

Cross-Border Cybercrime and Criminal Jurisdiction: Rethinking Indonesia's Extraterritorial Enforcement Framework

Kiki Pratiwi^{1*}, Edi Saputra Hasibuan², Diana Fitriana³

¹ Master of Laws Student, Faculty of Law, Universitas Bhayangkara Jakarta Raya

^{2,3} Lecturer, Faculty of Law, Universitas Bhayangkara Jakarta Raya

ABSTRACT: The decentralized architecture of cross-border cybercrime, where perpetrators, victims, data infrastructure, and digital evidence concurrently span multiple territories, routinely undermines traditional territoriality principles in criminal law. While Indonesia has expanded its domestic statutory reach through the Electronic Information and Transactions (ITE) Law, the New Penal Code (KUHP), the Criminal Procedure Code (KUHP), the Mutual Legal Assistance (MLA) Law, and the Personal Data Protection (PDP) Law, asserting prescriptive jurisdiction does not automatically confer enforcement authority abroad. Unauthorized extraterritorial investigative actions directly violate foreign state sovereignty. This article evaluates the systemic friction between Indonesia's expansive prescriptive frameworks and the strict territorial limitations governing cross-border evidence gathering and coercive maneuvers. Utilizing a normative-doctrinal method paired with a comparative statutory analysis, this study evaluates contemporary domestic laws against international legal instruments and foreign legal developments. To resolve jurisdictional conflicts, this article constructs a novel Digital Jurisdictional Nexus Test based on five distinct connecting factors: the locus of conduct, victimhood and localized harm, operational data infrastructure, national economic interest, and proximity to the data custodian or service provider. This framework clearly demarcates the legislative capacity to criminalize conduct from the procedural authority to seize electronic evidence globally. Consequently, the study introduces an operational Five-Stage Cross-Border Digital Investigation Protocol navigating nexus verification, sovereignty and comity assessments, evidentiary taxonomy, international cooperation channel selection, and judicial oversight. Finally, this paper evaluates the strategic implications of Indonesia's September 2026 signature of the United Nations Convention against Cybercrime, mapping out its potential to modernize mutual legal assistance frameworks ahead of its formal ratification and entry into force.

KEYWORDS: cybercrime jurisdiction, digital evidence, extraterritorial enforcement, Indonesia criminal law, UN cybercrime convention.

1. INTRODUCTION

The decentralized nature of contemporary cybercrime destabilizes the territorial paradigms that traditionally anchor criminal jurisdiction (Kusuma, 2025; Shurson, 2025; Tobing & Fitria, 2025). A singular digital incident routinely fractures geographical boundaries, involving an offender in one state, a target in another, data routing infrastructure across multiple transit points, and critical electronic evidence held by a service provider incorporated under a foreign legal system. This systemic fragmentation prevents any straightforward identification of the *locus delicti*, creating deep friction between a state's capacity to prescribe criminal law and its authority to execute investigative measures (Ryngaert, 2022; Shurson, 2025). The underlying crisis is not merely that digital misconduct evades physical borders, but that the conceptual ties determining legal jurisdiction have become structurally detached from the physical location of law enforcement mechanisms (MacNeil, 2026; Shurson, 2025).

This jurisdictional asymmetry necessitates a sharp doctrinal boundary between jurisdiction to prescribe and jurisdiction to enforce (Ryngaert, 2015, 2022). Prescriptive jurisdiction dictates a state's authority to subject specific conduct to its substantive criminal code, whereas enforcement jurisdiction governs the legitimate exercise of coercive sovereign power. In transnational digital investigations, these two concepts generate divergent legal boundaries (Shurson, 2025). A sovereign state may possess a legitimate national nexus sufficient to criminalize an extraterritorial offense, yet this substantive link does not generate an unfettered right to conduct coercive data seizures within a foreign territory. Current legal scholarship emphasizes that expanding prescriptive claims must not be conflated with the unauthorized projection of enforcement power across international borders (Arnell & Faturoti, 2023; Ryngaert, 2022).

This conflict has become a pressing institutional challenge for Indonesia following the rapid overhaul of its domestic penal architecture. The Electronic Information and Transactions (ITE) Law explicitly projects extraterritorial reach over specific digital actions, while the New Penal Code (KUHP) entered into formal effect on 2 January 2026 (Republic of Indonesia, 2008, 2023, 2024). Coupled with the procedural revisions under Law No. 20 of 2025 (the New Criminal Procedure Code/KUHAP) and the statutory adjustments under Law No. 1 of 2026, the post-2026 Indonesian legal landscape requires an immediate reassessment of how national criminal jurisdiction operates when an offense is digitally distributed across global networks (Republic of Indonesia, 2025, 2026).

The core dilemma for Indonesia is not the statutory formulation of an extraterritorial base to claim jurisdiction (Republic of Indonesia, 2008, 2024). The critical systemic challenge lies in operationalizing this jurisdiction when electronic evidence, intermediaries, physical infrastructure, or suspects reside abroad (Kusuma, 2025; Shurson, 2025). Digital prosecutions depend heavily on data held by transnational cloud providers, telecommunications conglomerates, social media platforms, and hosting intermediaries. As Shurson (2025) observes, digitally mediated investigations fundamentally disrupt the link between territorial sovereignty and investigative access to geographically dispersed data. Similarly, Sachoulidou (2024) demonstrates that securing cross-border electronic evidence forces public law enforcement into complex, non-traditional interactions with private corporate entities across different sovereign boundaries.

Indonesian legal scholarship has frequently evaluated transnational cyber threats through the lenses of concurrent jurisdiction, *locus delicti* ambiguities, and the structural inefficiencies of international cooperation (Kusuma, 2025; Tobing & Fitria, 2025). While these studies offer essential foundational perspectives on Indonesia's legal position, a critical analytical gap persists. Domestic literature has yet to establish a clear framework to separate a legitimate prescriptive nexus from the lawful execution of investigative authority when data custodians or evidence are located outside national boundaries (Kusuma, 2025; Shurson, 2025).

This article fills that gap by constructing a comprehensive Digital Jurisdictional Nexus Test. Rather than advocating for an unchecked expansion of Indonesian penal power over foreign cyber activities, this test establishes five specific connecting factors to determine if a digital incident maintains a substantial, lawful relationship with Indonesia:

- The exact locus of conduct
- The targeting of domestic victims and localized harm
- The utilization of domestic digital infrastructure
- The impact on national economic and security interests
- The physical or corporate proximity of the evidence and service providers

This analytical framework separates the evaluation of prescriptive jurisdiction from the execution of investigative enforcement. While the first four factors assess the substantive connection of the offense to Indonesia, the fifth factor isolates the distinct procedural question of how state actors can lawfully acquire data from transnational intermediaries. Maintaining this distinction is vital because a legitimate basis for domestic prosecution cannot serve as a unilateral license for cross-border enforcement maneuvers (Ryngaert, 2022; Shurson, 2025).

Consequently, this study delivers three primary theoretical and practical contributions to the field. First, it introduces a rigorous conceptual separation between prescriptive claims and investigative enforcement within the specific context of Indonesian cybercrime law. Second, it delivers the Digital Jurisdictional Nexus Test as a structured analytical tool for prosecutors and judges facing cross-border digital conflicts. Third, it operationalizes this nexus test into a practical Five-Stage Cross-Border Digital Investigation Protocol that integrates nexus verification, sovereignty and comity evaluations, evidentiary taxonomy, international cooperation channel selection, and mandatory judicial safeguards. Ultimately, this article advances a central thesis: the modernization of Indonesia's extraterritorial cybercrime framework must move away from simply expanding the geographical reach of its penal code, focusing instead on building a predictable equilibrium between jurisdictional legitimacy, enforcement limitations, international treaty compliance, and procedural due process (MacNeil, 2026; Shurson, 2025).

2. METHOD

This study adopts a normative-doctrinal legal research methodology complemented by a comparative law approach to analyze the architecture of Indonesia's criminal jurisdiction over cross-border cyber offences (Hutchinson, 2018; Hutchinson & Duncan, 2012; Van Hoecke, 2011). The normative framework serves to dissect the statutory foundations, systemic scope, and dogmatic limitations governing state action in digital enforcement. Through this lens, the study evaluates the structural friction

between prescriptive jurisdiction, which governs the authority to criminalize conduct, and enforcement jurisdiction, which dictates the executive capacity to deploy coercive procedural measures (Ryngaert, 2015, 2022). This conceptual division is critical when evaluating the legal validity of extraterritorial actions aimed at capturing electronic evidence located or controlled beyond national boundaries.

The primary legal materials consist of a synchronized matrix of Indonesian statutes regulating digital ecosystems, substantive criminal liability, procedural enforcement, international legal assistance, and data sovereignty. Specifically, the analysis evaluates the Electronic Information and Transactions (ITE) Law (Law No. 11/2008 as amended by Law No. 1/2024), the New Penal Code (KUHP) (Law No. 1/2023), the New Criminal Procedure Code (KUHP) (Law No. 20/2025), the Mutual Legal Assistance (MLA) Law (Law No. 1/2006), and the Personal Data Protection (PDP) Law (Law No. 27/2022) (Republic of Indonesia, 2006, 2008, 2022, 2023, 2024, 2025). The New KUHP entered into force on 2 January 2026 and replaced Law No. 8 of 1981, making the reference to “KUHP initiatives” in the original text outdated. Rather than interpreting these statutes in isolation, this study analyzes their systemic interaction to expose potential regulatory gaps and procedural conflicts in cross-border law enforcement.

To assess global structural alignments, this research incorporates international legal instruments dedicated to cybercrime and electronic evidence. Central to this evaluation is the Council of Europe Convention on Cybercrime (Budapest Convention), utilized as the benchmark for international standards on substantive criminalization, expedited data preservation, and mutual assistance channels (Council of Europe, 2001). Additionally, the study evaluates the United Nations Convention against Cybercrime, mapping its strategic implications for Indonesia’s evolving treaty obligations and future international cooperation frameworks (United Nations General Assembly, 2024).

The comparative legal approach analyzes selected foreign frameworks that regulate cross-border access to data custodians (Eberle, 2011). This includes the United States CLOUD Act, which establishes a data disclosure mechanism based on corporate possession, custody, or control, irrespective of the physical server location (Hemmings et al., 2020; United States Congress, 2018). It also examines European Union Regulation (EU) 2023/1543, focusing on the operational mechanics of European Production and Preservation Orders for electronic evidence (European Parliament & Council of the European Union, 2023; Sachoulidou, 2024). The Regulation expressly establishes mechanisms enabling competent authorities to order service providers to produce or preserve electronic evidence irrespective of the location of the data. Furthermore, the study analyzes Singapore’s Computer Misuse Act to evaluate how a regional common law jurisdiction utilizes specific connecting factors to codify its extraterritorial cyber reach (Singapore, 1993; Urbas, 2008).

This comparative analysis rejects the mechanical transplantation of foreign legal concepts into the Indonesian civil law tradition (Legrand, 1997). Instead, these jurisdictions serve as functional models to isolate alternative regulatory techniques regarding data access, service-provider obligations, and mandatory judicial oversight. The insights derived from these frameworks are synthesized to construct a localized legal architecture compatible with Indonesia’s constitutional and institutional realities.

Finally, the analytical matrix of this study is strictly doctrinal rather than empirical. It does not measure the quantitative frequency or operational metrics of domestic cyber investigations. Instead, it evaluates the internal coherence of existing legal norms to formulate structured propositions that align Indonesia’s cross-border enforcement capabilities with state sovereignty, international comity, and procedural due process (Hutchinson & Duncan, 2012; Van Hoecke, 2011).

3. INDONESIA’S EXTRATERRITORIAL CRIMINAL JURISDICTION IN CROSS-BORDER CYBERCRIME

3.1. *The Extraterritorial Dimension of the Electronic Information and Transactions Law*

Indonesia’s legislative departure from strict territoriality began with the enactment of the Electronic Information and Transactions (ITE) Law. This statutory framework decouples criminal liability from physical geography, explicitly recognizing that electronic conduct generates legal consequences independent of the actor’s physical locus (Republic of Indonesia, 2008, 2024). The extraterritorial reach of the ITE Law operates primarily through an effects-based doctrine, asserting jurisdiction over foreign-sourced digital activities that produce detrimental legal impacts within Indonesian sovereign territory or target domestic electronic systems (Kusuma, 2025; Tobing & Fitria, 2025).

The systemic value of this approach lies in its rejection of physical presence as the sole determinant of criminal jurisdiction in the digital ecosystem. A foreign threat actor can target Indonesian critical information infrastructure or execute financial cyber fraud against domestic victims without ever entering the state’s physical borders. Consequently, the primary legal inquiry shifts from

locating the perpetrator to evaluating whether the domestic effects of the foreign conduct constitute a substantial and legitimate nexus to justify the application of Indonesian penal sovereignty (Kusuma, 2025; Ryngaert, 2022).

However, this statutory extraterritorial extension must not be misconstrued as an expansive grant of cross-border enforcement power. The substantive authority to criminalize foreign digital conduct under the ITE Law is dogmatically distinct from the procedural authority to execute coercive investigative measures abroad (Arnell & Faturoti, 2023; Shurson, 2025). This conceptual boundary becomes highly problematic when essential electronic evidence is held by transnational data custodians or hosted in foreign cloud architectures, exposing the limits of unilateral domestic statutes (Sachoulidou, 2024; Shurson, 2025).

3.2. The 2026 Criminal-Law Reform and the Enforcement Gap

The formal entry into force of Law No. 1 of 2023 concerning the Criminal Code (KUHP) on 2 January 2026 marks a significant transformation in Indonesia's criminal justice system, replacing the previous colonial-era penal framework (Republic of Indonesia, 2023). The New KUHP establishes the contemporary national framework for criminal responsibility, including provisions governing Indonesia's jurisdiction over certain extraterritorial offences through modernized principles of active and passive nationality (Republic of Indonesia, 2023; Tobing & Fitria, 2025). This substantive reform must be examined in conjunction with the New Criminal Procedure Code (KUHP) under Law No. 20 of 2025, which also entered into force on 2 January 2026 and replaced Law No. 8 of 1981. The simultaneous application of the New KUHP and New KUHP therefore creates a new legal framework for assessing the relationship between Indonesia's substantive criminal jurisdiction and the procedural authority to investigate and obtain evidence in cross-border cybercrime cases.

To evaluate its operational impact, this substantive overhaul must be analyzed alongside the modernized Criminal Procedure Code (KUHP) and secondary legislative instruments intended to adjust transitional criminal procedures (Republic of Indonesia, 2025, 2026). This post-2026 legal landscape demands a rigorous reassessment of how state institutions manage criminal procedure, evidentiary chains, and constitutional safeguards when a triable offence is digitally fragmented across international boundaries (Kusuma, 2025).

Crucially, the expansion of substantive penal claims under the New KUHP does not resolve the tension between prescriptive and enforcement jurisdiction (Ryngaert, 2015, 2022). The statutory capacity to classify external digital conduct as an offence under Indonesian law does not create a lawful procedural pathway to seize evidence situated within foreign jurisdictions (Arnell & Faturoti, 2023; Shurson, 2025). Expanding the criminal code without corresponding multilateral enforcement mechanisms merely widens the enforcement gap, an institutional vulnerability evaluated in the subsequent analysis (Shurson, 2025).

3.3. Mutual Legal Assistance and Personal Data Protection

Cross-border cyber investigations in Indonesia frequently clash with the statutory rigidities of mutual legal assistance and the strict compliance mandates of data privacy (Kusuma, 2025; Tobing & Fitria, 2025). Law No. 1 of 2006 (the MLA Law) remains the principal statutory framework governing formal international cooperation in criminal matters (Republic of Indonesia, 2006). The operational challenge in cybercrime contexts arises because accessing foreign-held electronic evidence necessitates strict adherence to these formal state-to-state channels, which are structurally incompatible with the volatile and transient nature of digital data (Sachoulidou, 2024; Shurson, 2025).

This procedural friction is further compounded by the enforcement of the Personal Data Protection (PDP) Law (Republic of Indonesia, 2022). Because cross-border requests for electronic evidence routinely involve personal data belonging to suspects, victims, witnesses, or third parties, the legality of data acquisition cannot be viewed solely through the prism of criminal procedure (Liat & Wahyuningtyas, 2025; Sachoulidou, 2024). Data protection principles, particularly regarding international data transfers and processing limitations, impose strict obligations on state authorities to ensure that cross-border evidence gathering does not infringe upon statutory privacy rights (Liat & Wahyuningtyas, 2025; Rahman & Mulyania, 2025).

Consequently, Indonesian law enforcement faces a complex regulatory paradox. State actors must simultaneously satisfy the evidentiary standards of domestic criminal proceedings, respect the territorial sovereignty of the state where the data custodian resides, and comply with the strict privacy protections codified in the PDP Law (Arnell & Faturoti, 2023; Liat & Wahyuningtyas, 2025; Ryngaert, 2022).

3.4. The Limits of Prescriptive Jurisdiction

The current Indonesian framework highlights a fundamental conflict between possessing a statutory basis for jurisdiction and

having the practical capability to exercise investigative authority. The former establishes a legal link between the offense and the state, while the latter dictates the lawful mechanisms through which authorities may obtain evidence or deploy coercive powers (Shurson, 2025; United Nations Office on Drugs and Crime [UNODC], 2024).

This distinction becomes critical in cloud-based investigations. The physical location of a targeted server is frequently unknown, dynamically allocated, or distributed across multiple jurisdictions via virtualized environments. Concurrently, the private service providers controlling the data may split their corporate headquarters, regional operational nodes, and data storage infrastructure across separate foreign states (UNODC, 2024; Svantesson & Osula, 2025).

As a result, an extraterritorial legal framework that relies solely on the physical location of the offender or the victim cannot effectively handle the complex evidentiary demands of modern cybercrime. This structural mismatch between broad prescriptive laws and restricted enforcement capabilities creates a severe enforcement gap, which forms the subject of the following section (Shurson, 2025; UNODC, 2024).

4. THE ENFORCEMENT GAP: JURISDICTION, SOVEREIGNTY, AND DIGITAL EVIDENCE

4.1. *The Bifurcation of Prescriptive and Enforcement Jurisdiction*

The dogmatic separation between jurisdiction to prescribe and jurisdiction to enforce forms the baseline for analyzing cross-border cybercrime (Ryngaert, 2022; Shurson, 2025; Svantesson & Osula, 2025). The distinction is particularly important in cyberspace because a state may possess a legal basis to regulate conduct while lacking authority to undertake coercive investigative measures beyond its territory (Ryngaert, 2022; Shurson, 2025). Prescriptive jurisdiction dictates the legislative competence of a state to subject extraterritorial conduct to its substantive penal code. Conversely, enforcement jurisdiction governs the executive capacity of state actors to deploy coercive measures, including search, seizure, data interception, preservation mandates, and compulsory disclosure orders (Shurson, 2025).

This conceptual bifurcation invalidates any attempt to treat extraterritorial jurisdiction as a monolithic legal doctrine. A sovereign state may well establish a legitimate prescriptive nexus based on localized effects or national interests, yet remain fundamentally barred from executing coercive procedures inside a foreign territory (Ryngaert, 2022; Shurson, 2025). The distinction is also reflected in contemporary international cybercrime frameworks, which recognize jurisdictional bases while simultaneously requiring respect for sovereign equality and territorial integrity (United Nations, 2024).

In digital forensics, remote data access introduces deep systemic complexities. The mere fact that a domestic investigator remains physically seated within Indonesian territory does not absolve the state of sovereignty violations. When a unilateral investigative maneuver extracts data held by a foreign custodian or situated within an external digital infrastructure, that action directly impinges upon the territorial sovereignty of the host state, irrespective of the investigator's physical location (Ryngaert, 2022; Shurson, 2025). This concern is particularly significant because contemporary digital investigations increasingly involve data that is distributed across jurisdictions and controlled by service providers located outside the investigating state (Svantesson & Osula, 2025; UNODC, 2024). The Budapest Convention's Article 32 illustrates the exceptional nature of unilateral trans-border access by expressly permitting access in limited circumstances—where data is publicly available or where lawful and voluntary consent has been obtained from a person authorized to disclose it (Council of Europe, 2001).

4.2. *Territorial Sovereignty and the Paradox of Unilateral Access*

The principle of territorial sovereignty remains the structural bedrock of public international law. Consequently, executing coercive state authority within a foreign domain requires either an explicit treaty-based authorization or a universally recognized rule of international law (Ryngaert, 2022; United Nations, 1969).

This structural rigidity creates severe operational barriers for Indonesian cybercrime investigations. For example, if a severe cyberattack paralyzes Indonesian financial institutions, but the diagnostic server logs and account credentials reside with a corporate data custodian incorporated under foreign laws, a critical conflict emerges. While Indonesia possesses an undisputed substantive interest to criminalize and prosecute the offence, this national interest does not generate an automatic right to compel compliance from the foreign provider using domestic judicial warrants (Shurson, 2025; UNODC, 2024).

The core institutional challenge is therefore a matter of jurisdictional translation. The problem lies in how a legitimate domestic interest can be converted into a lawful cross-border request without violating foreign sovereignty or rendering the resulting evidence inadmissible (Sachoulidou, 2024; Shurson, 2025).

4.3. Evidentiary Volatility and Cloud-Based Data Fragmentation

Electronic evidence fundamentally differs from traditional physical evidence because its corporate custody, geographical storage, and remote accessibility are structurally decoupled. A single digital dataset routinely undergoes dynamic sharding and replication across multiple data centers globally, managed by a tech conglomerate in one jurisdiction, administered by network engineers in another, and accessed by users worldwide (Council of Europe, 2021; Svantesson & Osula, 2025).

This extreme data fragmentation undermines the geographical assumptions underlying traditional criminal procedure. As Sachoulidou (2024) demonstrates, the evolution of cross-border electronic evidence forces a reliance on non-traditional public-private interactions, bypassing traditional state-to-state channels while triggering severe concerns regarding state sovereignty and fundamental procedural rights (Sachoulidou, 2024; UNODC, 2024).

The legal friction intensifies when dealing with highly volatile digital materials. Critical data points, including subscriber information, dynamic IP routing logs, cloud metadata, and temporary access records, are subject to corporate retention policies that vary drastically across jurisdictions. This high rate of volatility creates an urgent need for rapid preservation, which frequently collides with the slow timelines required for international legal authorization (Eurojust, 2025; UNODC, 2024).

4.4. The Rise of "Investigative Jurisdiction" and Its Conceptual Limits

The emergence of unilateral data access mechanisms has forced international legal scholarship to confront the concept of investigative jurisdiction. Shurson (2025) identifies this development as a profound challenge to traditional extraterritoriality doctrines, noting that domestic law enforcement agencies increasingly circumvent classical territorial mechanisms by directly demanding data from transnational service providers (Shurson, 2025; Sachoulidou, 2024).

However, technical feasibility must not be conflated with international legality. The fact that a transnational service provider possesses the technical capability to extract and transmit data to a foreign investigator does not grant the requesting state an unrestricted legal right to compel such disclosure. The validity of direct access depends on a complex matrix of factors, including the provider's corporate structure, the blocking statutes of the host state, contractual data privacy clauses, multilateral executive agreements, and the legal taxonomy of the requested data (Hemmings et al., 2020; Shurson, 2025; Svantesson & Osula, 2025).

This systemic complexity demonstrates that Indonesia cannot rely on a simple expansion of its substantive penal reach. Instead, the state requires a structured framework designed to evaluate both the legitimacy of the initial criminal nexus and the international lawfulness of the specific mechanism used to capture the digital evidence (Shurson, 2025; Svantesson & Osula, 2025).

5. COMPARATIVE AND INTERNATIONAL LEGAL FRAMEWORK

5.1. Statutory Boundary Setting under Singapore's Computer Misuse Act

Singapore's Computer Misuse Act (CMA) provides a sophisticated regional template for structuring extraterritorial penal power through clearly defined statutory conditions rather than open-ended geographical expansion. The CMA links its extraterritorial application to specified statutory circumstances rather than relying on unrestricted geographical claims (Singapore, 1993; Urbas, 2008).

For the Indonesian legal reform process, the utility of the Singaporean model lies in its specific legislative drafting technique rather than any direct policy transplantation. Singapore demonstrates how a regional common-law jurisdiction can codify specific connecting circumstances that justify extraterritorial application while keeping its substantive prescriptive claims analytically separate from practical enforcement capabilities (Ministry of Home Affairs Singapore, 2017; Urbas, 2008).

This mechanism confirms that effective digital criminal frameworks require explicit statutory anchors. Indonesia cannot rely on broad rhetorical claims about the borderless nature of cyberspace; it must build a precise statutory framework that limits and justifies its external reach (Singapore, 1993; Urbas, 2008).

5.2. Possession, Custody, and Control under the United States CLOUD Act

The United States Clarifying Lawful Overseas Use of Data (CLOUD) Act shifts the paradigm of data jurisdiction by moving away from physical server locations to corporate control. Codified under Section 2713 of Title 18 of the U.S. Code, this framework mandates that covered electronic communication and remote computing service providers must disclose data within their possession, custody, or control, regardless of whether such digital assets are stored within or outside the physical territory of the United States (Hemmings et al., 2020; United States Congress, 2018).

The legal significance of the CLOUD Act rests on its replacement of spatial territoriality with corporate management and control. Simultaneously, the U.S. statutory framework builds in defensive legal tools, establishing explicit mechanisms for addressing conflicts with foreign law and international comity considerations (Hemmings et al., 2020; United States Congress, 2018).

This model highlights the clear advantage of separating physical data localization from corporate management. However, it also serves as a warning for Indonesia, demonstrating that unilateral provider-mediated access requires strong legal safeguards to protect foreign sovereign interests and individual constitutional rights (Liat & Wahyuningtyas, 2025; Rahman & Mulyania, 2025).

5.3. Institutionalized Order Mechanisms within the European Union e-Evidence Framework

The European Union has moved beyond traditional international cooperation by implementing Regulation (EU) 2023/1543, which introduces European Production Orders and European Preservation Orders for electronic evidence in criminal matters. This framework allows competent authorities to issue binding orders to service providers offering services in the Union, including providers established or represented in another Member State, irrespective of the location of the data (European Parliament & Council of the European Union, 2023; Sachoulidou, 2024).

The European model offers a highly structured approach to cross-border data access. Instead of treating every extraterritorial data request as an exceptional, high-friction violation of national boundaries, it builds a routinized procedural pipeline that clearly defines the legal obligations binding the issuing authorities, private corporate custodians, and relevant executing authorities (European Commission, 2026; Kuczyńska, 2024; Sachoulidou, 2024).

This framework is highly relevant to Indonesia's current legal reforms because it demonstrates how procedural rules must complement substantive penal claims. A well-defined prescriptive basis is insufficient on its own; a state must also establish clear procedural paths to legally capture data across borders (European Commission, 2026; Sachoulidou, 2024; Varbanova, 2025).

5.4. Structural Inefficiencies of Mutual Legal Assistance and the Budapest Benchmark

Traditional Mutual Legal Assistance Treaties (MLATs) remain a central method for securing foreign-held digital evidence because they respect state sovereignty by working through formal state-to-state channels (Council of Europe, 2001; UNODC, 2020). By routing evidence requests through competent authorities, the MLAT process ensures that the requested state retains control over the execution of coercive measures within its territory (Republic of Indonesia, 2006; UNODC, 2020).

However, the slow turnaround time of traditional MLAT procedures directly conflicts with the high volatility of electronic evidence. The Council of Europe Convention on Cybercrime (Budapest Convention) addresses this operational friction by providing international mechanisms for expedited data preservation and mutual assistance. The Second Additional Protocol to the Convention further expands these tools by establishing mechanisms for enhanced cooperation and disclosure of electronic evidence (Council of Europe, 2021, 2026; Sachoulidou, 2024).

For Indonesia, these international developments mean that mutual legal assistance cannot be treated as a slow, purely diplomatic tool. The state must integrate its domestic MLA processes with fast preservation mandates and specialized institutional paths that match the fast-changing nature of digital data (Council of Europe, 2021, 2026; Republic of Indonesia, 2006).

5.5. The Prospective Impact of the United Nations Convention against Cybercrime

The adoption of the United Nations Convention against Cybercrime on 24 December 2024 established a new global multilateral framework for criminalizing specific information and communications technology offenses and strengthening international cooperation concerning electronic evidence (United Nations General Assembly, 2024).

Indonesia formalized its initial commitment to this global regime by signing the Convention on 24 September 2026 (United Nations, 2026). The United Nations Treaty Collection confirms both the Indonesian signature date and that the Convention had not yet entered into force as of 28 September 2026.

From a dogmatic legal perspective, the impact of this signature must be analyzed prospectively. A formal signature does not equal immediate ratification, nor does it make the treaty provisions immediately operational within the Indonesian domestic legal order (Government of Indonesia, 2000; United Nations, 1969).

Nevertheless, the Convention serves as a critical guide for Indonesia's future legislative adjustments. It provides a formal, multilateral path to harmonize domestic criminal procedure with international standards. Implementing this treaty will require Indonesia to align its national laws with global cooperation networks, providing a timely opportunity to bridge the gap between its

broad prescriptive laws and restricted cross-border enforcement capabilities (United Nations General Assembly, 2024; UNODC, 2024).

To provide a structured analytical synthesis of the varying state practices and regional mechanisms discussed above, it is essential to map their jurisdictional components systematically. The shift from spatial-territorial paradigms to alternative legal links manifests differently across jurisdictions, creating distinct configurations of prescriptive capabilities and enforcement procedures. Table 1 maps the fundamental differences in jurisdictional approaches, primary connecting factors, data access mechanisms, and state sovereignty safeguards across Indonesia, Singapore, the United States, and the European Union.

Table 1: Comparative Jurisdictional Frameworks for Cross-Border Cybercrime and Data Access

Jurisdiction / Instrument	Prescriptive Basis & Core Approach	Primary Connecting Factors	Mechanism for Data Access	Sovereignty & Comity Safeguards
Indonesia (ITE Law & New KUHP)	Effects-based & Nationality Principles Expansive prescriptive reach focused on domestic impacts and national security interests.	• Locus of detrimental effect • Target infrastructure location • Active/passive nationality	Traditional Inbound Channels Relies primarily on formal, state-to-state MLAT channels and voluntary local intermediary compliance.	Strict Sovereignty Defense Requires reciprocal diplomatic validation; currently lacks domestic statutory comity clearinghouse tests.
Singapore (Computer Misuse Act)	Statutory Linkage Doctrine Extraterritoriality limited to specified, codified connecting links within a common law tradition.	• Physical locus of target computer • Citizenship/residency of actor • Specific localized harm	Hybrid Judicial Warrants Extends domestic warrants extraterritorially if the specific statutory connecting factors are satisfied.	Strict Statutory Construction Limits executive overreach by requiring precise alignment with explicitly codified statutory criteria.
United States (CLOUD Act)	Corporate Control Doctrine Replaces spatial server location with corporate custody, creating an enforcement-heavy approach.	• Corporate possession or custody • Management control over data • U.S. corporate nexus	Direct Provider Mandate Bypasses MLATs via direct statutory orders served to tech providers, regardless of global data location.	Executive Comity Agreements Provides statutory conflict-of-law resolution mechanisms and formal bilateral comity agreements.
European Union (e-Evidence Regulation)	Supranational Institutionalism Replaces traditional sovereignty friction with structured mutual recognition among member states.	• Service provider legal presence • EU regional nexus of crime • Institutional membership	Direct Binding Orders European Production and Preservation Orders served directly to providers across borders.	Systemic Notifications Mandatory notification systems involving the executing state authority to protect fundamental rights.

This comparative synthesis demonstrates that while the United States and the European Union have developed operational, provider-centric procedural pathways to bypass traditional state-to-state delays, Indonesia remains constrained by a structural

mismatch. The Indonesian legal framework possesses a highly modern, expansive prescriptive reach under the New KUHP and ITE Law, yet its enforcement capacity remains structurally dependent on slow, classical mutual legal assistance channels. This clear gap underscores the need for a systematic analytical tool, which is addressed by the Digital Jurisdictional Nexus Test proposed in the following section.

6. DISCUSSION: RETHINKING INDONESIA'S EXTRATERRITORIAL ENFORCEMENT FRAMEWORK

6.1. Recalibrating the Threshold of Extraterritorial Connectivity

The preceding comparative analysis demonstrates that Indonesia's primary enforcement obstacle is not a lack of extraterritorial provisions. The critical systemic challenge lies in determining what degree of territorial connection is legally sufficient to justify penal sovereignty, and how that substantive claim can be translated into a lawful cross-border investigative action (Kusuma, 2025; Shurson, 2025; UNODC, 2024).

A digital criminal framework that relies exclusively on isolated factors, such as the victim's nationality, the perpetrator's physical location, or the server's geographic coordinates, fails to address the complex reality of multi-jurisdictional cybercrime. Conversely, an overbroad effects-based doctrine that treats any minor domestic impact as an absolute license for extraterritorial enforcement risks creating severe jurisdictional conflicts and violating international comity (Ryngaert, 2022; Shurson, 2025; UNODC, 2024).

Therefore, international law enforcement requires a qualitative evaluation of the jurisdictional link rather than a quantitative counting of geographic points. This article introduces the Digital Jurisdictional Nexus Test to serve as a rigorous analytical tool for this purpose (Shurson, 2025).

This test does not function as a rigid mathematical formula. Instead, it provides a structured legal framework that allows investigators, prosecutors, and judges to systematically identify, weigh, and verify the legal connections binding a cross-border digital offense to the Indonesian sovereign order (Republic of Indonesia, 2023, 2024; Shurson, 2025).

6.2. The Digital Jurisdictional Nexus Test

The proposed framework operates through five distinct connecting factors (United Nations General Assembly, 2024; Council of Europe, 2021, 2026).

6.2.1. Conduct Nexus

The initial inquiry evaluates the relationship between the criminal action and the Indonesian territory. This factor requires analyzing whether the illicit digital conduct was initiated, directed, substantially executed, or technically integrated with computer systems located within Indonesia (Council of Europe, 2001; United Nations General Assembly, 2024).

The conduct nexus expands beyond the physical presence of the perpetrator. In cyberspace, criminal conduct includes the remote deployment of malicious code, unauthorized network intrusions, systemic manipulation of domestic databases, and the transmission of harmful data packages targeting local critical infrastructure (UNODC, 2024; United Nations General Assembly, 2024).

However, courts must apply this factor cautiously. The mere routing of digital data packets through Indonesian transit servers, without any substantive link to the execution or planning of the offense, cannot establish a sufficient legal nexus to assert criminal jurisdiction (Council of Europe, 2001; Ryngaert, 2022).

6.2.2. Victim and Harm Nexus

The second factor analyzes the physical location, legal status, and systemic impact of the offense on the victims (UNODC, 2024; United Nations General Assembly, 2024).

The targeting of Indonesian citizens, domestic corporations, or public institutions provides a strong connecting factor, provided that the resulting harm directly damages national interests (Kusuma, 2025; Tobing & Fitria, 2025). To prevent the overextension of passive personality or effects-based claims, the legal analysis must focus on the directness and severity of the harm rather than treating minor, incidental domestic impacts as a definitive basis for jurisdiction (Ryngaert, 2022).

This approach ensures that assertions of passive personality remain legally proportional, anchoring the state's prescriptive claims directly to the scale and intensity of the target-directed misconduct (Ryngaert, 2022; Shurson, 2025).

6.2.3. Digital Infrastructure Nexus

The third factor isolates the physical and logical components of the digital network used to facilitate the offense (Council of

Europe, 2001; United Nations General Assembly, 2024).

This nexus encompasses physical hardware, including localized servers, data centers, telecommunications channels, and network routing nodes situated within Indonesia that were directly compromised or used as a tool for the crime (Council of Europe, 2001; UNODC, 2024).

This infrastructure nexus acknowledges that modern cyber offenses frequently target systemic vulnerabilities rather than specific individuals. Nevertheless, incidental technical routing through Indonesian networks must be excluded from this nexus if the infrastructure connection remains completely detached from the core criminal scheme (Ryngaert, 2022; UNODC, 2024).

6.2.4. Economic and National-Interest Nexus

The fourth factor assesses the impact of the external conduct on vital public, economic, security, or state interests (United Nations General Assembly, 2024; UNODC, 2024).

This nexus becomes decisive when foreign digital actions target Indonesian critical information infrastructure, essential banking and financial networks, sovereign government databases, or national defense systems (United Nations General Assembly, 2024).

To prevent judicial overreach, this factor must remain strictly defined. Vague assertions of national security cannot serve as a blank check for extraterritorial overextension. A legitimate claim must identify the specific, statutorily protected interest and prove a direct, substantial threat to that interest (Ryngaert, 2022; Shurson, 2025).

6.2.5. Evidence and Service-Provider Nexus

The fifth factor evaluates the legal relationship between the state and the corporate entity holding or controlling the required electronic evidence (Council of Europe, 2021, 2026; United Nations General Assembly, 2024).

Unlike the first four factors, this nexus does not determine whether Indonesia possesses the substantive right to criminalize the underlying conduct. Instead, it serves a procedural purpose, identifying the lawful mechanism required to capture the digital assets (Council of Europe, 2021, 2026).

The operational assessment evaluates:

- The service provider's formal legal presence and corporate registration within Indonesia
- The availability of local subsidiaries or authorized corporate representatives
- The custodian's actual possession or control over the remote data fields
- The geographical locus of the data-processing operations
- The scale of commercial activities directed toward the Indonesian consumer market
- The blocking statutes and privacy laws of the host state
- Existing multilateral data-sharing agreements
- The legal classification and privacy sensitivity of the requested information

These considerations are consistent with contemporary international approaches to cross-border electronic evidence, which emphasize the location and control of data, service-provider cooperation, applicable domestic law, data protection, and international cooperation mechanisms (Council of Europe, 2021, 2026; Svantesson & Osula, 2025; United Nations General Assembly, 2024).

Consequently, the evidence and service-provider nexus serve as a critical procedural bridge, connecting the legitimacy of prescriptive claims with the international legality of investigative enforcement (Shurson, 2025; Svantesson & Osula, 2025).

6.3. Translating Prescriptive Authority into Lawful Enforcement

These five connecting factors demonstrate why a valid prescriptive nexus cannot be used as an automatic justification for unilateral cross-border investigations (Council of Europe, 2021, 2026; Shurson, 2025).

The first four factors answer a substantive question: Why does Indonesia have the right to claim jurisdiction over this foreign conduct? In contrast, the fifth factor addresses a distinct procedural question: How can Indonesia lawfully obtain the evidence required to prosecute that conduct? (Ryngaert, 2022; Shurson, 2025).

Maintaining this conceptual distinction is vital to respecting public international law. A strong substantive link to an offense does not erode foreign territorial sovereignty. Similarly, the mere fact that a transnational tech conglomerate maintains a local commercial office or marketing subsidiary in Jakarta does not grant domestic law enforcement an absolute right to issue compulsory data production orders for data stored in foreign cloud architectures (Council of Europe, 2021, 2026; Shurson, 2025).

The selection of the investigative mechanism must depend on a complex evaluation of data classification, provider control,

sovereign interests, data volatility, and available treaty-based cooperation channels (Council of Europe, 2021, 2026; Republic of Indonesia, 2006; Shurson, 2025).

6.4. *The Five-Stage Cross-Border Digital Investigation Protocol*

To operationalize the Digital Jurisdictional Nexus Test, this article constructs a systematic, five-stage procedural protocol (Shurson, 2025; Eurojust, 2026).

Stage 1: Jurisdictional Nexus Verification

Investigators must first document and verify the presence of the required connecting factors. The resulting investigative record must explicitly map out the conduct, harm, infrastructure, protected national interests, and provider connections that justify the domestic claim. This stage ensures a solid, reviewable legal basis exists before any cross-border enforcement steps are initiated (Shurson, 2025; UNODC, 2024).

Stage 2: Sovereignty and Comity Assessment

The second stage requires an explicit evaluation of how the proposed data acquisition affects the sovereign laws and political interests of the host state. Law enforcement must determine if the targeted digital actions cross into foreign territories, involve foreign-regulated entities, or disrupt data protected by foreign blocking statutes. If foreign sovereign interests are materially impacted, investigators must prioritize international cooperation channels over unilateral domestic expansion (Ryngaert, 2022; Shurson, 2025).

Stage 3: Evidentiary Taxonomy and Classification

The third stage classifies the targeted digital assets based on legal taxonomy and privacy intrusiveness. Basic subscriber records and account metadata trigger different privacy thresholds and sovereignty concerns than volatile traffic data or deep content data. This taxonomic sorting directly dictates the judicial authorization required and determines whether fast-track direct preservation or formal state-to-state channels are legally mandatory (Council of Europe, 2021, 2026; Sachoulidou, 2024; Eurojust, 2026).

Stage 4: Strategic International Cooperation Channel Selection

The fourth stage dictates the operational route for cross-border data acquisition. Rather than prioritizing administrative convenience, law enforcement must select the appropriate legal channel based on a strict analysis of treaty obligations, the nature of the data, and the legal restrictions of the host state. The procedural options include (Council of Europe, 2001, 2021, 2026; Republic of Indonesia, 2006; Sachoulidou, 2024):

- Formal mutual legal assistance channels through the designated Central Authority
- Expedited data preservation requests under the Budapest Convention framework
- Direct cross-border requests to service providers when explicitly permitted by applicable law
- Police-to-police networks via Interpol National Central Bureaus
- Bilateral or multilateral law enforcement treaties
- Ad hoc international agreements recognized under public international law

The selection of the mechanism must be based on legality rather than convenience alone, ensuring that the evidence gathered remains admissible in domestic courts (Council of Europe, 2021, 2026; Eurojust, 2026; Shurson, 2025).

Stage 5: Independent Judicial and Procedural Review

The final stage requires independent judicial oversight to review the legality and proportionality of the cross-border investigative measure before the evidence is introduced at trial. This oversight mechanism acts as a constitutional filter to evaluate (Sachoulidou, 2024; Shurson, 2025):

- The substantive jurisdictional basis established in Stage 1
- The operational necessity of the coercive data invasion
- The proportionality of the request relative to the severity of the offense
- The direct relevance of the targeted digital assets to the indictment
- The protection of third-party personal data under the PDP Law
- Adherence to domestic criminal procedure and international evidence-gathering treaties
- The integrity of the digital chain of custody during transnational transit

This final stage is critical because electronic evidence obtained abroad is highly vulnerable to subsequent procedural challenges during domestic trial proceedings (Putra, 2026; Sachoulidou, 2024; Eurojust, 2026).

6.5. Balancing Sovereignty, Effectiveness, and Procedural Safeguards

The proposed framework reconciles three competing objectives within cross-border criminal justice. First, operational effectiveness requires Indonesian law enforcement to rapidly preserve and seize highly volatile electronic evidence before it is permanently deleted (Eurojust, 2026; UNODC, 2024). Second, state sovereignty demands respect for the territorial and regulatory authority of foreign jurisdictions (MacNeil, 2026; Shurson, 2025). Third, procedural rights require that all investigative measures strictly adhere to the principles of legality, necessity, proportionality, data privacy, and judicial review (Council of Europe, 2021; European Parliament & Council of the European Union, 2023; Shurson, 2025).

Consequently, this framework does not treat international cooperation as an institutional barrier to effective law enforcement. Instead, it integrates cooperation directly into the enforcement architecture (Council of Europe, 2021; Eurojust, 2026). This approach directly addresses the systemic concerns raised in contemporary legal scholarship regarding unrestricted extraterritoriality. Arnell and Faturoti (2023) emphasize the severe geopolitical risks associated with overbroad transnational criminal claims, while Shurson (2025) demonstrates how emerging investigative practices increasingly bypass traditional state-to-state checks.

The Digital Jurisdictional Nexus Test serves as a limiting principle rather than an expansion tool. Its primary purpose is to make Indonesia's extraterritorial claims predictable and transparent, while ensuring that any cross-border investigative measure remains tethered to international law and constitutional due process (MacNeil, 2026; Shurson, 2025).

7. IMPLICATIONS FOR INDONESIAN CRIMINAL LAW REFORM

7.1. Legislative Harmonization and Statutory Decoupling

The modern architecture of Indonesian criminal law requires a structural realignment to harmonize substantive and procedural statutes (Republic of Indonesia, 2023, 2025, 2026). The post-2026 legal framework must explicitly separate prescriptive competency from enforcement authority within its statutory text (Republic of Indonesia, 2023, 2025; Shurson, 2025). To achieve this, future implementing regulations or formal guidelines from the Supreme Court (MA) and the Attorney General's Office (Kejaksaan Agung) should adopt the connecting factors of the Digital Jurisdictional Nexus Test. Rather than enacting a rigid statutory formula, formatting these factors into flexible evidentiary guidelines will allow investigators, prosecutors, and judges to systematically document the legal basis of cross-border investigations (Council of Europe, 2021, 2026; UNODC, 2024). This approach reduces structural uncertainty, preventing broad substantive penal claims from being misused as unauthorized licenses for cross-border enforcement (Shurson, 2025).

7.2. Codification of Cross-Border Electronic Evidence Procedures

Indonesia must urgently codify specific procedural pathways dedicated to cross-border electronic evidence, taking account of the new Criminal Procedure Code and the distinctive requirements of electronic evidence (Republic of Indonesia, 2025; Council of Europe, 2021, 2026). The New KUHAP entered into force on 2 January 2026 and replaced Law No. 8 of 1981, making it the appropriate current procedural reference. This specialized procedural framework must establish explicit rules governing:

- Fast-track preservation mandates for volatile data fields
- Extraterritorial production requests directed at corporate entities
- Emergency evidence preservation protocols during active cyberattacks
- Digital authentication methodologies for untrusted network environments
- Chain of custody verification for data crossing multiple jurisdictions
- Transnational admissibility standards for electronic court trials
- Certified translation and validation procedures for foreign data packets
- Legal classification and extraction of system metadata
- Forensic extraction of dynamic, cloud-hosted virtual environments
- Data minimization techniques to protect unrelated third-party personal data.

This procedural modernization ensures that electronic evidence captured via international cooperation channels meets strict domestic standards of legality, preserving its integrity for trial (Republic of Indonesia, 2025; Sachoulidou, 2024; UNODC, 2024).

7.3. Modernizing Mutual Legal Assistance for Volatile Data

While Mutual Legal Assistance (MLA) remains the cornerstone of formal international cooperation, its operational mechanics must adapt to the fast-changing nature of electronic evidence (Council of Europe, 2001, 2021, 2026; United Nations General Assembly, 2024). Indonesia needs to remodel its Central Authority operations within the Ministry of Law and Human Rights by establishing specialized, 24/7 fast-track channels for cybercrime requests. This specialized pipeline must separate the immediate preservation of volatile data from the slower formal acquisition of evidence (Council of Europe, 2021, 2026). By securing data preservation orders instantly while formal diplomatic channels process the substantive request, Indonesia can prevent foreign data custodians from deleting critical data under standard corporate retention policies (Council of Europe, 2001, 2021). This operational update directly complements the cooperation structures of the Budapest Convention and the global United Nations cybercrime framework (Council of Europe, 2021, 2026; United Nations General Assembly, 2024).

7.4. Regulating Public-Private Interactions with Transnational Providers

Indonesia must establish clear, binding regulations governing interactions between state law enforcement and transnational service providers (Council of Europe, 2021, 2026). These rules must draw a sharp line between voluntary public-private data sharing and compulsory extraterritorial disclosures, explicitly defining when a direct request to a foreign data custodian is legally valid (Council of Europe, 2021, 2026). The state must resist the urge to turn a provider's local commercial footprint or marketing presence into an excuse for unilateral jurisdiction. Instead, interactions with foreign service providers must always require explicit legal authorization, strict privacy protections under the PDP Law, and full alignment with international comity obligations (Republic of Indonesia, 2022; Shurson, 2025; United Nations General Assembly, 2024).

7.5. Judicial Oversight as a Constitutional Filter

Independent judicial oversight must serve as the primary constitutional filter for all cross-border evidence collection (Republic of Indonesia, 2025; United Nations General Assembly, 2024). Domestic courts cannot merely act as passive recipients of foreign-sourced evidence; judges must actively review the legality of cross-border data collection before trials begin (Republic of Indonesia, 2025; Sachoulidou, 2024). This review requires judges to verify that:

1. A valid, documented jurisdictional nexus exists under Stage 1
2. The targeted digital evidence is necessary and directly relevant to the charge
3. The scope of data invasion remains strictly proportional to the offense
4. Foreign sovereign interests and comity limitations have been assessed
5. Personal data and third-party privacy interests remain fully protected
6. The foreign-sourced data fully satisfies domestic admissibility requirements

This active judicial review strengthens the legitimacy of Indonesia's cross-border actions and provides a clear mechanism to identify and reject procedurally defective evidence (Republic of Indonesia, 2025; Sachoulidou, 2024).

7.6. Strategic Treaty Implementation and Ratification Post-September 2026

Indonesia's signature of the United Nations Convention against Cybercrime on 24 September 2026 marks a significant step forward for international cooperation, but its domestic implementation requires careful management (United Nations, 2026). The UN Treaty Collection records Indonesia's signature on that date and confirms that the Convention was not yet in force as of 28 September 2026. A formal signature does not justify rushing into domestic enforcement changes. The state must perform a comprehensive assessment of its treaty obligations and analyze how the convention interacts with existing laws (Government of Indonesia, 2000; United Nations, 1969).

Consequently, the Convention must be treated as a long-term goal for Indonesia's cybercrime architecture rather than an immediate replacement for existing MLA treaties (United Nations General Assembly, 2024; Council of Europe, 2021, 2026). Future ratification efforts must focus on ensuring full compatibility between new international commitments and Indonesia's domestic rules on jurisdiction, data privacy, judicial authorization, and state sovereignty (Republic of Indonesia, 2022, 2025; United Nations General Assembly, 2024).

8. CONCLUSION

The rise of cross-border cybercrime permanently destabilizes the traditional legal links between geographic territory, criminal jurisdiction, and state enforcement power. In response to this digital shift, Indonesia has steadily expanded its domestic criminal law architecture through the Electronic Information and Transactions (ITE) Law, the New Criminal Code (KUHP), the Mutual Legal Assistance (MLA) Law, and the Personal Data Protection (PDP) Law (Republic of Indonesia, 2006, 2008, 2022, 2023, 2024). However, this study demonstrates that establishing a broad statutory basis for extraterritorial criminal jurisdiction does not automatically grant state actors the authority to execute coercive investigative measures outside national borders (Ryngaert, 2022; Shurson, 2025). Unilateral digital enforcement actions conducted in foreign jurisdictions without explicit authorization remain subject to the constraints of international law and state sovereignty (United Nations, 1969; Shurson, 2025).

The primary doctrinal contribution of this article lies in its strict separation of prescriptive jurisdiction from enforcement jurisdiction. Prescriptive jurisdiction determines whether Indonesia possesses a sufficient national nexus to criminalize a specific digital action. Enforcement jurisdiction, by contrast, dictates the precise international and domestic mechanisms required to capture evidence when the perpetrators, data custodians, or server architectures reside abroad (Ryngaert, 2015, 2022; Shurson, 2025).

To operationalize this conceptual separation, this article introduces the Digital Jurisdictional Nexus Test based on five distinct connecting factors: the locus of conduct, victimhood and localized harm, operational data infrastructure, national economic interest, and proximity to the data custodian or service provider. While the first four factors measure the substantive connection linking the digital offense to Indonesia, the fifth factor isolates the procedural legality of cross-border data acquisition (Council of Europe, 2021, 2026; Shurson, 2025).

Building upon this nexus test, the study introduces a Five-Stage Cross-Border Digital Investigation Protocol navigating nexus verification, sovereignty and comity assessments, evidentiary taxonomy, international cooperation channel selection, and independent judicial review. This protocol provides a structured, reviewable pathway that successfully balances the technical need for rapid data collection with the strict demands of state sovereignty and constitutional due process (Council of Europe, 2021, 2026; Sachoulidou, 2024).

Furthermore, comparative frameworks from Singapore, the United States, and the European Union demonstrate that global legal systems are shifting away from spatial paradigms toward provider-centric and institutionalized data access models (European Parliament & Council of the European Union, 2023; Hemmings et al., 2020; Singapore, 1993). These foreign frameworks confirm that effective cybercrime enforcement cannot rely on the simple expansion of substantive penal codes. Instead, modern states require clear procedural pathways that can translate legitimate prescriptive claims into lawful, admissible electronic evidence (Sachoulidou, 2024; Shurson, 2025).

Finally, Indonesia's signature of the United Nations Convention against Cybercrime on 24 September 2026 marks a strategic opportunity to modernize its international cooperation networks (United Nations, 2026). Because the Convention has not yet entered into force, its current value is prospective, serving as a legislative blueprint for future institutional reforms rather than an immediate source of investigative power. Ultimately, Indonesia's extraterritorial cybercrime framework must move away from unchecked statutory expansion. The state must focus instead on building a predictable equilibrium balanced on clear jurisdictional connections, specialized procedural pathways, international treaty compliance, and robust judicial safeguards (MacNeil, 2026; Shurson, 2025).

CONFLICT OF INTEREST

The authors declare no conflict of interest in relation to the publication of this manuscript.

REFERENCES

1. Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime—Why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, 37(1), 29–51. <https://doi.org/10.1080/13600869.2022.2061888>
2. Cane, P., & Kritzer, H. M. (Eds.). (2010). *The Oxford handbook of empirical legal research*. Oxford University Press.
3. Council of Europe. (2001). *Convention on cybercrime* (European Treaty Series No. 185). Council of Europe.
4. Council of Europe. (2021). *Second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224). Council of Europe.

5. Council of Europe. (2025). 2025 Council of Europe/Eurojust joint workshop on the Second Additional Protocol to the Convention on Cybercrime. Council of Europe. <https://www.coe.int/en/web/cybercrime/-/2025-council-of-europe/eurojust-joint-workshop-on-the-second-additional-protocol-to-the-convention-on-cybercrime>
6. Council of Europe. (2026). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Council of Europe. <https://www.coe.int/en/web/cybercrime/second-additional-protocol>
7. Eberle, E. J. (2011). The methodology of comparative law. *Roger Williams University Law Review*, 16(1), 51–71.
8. Eurojust. (2025). E-evidence: Cross-border access to electronic evidence. In Annual report 2025. European Union Agency for Criminal Justice Cooperation.
9. Eurojust. (2026). SIRIUS electronic evidence situation report 2025. European Union Agency for Criminal Justice Cooperation.
10. European Commission. (2026, September 29). E-evidence. European Commission.
11. European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. *Official Journal of the European Union*, L 191, 118–180.
12. European Union. (2025). Council Decision (EU) 2025/2307 of 13 October 2025 on the signing, on behalf of the European Union, of the United Nations Convention against Cybercrime. *Official Journal of the European Union*.
13. Government of Indonesia. (2000). *Undang-Undang Republik Indonesia Nomor 24 Tahun 2000 tentang Perjanjian Internasional*. <https://peraturan.bpk.go.id/Details/44991/uu-no-24-tahun-2000>
14. Hemmings, J., Srinivasan, S., & Swire, P. (2020). Defining the scope of “possession, custody, or control” for privacy issues and the CLOUD Act. *Journal of National Security Law & Policy*, 10, 631–660.
15. Hutchinson, T. (2018). Doctrinal research: Researching the jury. In D. Watkins & M. Burton (Eds.), *Research methods in law* (2nd ed., pp. 8–39). Routledge.
16. Hutchinson, T., & Duncan, N. (2012). Defining and describing doctrinal legal research. *Deakin Law Review*, 17(1), 83–119.
17. Kuczyńska, H. (2024). The EU e-evidence package from the Polish perspective: High time for a systemic change. *Studia Iuridica Lublinensia*, 33(5), 125–153. <https://doi.org/10.17951/sil.2024.33.5.125-153>
18. Kusuma, A. B. (2025). Jurisdictional challenges in prosecuting transnational cyber offenders in Indonesia. *Indonesian Journal of Digital Crime and Criminal Justice*, 1(2), 309–346. <https://doi.org/10.68080/jdccj.v1i2.29>
19. Legrand, P. (1997). The impossibility of “legal transplants.” *Maastricht Journal of European and Comparative Law*, 4(2), 111–124.
20. Liat, K. E., & Wahyuningtyas, S. Y. (2025). Personal data protection in cloud computing businesses in Indonesia: Cross-border data transfers and access by public authorities. *Refleksi Hukum: Jurnal Ilmu Hukum*, 9(2), 195–214. <https://doi.org/10.24246/jrh.2025.v9.i2.p195-214>
21. MacNeil, G. (2026). Extraterritoriality in transnational criminal law: The sovereignty paradox. *AJIL Unbound*, 120, 225–230. <https://doi.org/10.1017/aju.2026.10082>
22. Ministry of Home Affairs Singapore. (2017, January 9). *Computer Misuse and Cybersecurity (Amendment) Bill*. <https://www.mha.gov.sg/media-room/newsroom/computer-misuse-and-cybersecurity-amendment-bill/>
23. Rahman, F., & Mulyania, C. K. (2025). Minimising unnecessary restrictions on cross-border data flows? Indonesia’s position and challenges post personal data protection act enactment. *International Review of Law, Computers & Technology*, 39(2), 281–300. <https://doi.org/10.1080/13600869.2024.2359901>
24. O’Sullivan, A. B. (2025). Legal and national security reform: Reconstructing data privacy regulations in the era of Indonesia’s digital sovereignty. *Vifada Assumption Journal of Law*, 3(1). <https://doi.org/10.70184/9c2pfk27>
25. Putra, G. R. A. (2026). Kedudukan bukti digital dalam sistem peradilan pidana Indonesia: Rekonsepsi pengaturan dan penguatan *chain of custody* di era *cyber-enabled crime*. *BULETIN ADALAH*, 8(7). <https://doi.org/10.15408/adalah.v8i7.51879>
26. Republic of Indonesia. (2006). *Law No. 1 of 2006 concerning mutual legal assistance in criminal matters*.
27. Republic of Indonesia. (2008). *Law No. 11 of 2008 concerning electronic information and transactions*.

28. Republic of Indonesia. (2022). *Law No. 27 of 2022 concerning personal data protection*.
29. Republic of Indonesia. (2023). *Law No. 1 of 2023 concerning the Criminal Code*.
30. Republic of Indonesia. (2024). *Law No. 1 of 2024 concerning the second amendment to Law No. 11 of 2008 concerning electronic information and transactions*.
31. Republic of Indonesia. (2025). *Law No. 20 of 2025 concerning the Criminal Procedure Code*.
32. Republic of Indonesia. (2026). *Law No. 1 of 2026 concerning criminal adjustment*.
33. Ryngaert, C. (2015). *Jurisdiction in international law* (2nd ed.). Oxford University Press.
34. Ryngaert, C. (2022). Extraterritorial enforcement jurisdiction in cyberspace: Normative shifts. *German Law Journal*, 23, 757–780. <https://doi.org/10.1017/glj.2022.48>
35. Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of “judicial” cooperation. *New Journal of European Criminal Law*, 15(3), 256–
36. 274. <https://doi.org/10.1177/20322844241258649>
37. Shurson, J. (2025). Investigative jurisdiction: The evolving limits of extraterritoriality in transnational digital investigations.
38. *International & Comparative Law Quarterly*, 74, 675–705. <https://doi.org/10.1017/S0020589325100985>
39. Singapore. (1993). *Computer Misuse Act 1993* (Cap. 50A). Singapore Statutes Online. <https://sso.agc.gov.sg/Act/CMA1993>
40. Svantesson, D. J. B., & Osula, A.-M. (2025). Unresolved jurisdictional issues in law enforcement access to data. In V. Franssen & S. Tosza (Eds.), *The Cambridge handbook of digital evidence in criminal investigations* (pp. 43–67). Cambridge University Press. <https://doi.org/10.1017/9781009049771.004>
41. Tobing, A. N. L., & 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>
42. United Nations. (1969). *Vienna Convention on the Law of Treaties*. United Nations Treaty Collection. https://treaties.un.org/pages/ViewDetailsIII.aspx?chapter=23&lang=en&mtdsg_no=XXIII-1&src=TREATY
43. United Nations. (2024). *United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes*. United Nations.
44. United Nations General Assembly. (2024). *United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes* (A/RES/79/243). United Nations.
45. United Nations Office on Drugs and Crime. (2020). *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime*. United Nations. https://www.unodc.org/documents/Cybercrime/IEG_Cyber_website/UNODC_CCPCJ_EG.4_2020_2/UNODC_CCPCJ_EG_4_2020_2_E.pdf
46. United Nations Office on Drugs and Crime. (2024). *Electronic evidence: Cross-border access to electronic evidence*. United Nations.
47. United Nations Office on Drugs and Crime. (2025a). *International cooperation against cybercrime and electronic evidence* [Working paper]. United Nations.
48. United Nations Office on Drugs and Crime. (2025b). *The nexus between cybercrime and corruption*. United Nations Office on Drugs and Crime.
49. United Nations. (2026). *United Nations Convention against Cybercrime: Status of treaties—Indonesia*. United Nations Treaty Collection. https://treaties.un.org/Pages/ViewDetails.aspx?chapter=18&mtdsg_no=XVIII-16&src=TREATY
50. United States Code. (2026). *18 U.S.C. § 2703: Required disclosure of customer communications or records*. Office of the Law Revision Counsel, U.S. House of Representatives.
51. United States Congress. (2018). *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, Pub. L. 115-141, div. V, 132 Stat. 1213.

-
52. Urbas, G. (2008). *An overview of cybercrime legislation and cases in Singapore* (Working Paper Series No. 001). Asian Law Institute, National University of Singapore. <https://law1a.nus.edu.sg/asli/publications/wps001.html>
53. Van Hoecke, M. (Ed.). (2011). *Methodology of legal research: Which method for what kind of discipline?* Hart Publishing.
54. Varbanova, G. (2025). Electronic evidence as an independent legal phenomenon: Theoretical framework and European practice. *Journal of Digital Technologies and Law*, 3(3), 497–511. <https://doi.org/10.21202/jdtl.2025.20>

Cite this Article: Pratiwi, K., Hasibuan, E.S., Fitriana, D. (2026). Cross-Border Cybercrime and Criminal Jurisdiction: Rethinking Indonesia's Extraterritorial Enforcement Framework. International Journal of Current Science Research and Review, 9(10), pp. 5321-5337. DOI: <https://doi.org/10.47191/ijcsrr/V9-i10-10>