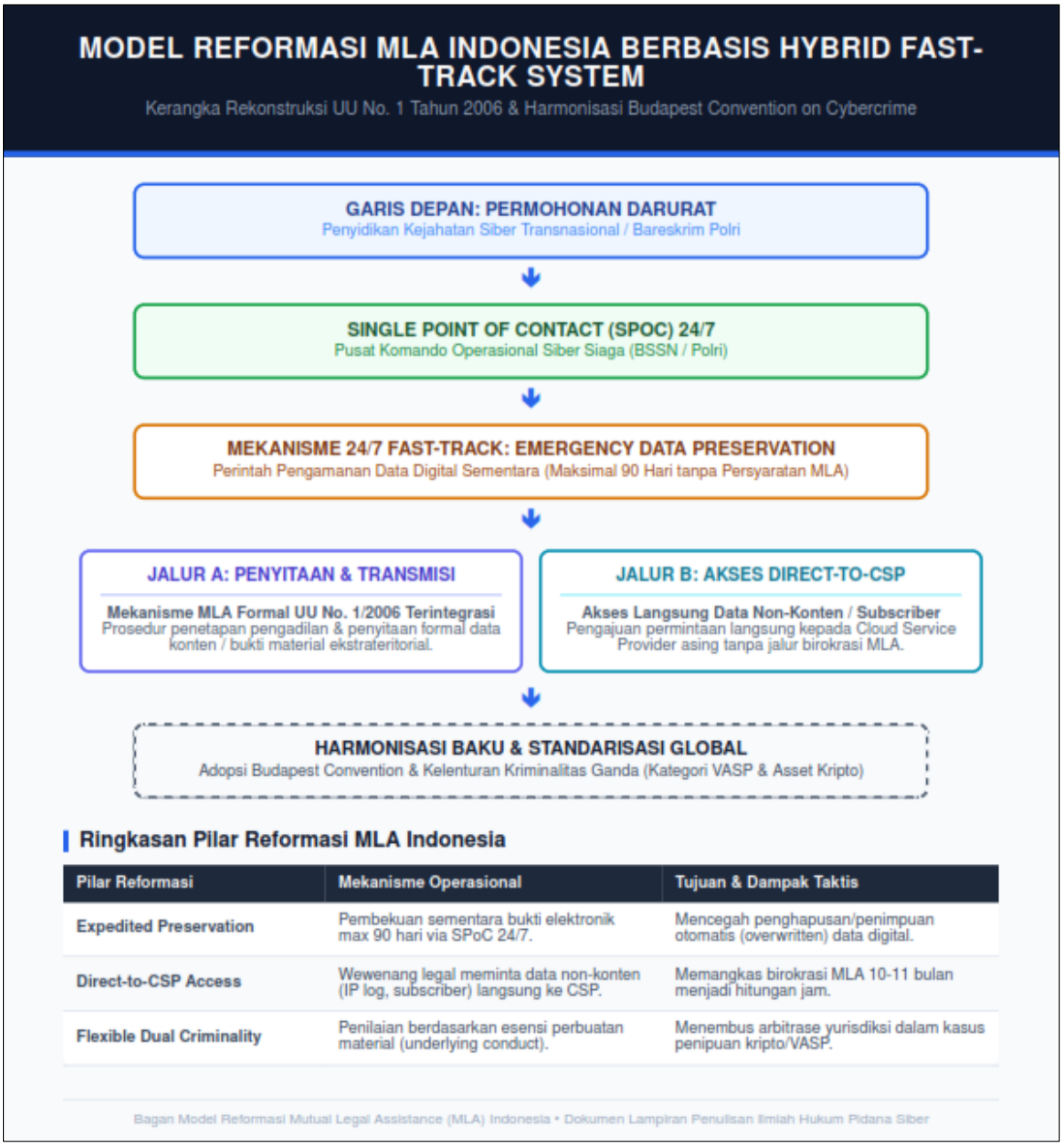

Figure 1. Hybrid Fast-Track System for Indonesia's MLA Reform

Source: Processed and developed by the authors with the assistance of artificial intelligence (AI) using Google Gemini.

a) Regulatory Reform Framework: Revision of Law Number 1 of 2006

The reform of Law Number 1 of 2006 should introduce a dedicated chapter on "Mutual Legal Assistance in Technology-Facilitated Crime and Electronic Evidence." The proposed normative framework should incorporate the following mechanisms:

1) Expedited Data Preservation. A new provision should authorize the Central Authority, or a designated Single Point of Contact (SPOC), to request the immediate preservation of traffic data and subscriber data held in a foreign jurisdiction before a

formal MLA request is submitted. The preservation order should remain effective for a maximum period of 90 days, thereby providing the requesting authority with sufficient time to prepare and transmit the formal MLA documentation required for subsequent disclosure or production of the preserved data.

2) Flexibility of the Dual Criminality Requirement. Article 7(a) of Law Number 1 of 2006 should be reconstructed so that dual criminality is assessed on the basis of the substantive equivalence of the underlying conduct rather than the identical legal classification or nomenclature of the offense in the requesting and requested States. In cases involving cryptocurrency-related money laundering or cyber-enabled fraud, the requirement should be regarded as satisfied where the underlying conduct is criminalized in substance under the laws of both jurisdictions, notwithstanding differences in statutory terminology or the constituent legal elements of the relevant offenses.

3) Direct-to-CSP Request Mechanism. The revised framework should establish a legal basis enabling competent Indonesian law enforcement authorities to submit requests directly to foreign Cloud Service Providers (CSPs) offering services within Indonesia for specified categories of non-content data, including IP logs, account identification information, and access-related records, without requiring the initial request to proceed through conventional diplomatic MLA channels. Such direct requests should remain subject to applicable domestic law, the law governing the CSP, data-protection requirements, and appropriate procedural safeguards.

b) Operational Legal Harmonization Matrix: Synergy between Law Number 1 of 2006 and the Budapest Convention

The following table presents the proposed operational harmonization framework between Indonesia's existing domestic legal framework, the proposed legislative reforms, and the relevant standards established under the *Budapest Convention on Cybercrime*.

Table 2. Operational Legal Harmonization Framework

Operational Issue	**Current Framework (Law Number 1 of 2006)**	**Proposed Reformulation (Revised MLA Law)**	***Budapest Convention*Standard**
Emergency Response	Reliance on multilayered government-to-government (G2G) bureaucratic channels involving the Ministry of Foreign Affairs and the Ministry of Law and Human Rights, with conventional MLA procedures potentially requiring 10–11 months.	Formal recognition of a 24/7 Network contact point as a specialized mechanism for urgent cybercrime cooperation within Indonesia's MLA institutional framework.	Article 35: Establishment of a 24/7 point of contact to ensure the provision of immediate assistance for cybercrime investigations and the collection of electronic evidence.

Volatility of Digital Evidence	No specific expedited mechanism for temporarily preserving volatile digital evidence before the completion of formal MLA documentation.	Introduction of an electronically transmitted Emergency Preservation Order that can be issued and processed within a maximum period of 2 × 24 hours.	Articles 29–30: Expedited preservation of stored computer data and expedited disclosure of preserved traffic data under the conditions prescribed by the Convention.
Dual Criminality	Dual criminality is applied rigidly, with emphasis on the legal classification or nomenclature of the relevant criminal offense.	A more flexible interpretation based on the substantive equivalence of the underlying criminal conduct rather than identical statutory terminology.	Harmonization of substantive cybercrime offenses, including illegal access, illegal interception, and system interference, to reduce disparities in criminalization across jurisdictions.
Access to Cloud-Based Evidence	Access to cloud-based evidence generally depends on conventional MLA procedures directed to the foreign jurisdiction in which the relevant data or service provider is located.	Establishment of a legal framework addressing extraterritorial jurisdiction and cross-border access to specified categories of cloud-based and electronically transmitted data, subject to appropriate legal safeguards.	Article 32: Limited trans-border access to stored computer data where the data are publicly available or where lawful and voluntary consent is obtained from a person legally authorized to disclose the data.

c) Accession Roadmap and Constitutional Implications

To operationalize the proposed framework, this study recommends that the Government of Indonesia adopt a phased roadmap combining administrative, legislative, and diplomatic measures:

1) Phase I (Short-Term/Pragmatic): Administrative and Institutional Preparation. The Government should establish a regulatory and operational framework, through an appropriate Presidential Regulation and/or ministerial regulation, governing Standard Operating Procedures (SOPs) for the emergency handling and preservation of cross-border electronic evidence. This phase should also include the designation of an appropriate national authority, potentially involving the National Cyber and Crypto Agency (BSSN) and/or the Criminal Investigation Agency of the Indonesian National Police (Bareskrim Polri), to perform the functions of a 24/7 Single Point of Contact (SPOC) for urgent cybercrime cooperation.
2) Phase II (Medium-Term/Legislative): Reform of the Domestic MLA Framework. The Government should prioritize the revision of Law Number 1 of 2006 through the National Legislative Program (*Program Legislasi Nasional* or Prolegnas). The revised legislation should incorporate a dedicated chapter addressing mutual legal assistance in cybercrime investigations, electronic evidence, and the digital-asset

ecosystem, including expedited preservation mechanisms and procedures for cross-border cooperation involving digital evidence.

Phase III (Long-Term/Diplomatic): Accession to the *Budapest Convention on Cybercrime*. Following the necessary domestic legal and institutional adjustments, Indonesia should pursue formal accession to the *Budapest Convention on Cybercrime*. Where legally permissible under the Convention, Indonesia may consider appropriate declarations or reservations to clarify the application of relevant provisions in accordance with its constitutional requirements, national data-sovereignty interests, and personal data protection framework. Any such measures should be formulated consistently with the reservation and declaration mechanisms permitted under the Convention and with Indonesia's constitutional and statutory framework, including the 1945 Constitution and the Personal Data Protection Law.

E. Conclusion

This study concludes that the conventional Mutual Legal Assistance (MLA) mechanism established under Law Number 1 of 2006 is increasingly inadequate to address the distinctive operational characteristics of Transnational Organized Crime (TOC) in cyberspace. This inadequacy stems primarily from three structural constraints. First, temporal asymmetry between lengthy MLA procedures and the rapid execution of cybercriminal activities creates a substantial risk that volatile digital evidence will be altered, overwritten, transferred, or deleted before formal legal assistance can be executed. Second, the rigid application of the dual criminality requirement may impede cross-border cooperation where the underlying cybercriminal conduct is classified or criminalized differently across jurisdictions. Third, the jurisdictional fragmentation of cloud-based evidence complicates the preservation, acquisition, and transfer of electronic evidence distributed across multiple States and service providers. At the regional level, the ASEAN Mutual Legal Assistance Treaty also exhibits limitations in responding to time-sensitive cybercrime investigations, particularly due to the absence of a dedicated expedited digital evidence preservation mechanism and broader institutional constraints affecting regional cooperation.

In response to these jurisdictional and procedural challenges, this study argues that Indonesia should seriously pursue accession to the *Budapest Convention on Cybercrime* as part of a broader strategy for reforming its international cybercrime cooperation framework. The Convention provides procedural mechanisms capable of addressing several deficiencies identified in Indonesia's existing MLA regime, particularly through the 24/7 Network under Article 35 and the expedited preservation and disclosure mechanisms established under Articles 29 and 30. These mechanisms could enable Indonesian authorities to secure volatile electronic evidence more rapidly while formal cross-border legal procedures are being completed.

Accordingly, international legal harmonization should be accompanied by the reconstruction of Indonesia's domestic MLA framework through the proposed Hybrid Fast-Track System, including expedited data preservation, a more conduct-based application of dual criminality, strengthened mechanisms for accessing cross-border electronic evidence, and institutionalized 24/7 cooperation. The integration of domestic legal reform, optimization of ASEAN-level cooperation, and prospective accession to the *Budapest Convention* could provide a more responsive and interoperable framework for overcoming jurisdictional fragmentation, reducing opportunities for jurisdictional arbitrage, and

strengthening Indonesia's capacity to investigate and prosecute transnational organized cybercrime.

References

Akilal, A., & Kechadi, M.-T. (2025). Cloud Digital Forensic Readiness: An Open Source Approach to Law Enforcement Request Management. *arXiv*.

Aksa, Hadiyanto, A., & Ciptono. (2024). Anti-Money-Laundering Efforts by the Financial Transaction Reporting and Analysis Centre Through International Cooperation. *Jurnal USM Law Review*, *7*(2), 586–602. https://doi.org/10.26623/julr.v7i2.8896

Anggara, R., Parlindungan, Y. O. S., & Yakin, B. A. (2025). The Principle of Legality in Cybercrime Investigation Based on the Electronic Information and Transactions Law. *Lex Journal: Kajian Hukum Dan Keadilan*, *9*(2), 344–363. https://doi.org/10.25139/lex.v9i2.10606

Apriansyah, M. I., Lestari, M. M., & Deliana, E. (2024). Efektivitas Asean Treaty on Mutual Legal Assistance (Amlat) dalam Menghadapi Kejahatan Transnasional di Negara Indonesia. *Jurnal Pro Justitia*, *5*(1).

Ashalirrohman, Y. (2024). Asset Forfeiture for the Offense of Illicit Enrichment: Between Eradication and Deterrence. *Lex Journal: Kajian Hukum Dan Keadilan*, *8*(1), 1–12. https://doi.org/10.25139/lex.v8i1.8771

Azizurrahman, Sy. H., Ismawati, S., Siagian, P., Had, A., Tahir, M., & Alkadri, Sy. M. R. R. M. (2023). The Early Warning System in Preventing Human Trafficking: Border (In) Security and Challenges for Indonesia. *Hasanuddin Law Review*, *9*(3). https://doi.org/10.20956/halrev.v9i3.4692

Busser, E. De. (2017). The Digital Unfitness of Mutual Legal Assistance. In *Security and Human Rights* (pp. 161–179). Brill Nijhoff. https://doi.org/10.1163/18750230-02801008

Fachuda, F. A., & Risma, S. S. A. (2025). Formulasi Tindak Pidana Ekosida dalam Hukum Pidana Nasional Urgensi Pembaruan Hukum di Era Krisis Lingkungan Global. *Jaksa: Jurnal Kajian Ilmu Hukum Dan Politik*, *3*(4), 1–16. https://doi.org/10.51903/72g3vs46

Farhan, Hamdani, F., Astuti, N. L. V. P., Fiqry, H. A. H., & Aulia, M. R. (2022). Reformasi hukum perlindungan data pribadi korban pinjaman online (perbandingan Uni Eropa dan Malaysia). *Jurnal Indonesia Berdaya*, *3*(3), 567–576. https://doi.org/10.47679/ib.2022264

Fauzia, A., & Hamdani, F. (2021). Analysis of the Implementation of the Non-Conviction-Based Concept in the Practice of Asset Recovery of Money Laundering Criminal Act in Indonesia from the Perspective of Presumption of Innocence. *Jurnal Jurisprudence*, *11*(1), 57–67. https://doi.org/10.23917/jurisprudence.v11i1.13961

Fidler, M. (2025). Fragmentation of International Cybercrime Law. *Utah Law Review*, *515*(3), 737–804. https://doi.org/10.63140/wez4rujib0

Hamdani, F., Asmara, M. G., & Zunnuraeni. (2023). Advancing Democratic Engagement in Indonesia's Treaty Ratification Process. *Rechtsidee*, *12*(2), 1–15. https://doi.org/10.21070/jihr.v12i2.1007

Hamid, H., & Rasyid, M. F. F. (2025). Criminal Policy in Combating Digital Banking Crime: Challenges and Prevention Strategies. *International Journal of Law and Society*, *2*(4), 96–106. https://doi.org/10.62951/ijls.v2i4.781

Harahap, N. K., Mangku, D. G. S., & Yuliartini, N. P. R. (2025). Addressing Online Fraud and Illegal Gambling as Cross Border Cybercrime through the Budapest Convention. *Journal of Innovative and Creativity*, *5*(3), 38542–38548.

Jackson, H. M. (2016). *ASEAN Cybersecurity Profile: Finding a Path to a Resilient Regime*. https://jsis.washington.edu/news/asean-cybersecurity-profile-finding-path-resilient-regime/

Martono, Akbar, M. G. G., & Rahmatiar, Y. (2025). Law Enforcement of Transnational Cybercrime: Case Study in Indonesia. *DE LEGA LATA: Jurnal Ilmu Hukum*, *10*(2), 279–286. https://doi.org/10.30596/dll.v10i2.24627

Marzuki, P. M. (2014). *Metode Penelitian Hukum*. Kencana Prenada Media Group.

Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram University Press.

Orias, M. (2019). Tindak Pidana Dunia Maya Berupa Virus dan Trojan Horse Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Lex Journal: Kajian Hukum Dan Keadilan*, *3*(1), 68–92. https://doi.org/10.25139/lex.v3i1.1820

Qohirunnisa, A. Z., Siregar, E. M. S., & Adinda, F. (2026). Law Enforcement Against Cybercrime from the Perspective of the Rule of Law. *Journal of Law, Politic and Humanities*, *6*(4), 2368–2377. https://doi.org/10.38035/jlph.v6i4

Rampadio, H., Fauzia, A., & Hamdani, F. (2022). The urgency of arrangement regarding illicit enrichment in indonesia in order to eradication of corruption crimes by corporations. *Jurnal Pembaharuan Hukum*, *9*(2), 225–241. https://doi.org/10.26532/jph.v9i2.17625

Rogers, S. (2024). Cyber-Fraud, Underground Banking, and Technological Innovation Fuels Crime in SE Asia. *Southeast Asia Grapples with Transnational Organized Crime in New UNODC Report*.

Secretariat, A. P. E. C. (2014). *Requesting Mutual Legal Assistance in Criminal Matters from Apec Economies: A Step-By-Step Guide*.

Setiawan, Y., Farida, A., & Hastuti, S. Y. (2026). Transformasi Digital Kejahatan Narkotika: Analisis Kriminologis dan Tantangan Penegakan Hukum Pidana di Era Cyber Narcotic. *Lex Journal: Kajian Hukum Dan Keadilan*, *10*(1), 38–55. https://doi.org/10.25139/lex.v10i1.11472

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

Spicer, J. (2020). *Mutual legal assistance in practice: Presentation for Indonesian anti-corruption officials*. https://baselgovernance.org/resources/news/mutual-legal-assistance-in-practice-presentation-for-indonesian-anti-corruption-officials-1808/

Suharyo. (2010). *Laporan Penelitian Penerapan Bantuan Timbal Balik dalam Masalah Pidana terhadap Kasus Kasus Cybercrime*.

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

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

Tropina, T. (2024). 'This is not a human rights convention!': The perils of overlooking human rights in the UN cybercrime treaty. *Journal of Cyber Policy*, *9*(2), 200–220. https://doi.org/10.1080/23738871.2024.2419517

United Nations Office on Drugs and Crime. (2024). *Billion-dollar cyberfraud industry expands in Southeast Asia as criminals adopt new technologies*. https://www.unodc.org/roseap/en/2024/10/cyberfraud-industry-expands-southeast-asia/story.html

United Nations Office on Drugs and Crime. (2025). *The Nexus Between Cybercrime and Corruption*.

United Nations Office on Drugs and Crime. (2023). *Electronic Evidence Fiche: Indonesia*. https://www.unodc.org/cld/uploads/pdf/El Evidence Hub/Electronic_Evidence_Fiche_as_8_February_2023_INDONESIA.pdf

U.S Department of State. (2025). United States Department of State Bureau for International Narcotics and Law Enforcement Affairs. *International Narcotics Control Strategy Report*, *2*, 1–305.

Yasir, M. (2025). The Position of Digital Evidence in the KUHAP Evidence System Normative Analysis and Implementation Challenges. *International Journal of Educational Review, Law and Social Sciences*, *5*(3), 3744–3751. https://doi.org/10.54443/ijerlas.v5i3.3852