Indonesian Journal *of* Digital Crime *and* Criminal Justice
Vol. 1 No. 1. January 2025. pp. 163-198
E-ISSN: XXXX-XXXX| P-ISSN: XXXX-XXX
Original Research Article

Cross-Border Cybercrime Investigation: Legal Challenges in Obtaining Digital Evidence

Fadhel Arjuna Adinda [1,2]*, Ridwan Arifin [3]
[1] Universitas Padjadjaran, Bandung, Indonesia
[2] Universitas Islam Riau, Pekanbaru, Indonesia
[3] Universitas Negeri Semarang, Semarang, Indonesia
* Corresponding author: fadhelarjuna@gmail.com

ABSTRACT

Cross-border cybercrime poses significant challenges to traditional criminal investigation mechanisms due to the borderless nature of digital networks and data storage systems. Law enforcement authorities frequently encounter legal and procedural obstacles in obtaining digital evidence located in foreign jurisdictions, particularly in cases involving cloud computing, encrypted communications, and decentralized platforms. This article analyzes the legal challenges associated with cross-border cybercrime investigations, with a focus on digital evidence acquisition. Employing normative legal research and comparative analysis of international cooperation mechanisms, the study evaluates the effectiveness of Mutual Legal Assistance Treaties (MLATs) and emerging frameworks such as direct data access agreements. The findings demonstrate that existing cooperation mechanisms are often slow, bureaucratic, and inadequate for time-sensitive cybercrime investigations. Jurisdictional conflicts, data sovereignty concerns, and differing evidentiary standards further complicate prosecution efforts. The article argues that the evolution of cybercrime necessitates the modernization of international legal cooperation frameworks to ensure timely and lawful access to digital evidence. It recommends enhanced multilateral agreements, standardized digital evidence protocols, and stronger cooperation between states and digital service providers. The study concludes that effective cybercrime enforcement depends on harmonizing legal frameworks with the realities of digital globalization.

KEYWORDS: Cross-Border Cybercrime, Digital Evidence, Mutual Legal Assistance, Jurisdiction, Cyber Law, International Cooperation

Available online at https://journal.criminallawinstitute.org/JDCCJ/article/view/20, since January 15, 2025
Submitted: November 11, 2024 ■ Reviewed: November 27, 2024 ■ Revised: January 5, 2026 ■ Accepted: January 15, 2025

INTRODUCTION

The rapid expansion of digital technologies has fundamentally reshaped the nature of criminal activity, producing a form of wrongdoing that is increasingly transnational, decentralized, and technologically mediated. Cybercrime is widely recognized in the literature as inherently borderless, operating beyond the constraints of physical geography and jurisdictional sovereignty (Wall 2007; Brenner 2010). Unlike traditional crimes that are typically confined within territorial boundaries, cybercrime can be executed in real time across multiple jurisdictions simultaneously, often relying on distributed infrastructures such as cloud computing systems, peer-to-peer networks, and anonymized communication platforms. This structural transformation has led scholars such as Yar (2013) and Clough (2015) to argue that cybercrime represents not merely a new category of offense but a fundamental reconfiguration of criminal opportunity structures in the digital age. Consequently, law enforcement agencies are increasingly confronted with investigative environments in which perpetrators, victims, and evidence are located in different legal jurisdictions, complicating conventional approaches to criminal investigation and enforcement.

At the center of modern cybercrime investigations lies digital evidence, which has become a primary—if not exclusive—source of evidentiary material in many cases. Digital evidence encompasses a broad range of electronically stored information, including electronic records, metadata, cloud-based data, communication logs, system access records, and transactional histories (Casey 2011; Rahmawati, et.al., 2024; Saputra, et.al. 2023). Unlike traditional physical evidence, digital evidence is characterized by its volatility, replicability, and dependence on complex technological infrastructures. In many cybercrime cases, it is often the only available form of evidence capable of reconstructing criminal activity, identifying perpetrators, and establishing intent. As Casey (2011) and Casey and Turnbull (2017) emphasize, the evidentiary value of digital traces lies not only in their content but also in their contextual metadata, which can reveal patterns of behavior, timing, and digital interactions critical for criminal

attribution. However, the same characteristics that make digital evidence valuable also render it highly vulnerable to alteration, deletion, and jurisdictional fragmentation.

The cross-border dimension of digital evidence further complicates its acquisition and use in criminal proceedings. Contemporary digital infrastructures are inherently transnational, with data frequently stored across multiple jurisdictions through cloud computing systems operated by global service providers such as Amazon Web Services, Google Cloud, and Microsoft Azure. As Kerr (2013) notes, the localization of data is often ambiguous, as information may be simultaneously stored, mirrored, or processed in several countries depending on server load, contractual arrangements, and technical configurations. Similarly, encrypted communication platforms such as WhatsApp, Telegram, and Signal present additional challenges by limiting law enforcement access to content through end-to-end encryption protocols. While these technologies enhance user privacy and security, they also create significant obstacles for lawful interception and evidence collection (Greenwald 2014; Abelson et al. 2015). Furthermore, decentralized systems such as blockchain-based platforms introduce additional layers of complexity, as data is distributed across peer-to-peer networks without centralized control, making traditional subpoena-based approaches increasingly ineffective.

These technological developments have generated significant legal and operational challenges for criminal justice systems worldwide. A core problem is that relevant digital evidence is often located outside the territorial jurisdiction of investigating authorities, rendering domestic legal instruments insufficient for effective access and retrieval. Traditional principles of sovereignty and territorial jurisdiction are ill-suited to address the fluid and distributed nature of digital data flows, particularly in cases involving multinational service providers and cross-border data storage. As Swire and Hemmings (2015) argue, the fragmentation of data across jurisdictions creates "jurisdictional fragmentation," where multiple legal systems simultaneously assert authority over different components of the same dataset. This situation frequently results in legal uncertainty, procedural delays, and conflicts of law

that undermine investigative efficiency.

In response to these challenges, states have increasingly relied on international cooperation mechanisms such as Mutual Legal Assistance Treaties (MLATs). However, the effectiveness of MLAT systems has been widely questioned in academic literature and policy reports. Studies by Kerr (2013) and the Council of Europe (2020) highlight that MLAT processes are often slow, bureaucratic, and ill-equipped to handle the urgency of digital evidence preservation in real-time cybercrime investigations. Requests for data preservation or disclosure may take weeks or even months to process, by which time critical evidence may have already been deleted, encrypted, or overwritten. This temporal mismatch between the speed of cybercrime and the procedural rigidity of MLAT frameworks significantly undermines their utility in modern investigations. As a result, law enforcement agencies increasingly seek alternative mechanisms such as direct access agreements with service providers or unilateral extraterritorial data requests, raising further concerns about sovereignty and privacy rights.

Despite extensive scholarly attention to cybercrime regulation, data protection, and privacy law, there remains a significant research gap in relation to the operational mechanics of cross-border digital evidence acquisition. Existing literature has largely focused on normative and doctrinal issues, such as the regulation of cybercrime offenses (Clough 2015), the protection of personal data (Zuboff 2019), and the governance of digital privacy (Solove 2008). However, comparatively limited attention has been paid to the practical effectiveness of international cooperation mechanisms in facilitating timely and reliable access to digital evidence. In particular, there is insufficient empirical and doctrinal analysis of how MLAT frameworks operate in the context of cloud computing environments, where data is dynamically distributed and continuously replicated across jurisdictions. Furthermore, the literature has not adequately addressed jurisdictional conflicts arising in real-time investigations, especially where multiple states simultaneously assert legal authority over the same digital infrastructure.

This gap is particularly significant given the increasing reliance of criminal justice systems on digital evidence in prosecuting cybercrime,

terrorism, financial fraud, and organized crime. As Carrier and Spohn (2018) argue, the effectiveness of modern criminal justice systems is increasingly contingent upon their ability to access and interpret digital traces in a legally admissible manner. The absence of efficient cross-border evidence acquisition mechanisms therefore poses a direct threat to the integrity and effectiveness of criminal justice processes. Moreover, the rapid evolution of encryption technologies, cloud infrastructures, and decentralized platforms has further intensified the urgency of developing more adaptive and responsive legal frameworks.

Against this backdrop, this study addresses three central research questions. First, what are the primary legal and operational challenges in obtaining digital evidence across national borders in cybercrime investigations? Second, to what extent do existing Mutual Legal Assistance Treaty (MLAT) mechanisms remain effective in addressing the demands of modern cybercrime cases? Third, what alternative models of international cooperation may offer more efficient and legally coherent solutions for cross-border digital evidence acquisition? These questions are designed to bridge the gap between doctrinal legal analysis and the practical realities of digital forensic investigation in transnational contexts.

The central argument of this article is that existing international legal cooperation mechanisms are structurally outdated and insufficient to meet the speed, scale, and complexity of cross-border digital evidence acquisition in contemporary cybercrime investigations. While MLAT systems and traditional sovereignty-based frameworks remain foundational to international criminal cooperation, they are increasingly misaligned with the technological realities of cloud computing, encrypted communications, and decentralized data infrastructures. As such, there is an urgent need to rethink and redesign international legal frameworks governing digital evidence to ensure that they are capable of responding effectively to the evolving landscape of cybercrime. This study therefore contributes to the growing body of scholarship advocating for more adaptive, technology-responsive, and transnational approaches to cybercrime governance in the digital age.

CONCEPTUAL FOUNDATIONS: CYBERCRIME, JURISDICTION, AND DIGITAL EVIDENCE

A. Concept of Cross-Border Cybercrime

Cross-border cybercrime constitutes a distinct category of transnational criminal activity that operates through interconnected digital networks rather than territorially bounded physical spaces. Unlike conventional offenses, cybercrime is structurally embedded in global information infrastructures, enabling offenders, victims, and facilitators to be located in different jurisdictions simultaneously. This phenomenon reflects what Wall (2007) conceptualizes as the "transformation of crime in the information age," where criminal conduct is increasingly mediated by digital technologies and networked environments.

From a criminological perspective, cybercrime is characterized by network-based offending patterns, where criminal activities are coordinated through distributed systems rather than centralized physical locations. Brenner (2010) argues that cybercrime fundamentally disrupts traditional assumptions of spatiality and causality in criminal law, as offenses can be executed instantaneously across multiple legal systems. Similarly, Yar (2013) emphasizes that cybercrime involves distributed actors whose identities, roles, and locations are often obscured through anonymization technologies, proxy servers, and encrypted communication channels.

The transnational nature of cybercrime is further reinforced by the global architecture of the internet, which enables real-time communication and data exchange across borders. As Clough (2015) notes, cybercriminal operations frequently exploit jurisdictional disparities, regulatory inconsistencies, and enforcement gaps between states, making cross-border coordination a structural necessity in modern cybercrime governance.

B. Nature of Digital Evidence

Digital evidence occupies a central role in contemporary criminal investigations, particularly in cybercrime cases where physical traces are

often absent. It is broadly defined as any information of probative value that is stored or transmitted in digital form, including electronic records, metadata, communication logs, and cloud-based datasets (Casey 2011).

One of the defining characteristics of digital evidence is its intangibility. Unlike physical evidence, digital data does not have a fixed material form and exists as binary information that requires technological systems for interpretation. This intangibility complicates traditional evidentiary paradigms, which are historically grounded in physicality and direct observation.

Digital evidence is also highly susceptible to alteration. Even minor interactions with digital systems can modify metadata, timestamps, or file structures, raising concerns about authenticity and integrity. Casey and Turnbull (2017) emphasize that ensuring evidentiary integrity requires strict chain-of-custody protocols and forensic preservation techniques.

Another critical characteristic is time sensitivity. Digital data can be rapidly deleted, overwritten, or encrypted, particularly in cybercrime contexts where perpetrators actively attempt to destroy traces of their activity. This temporal fragility creates urgency in evidence preservation and acquisition processes. Finally, digital evidence is geographically dispersed. In cloud computing environments, data is often distributed across multiple servers located in different jurisdictions. Kerr (2013) highlights that this dispersion creates significant legal uncertainty regarding which state has authority over specific datasets, complicating investigative access and judicial oversight.

C. Jurisdiction in Cybercrime

Jurisdictional authority in cybercrime cases is governed by a combination of territorial and extraterritorial principles that seek to establish legal competence over cross-border digital conduct. However, the application of these principles in cyberspace is increasingly contested due to the borderless nature of digital networks.

The principle of territorial jurisdiction remains the foundational doctrine in criminal law, asserting that states have authority over offenses committed

within their geographical boundaries. However, in cybercrime cases, determining the location of an offense is often complex, as digital actions may simultaneously occur across multiple jurisdictions.

Extraterritorial jurisdiction extends a state's legal authority beyond its territorial boundaries, particularly in cases where conduct abroad produces effects within the state. This principle is frequently invoked in cybercrime cases involving cross-border harm, such as financial fraud or data breaches affecting domestic victims.

The effects doctrine further strengthens extraterritorial claims by asserting jurisdiction when foreign conduct has substantial effects within the territory of a state. This doctrine has been widely applied in transnational cybercrime cases where digital activities produce localized harm despite being executed abroad. In addition, the passive nationality principle allows states to assert jurisdiction over offenses committed against their nationals, while the active nationality principle extends jurisdiction over offenses committed by their nationals abroad. These principles collectively form a complex jurisdictional matrix that governs cross-border cybercrime investigations (Cassese 2008; Shaw 2017).

D. Conflict of Laws in Cybercrime Investigation

The transnational nature of cybercrime frequently results in conflicts of law, particularly when multiple jurisdictions assert overlapping claims of authority over the same digital activity or evidence. These conflicts arise due to differences in substantive criminal law, procedural rules, and evidentiary standards across jurisdictions.

Overlapping jurisdiction is a common feature of cybercrime investigations, where multiple states may simultaneously claim authority based on territorial presence, victim location, or data storage location. This multiplicity of jurisdictional claims often leads to legal uncertainty and procedural delays. Competing sovereignty claims further complicate cross-border investigations, particularly when states adopt divergent legal standards regarding data access, privacy protection, and surveillance authority. As Schünemann (2018) notes, such conflicts reflect deeper tensions

between national sovereignty and the transnational nature of digital infrastructure.

Legal fragmentation is another critical challenge, as the absence of harmonized global standards for cybercrime regulation results in inconsistent legal frameworks. This fragmentation creates enforcement gaps that can be exploited by cybercriminal actors who strategically operate across jurisdictions with weaker regulatory regimes.

E. Mutual Legal Assistance in Criminal Matters (MLA)

Mutual Legal Assistance (MLA) constitutes the primary formal mechanism for international cooperation in criminal investigations, including cybercrime cases. It refers to a system of treaties and agreements through which states assist one another in gathering and exchanging evidence for criminal proceedings. The legal purpose of MLA is to facilitate cross-border cooperation while respecting the sovereignty of participating states. It ensures that evidence obtained in one jurisdiction can be lawfully used in another, thereby supporting transnational criminal justice processes.

Procedurally, MLA frameworks govern requests for evidence collection, witness testimony, asset freezing, and information sharing. Instruments such as the Council of Europe's Budapest Convention on Cybercrime (2001) and various bilateral treaties provide standardized procedures for submitting and processing MLA requests.

However, as Kerr (2013) and Swire and Hemmings (2015) observe, MLA systems are often criticized for their procedural complexity, delays, and limited responsiveness to the speed of digital investigations. In cybercrime cases where evidence may be transient, such delays can significantly undermine investigative effectiveness.

F. Analytical Lens

This article adopts a tripartite analytical framework to examine cross-border cybercrime investigation and digital evidence acquisition. The first dimension is jurisdictional efficiency, which evaluates the ability of legal systems to assert and coordinate authority over transnational cybercrime

cases in a timely and coherent manner.

The second dimension is evidentiary reliability, which focuses on the integrity, authenticity, and admissibility of digital evidence obtained through cross-border processes. This includes considerations of chain of custody, forensic standards, and the impact of jurisdictional fragmentation on evidentiary quality (Casey 2011; Casey and Turnbull 2017).

The third dimension is international cooperation effectiveness, which assesses the functionality of mechanisms such as MLA, extradition treaties, and multilateral frameworks in facilitating timely access to digital evidence. This includes evaluating procedural speed, legal interoperability, and institutional coordination across states. Together, these three analytical lenses provide a comprehensive framework for understanding the structural challenges of cross-border cybercrime investigation in the digital age, particularly in relation to jurisdictional complexity and digital evidence governance.

THE ROLE OF DIGITAL EVIDENCE IN CYBERCRIME PROSECUTION

Digital evidence has become the cornerstone of modern cybercrime prosecution, fundamentally reshaping evidentiary paradigms in criminal justice systems worldwide. Unlike traditional physical evidence, which is tangible and relatively stable, digital evidence is dynamic, distributed, and highly susceptible to alteration. Its evidentiary value lies in its ability to reconstruct digital activities, trace user behavior, and establish connections between actors in cyber environments. As Casey (2011) emphasizes, digital evidence often provides the only viable means of proving criminal conduct in cyberspace, particularly in cases involving hacking, fraud, identity theft, and online financial crimes. Consequently, the effectiveness of cybercrime prosecution is increasingly dependent on the ability of law enforcement agencies and courts to identify, preserve, and interpret digital traces in a legally admissible manner.

A. Categories of Digital Evidence

Digital evidence in cybercrime cases can be classified into several interrelated categories, each of which plays a distinct role in reconstructing criminal activity and establishing legal accountability. Communication data constitutes one of the most significant forms of digital evidence. This category includes emails, instant messaging logs, social media communications, and other forms of electronic correspondence. Such data is frequently used to establish intent, coordination among offenders, and patterns of communication relevant to criminal planning. According to Quick and Choo (2018), communication data often serves as critical corroborative evidence in cybercrime investigations, particularly in cases involving fraud, harassment, or conspiracy.

Transaction records represent another key category of digital evidence, particularly in financial cybercrime cases. These records include banking transactions, cryptocurrency transfers, online payment histories, and e-commerce activities. Transactional data is essential for tracing financial flows, identifying beneficiaries of illicit activities, and establishing monetary harm. Casey and Turnbull (2017) highlight that financial logs often provide a chronological structure that enables investigators to reconstruct the sequence of criminal events.

Device data refers to information extracted from physical devices such as computers, smartphones, tablets, and IoT devices. This includes system logs, installed applications, browsing histories, GPS data, and stored files. Device-level evidence is particularly valuable because it can link specific users to specific actions, thereby strengthening attribution in cybercrime cases. However, as Carrier and Spohn (2018) note, device data must be carefully interpreted within its technical context to avoid misattribution or evidentiary misinterpretation.

Cloud storage data has become increasingly important with the widespread adoption of cloud computing services. This category includes files stored on remote servers, synchronized backups, and distributed datasets hosted by third-party providers. Kerr (2013) argues that cloud-based

evidence presents unique jurisdictional and procedural challenges, as data is often distributed across multiple legal systems and controlled by private corporations. Despite these complexities, cloud storage data is frequently central to modern cybercrime investigations due to its volume and accessibility.

B. Chain of Custody in Digital Context

The chain of custody is a fundamental principle in criminal evidence law that ensures the integrity, authenticity, and reliability of evidence from the moment of collection to its presentation in court. In the context of digital evidence, maintaining an unbroken chain of custody is particularly challenging due to the mutable and replicable nature of electronic data.

The integrity of evidence refers to the assurance that digital data has not been altered, tampered with, or corrupted during collection, storage, or transmission. Unlike physical evidence, digital data can be modified without leaving visible traces, making integrity verification dependent on cryptographic hashing techniques and forensic imaging procedures (Casey 2011).

Authentication processes are essential for establishing that digital evidence is what it purports to be. This involves verifying metadata, timestamps, file origins, and system logs to confirm the authenticity of electronic records. Courts increasingly rely on forensic expert testimony to validate authentication processes, particularly in complex cybercrime cases involving multiple data sources. Forensic handling refers to the procedures used by investigators to collect, preserve, and analyze digital evidence in a manner that preserves its admissibility. This includes the use of write-blocking tools, secure storage environments, and standardized forensic methodologies. As Quick and Choo (2018) emphasize, improper forensic handling can render digital evidence inadmissible, regardless of its probative value.

C. Admissibility Standards

The admissibility of digital evidence in criminal proceedings is governed

by three core criteria: reliability, authenticity, and relevance. These standards ensure that only credible and legally obtained evidence is presented in court.

Reliability refers to the degree to which digital evidence can be trusted as an accurate representation of events or activities. Courts assess reliability by examining the methods used to collect and analyze evidence, as well as the integrity of the underlying technological systems. Brenner (2010) notes that reliability is particularly challenging in cybercrime cases due to the complexity of digital systems and the potential for technical errors.

Authenticity requires that digital evidence be demonstrably linked to its source and that it has not been altered or fabricated. This often involves the use of digital signatures, hash values, and forensic validation techniques. As Casey and Turnbull (2017) argue, authenticity is one of the most frequently contested issues in cybercrime litigation, particularly in cases involving metadata manipulation or deepfake technologies.

Relevance ensures that digital evidence has a direct bearing on the facts in issue within a criminal case. Even highly reliable and authentic evidence may be excluded if it does not contribute meaningfully to establishing guilt or innocence. The principle of relevance thus serves as a limiting mechanism to prevent the introduction of excessive or prejudicial digital material.

D. Challenges in Digital Evidence Preservation

Despite its critical importance, the preservation of digital evidence presents significant technical and legal challenges that complicate cybercrime prosecution. One of the most pressing challenges is the risk of data deletion. Digital evidence can be intentionally or unintentionally erased through user actions, system processes, or automated data management policies. In cloud environments, data retention policies may lead to automatic deletion after a specified period, further complicating preservation efforts.

Encryption represents another major obstacle. End-to-end encryption technologies, widely used in communication platforms such as WhatsApp, Signal, and Telegram, prevent unauthorized access to data even when it is lawfully obtained by investigators. While encryption enhances privacy and security, it simultaneously restricts law enforcement access to potentially

critical evidence (Abelson et al. 2015).

The volatility of digital data further exacerbates preservation challenges. Unlike physical evidence, digital information can change rapidly due to system updates, user interactions, or background processes. Volatility is particularly acute in volatile memory (RAM), where data is lost when devices are powered off. Casey (2011) highlights that timely acquisition is essential to prevent the loss of transient digital evidence.

Collectively, these challenges underscore the fragile nature of digital evidence and highlight the need for advanced forensic methodologies, robust legal frameworks, and international cooperation mechanisms to ensure effective cybercrime prosecution in the digital age.

LEGAL AND PRACTICAL CHALLENGES IN CROSS-BORDER EVIDENCE ACQUISITION

A. Jurisdictional Barriers

Jurisdictional fragmentation constitutes the foundational legal obstacle in cross-border cybercrime investigation, primarily because the internet dismantles the classical alignment between territory, authority, and enforcement capacity. In traditional criminal law, jurisdiction is anchored in territorial sovereignty, yet cyber operations routinely span multiple states simultaneously, making it difficult to locate the "place" of the offense. As Brenner (2010) argues, cybercrime fundamentally destabilizes the territorial logic of criminal jurisdiction because acts may be initiated in one state, executed through servers in another, and produce harm in a third. This creates overlapping assertions of authority, particularly when states apply effects doctrine or nationality principles to justify extraterritorial reach.

The problem is further intensified by the absence of global harmonization in cybercrime legislation. Although instruments such as the Budapest Convention attempt to standardize substantive and procedural rules, significant divergences persist regarding investigative powers, privacy thresholds, and data access rules (Clough 2015). These inconsistencies produce legal uncertainty in determining which state has priority over

evidence collection. As Swire and Hemmings (2015) note, jurisdictional overlap frequently leads not to cooperation but to institutional paralysis, where no single authority can act decisively without risking violation of another state's sovereignty or domestic law.

B. Mutual Legal Assistance Treaty (MLAT) Limitations

Mutual Legal Assistance Treaties (MLATs) remain the dominant formal mechanism for transnational evidence gathering, yet their operational design reflects a pre-digital era characterized by slower forms of criminal activity. In cybercrime investigations, this structural mismatch becomes particularly problematic because digital evidence is often transient and requires immediate preservation. Kerr (2013) observes that MLAT processes typically involve multiple bureaucratic layers, including central authorities, diplomatic channels, and judicial review mechanisms, all of which contribute to significant delays.

Empirical assessments by the Council of Europe (2020) and UNODC (2020) consistently demonstrate that MLAT response times can extend from several weeks to months, rendering them ineffective in urgent cyber incidents such as ransomware attacks or financial fraud schemes where data may be deleted or encrypted within hours. Brenner (2010) further argues that cybercrime operates at "network speed," whereas MLATs function at "bureaucratic speed," producing a structural temporal gap that undermines investigative effectiveness. Consequently, law enforcement agencies increasingly bypass MLAT channels in favor of informal cooperation or direct requests to service providers, raising new legal concerns regarding due process and sovereignty.

C. Data Localization and Sovereignty Issues

Data localization laws have emerged as a central expression of digital sovereignty, reflecting state efforts to retain control over data generated within their territory. These laws require data to be stored, processed, or accessed within national borders, often justified by privacy protection, cybersecurity, or national security imperatives (Kuner 2017). However, in the

context of cross-border cybercrime investigation, such regulations introduce significant operational constraints by restricting access to evidence stored abroad or controlled by foreign entities.

The tension between data sovereignty and investigative necessity becomes particularly acute in cloud computing environments, where data is dynamically distributed across multiple jurisdictions. De Hert and Papakonstantinou (2016) argue that this "data fragmentation" undermines traditional legal assumptions about territorial control, as no single state can claim exclusive authority over cloud-based information. Moreover, conflicting national data protection regimes may prevent lawful cross-border transfers, even when such transfers are necessary for criminal investigations. This creates a paradox in which legal frameworks designed to enhance data protection simultaneously hinder legitimate law enforcement access, thereby complicating the balance between privacy rights and criminal justice needs.

D. Role of Private Technology Companies

Private technology companies have become de facto gatekeepers of digital evidence due to their control over global communication and data infrastructure. Major platform providers such as Google, Meta, Microsoft, and Amazon possess centralized access to vast datasets that are often critical in cybercrime investigations. This structural dependency effectively privatizes key aspects of law enforcement, shifting evidentiary control from states to corporate actors (Zuboff 2019).

However, this privatization introduces significant legal and normative tensions. Technology companies are frequently subject to conflicting legal obligations across jurisdictions, particularly when one state's legal order mandates disclosure while another prohibits it under privacy or data protection laws. Kerr and Swire (2020) describe this phenomenon as "cross-border legal conflict of laws," where compliance with one jurisdiction may result in violation of another. As a result, companies are placed in a quasi-judicial position, forced to interpret and balance competing sovereign demands.

This dynamic raises broader concerns regarding accountability and

transparency. Unlike public authorities, private companies are not democratically accountable, yet they play a decisive role in determining access to critical evidence. Swire and Hemmings (2015) argue that this shift reflects a broader transformation in governance, where regulatory authority is increasingly dispersed across hybrid public-private networks, complicating traditional notions of state-centric criminal justice.

E. Encryption and Access Barriers

Encryption technologies, particularly end-to-end encryption (E2EE), represent one of the most significant technical barriers to digital evidence acquisition in modern cybercrime investigations. E2EE ensures that only communicating users can access message content, rendering interception by third parties—including service providers and law enforcement—technically infeasible. While encryption is widely recognized as essential for safeguarding privacy and securing digital communications, it simultaneously limits investigative capacity in serious criminal cases (Abelson et al. 2015).

The so-called "lawful access" debate centers on whether governments should mandate exceptional access mechanisms, such as encryption backdoors, to facilitate criminal investigations. However, leading cryptography scholars warn that such mechanisms introduce systemic vulnerabilities that can be exploited by malicious actors, thereby weakening overall cybersecurity (Abelson et al. 2015; Greenwald 2014). Brenner (2010) further argues that the erosion of strong encryption could have unintended consequences, including increased exposure to cyberattacks, financial fraud, and state surveillance abuse. This creates a structural dilemma between security enforcement and digital rights protection, with no universally accepted resolution.

F. Evidentiary Standard Divergence

Cross-border cybercrime investigations are also hindered by significant divergence in evidentiary standards across jurisdictions. Legal systems differ in their requirements for admissibility, authentication, and evaluation of digital evidence, creating inconsistencies in transnational prosecutions. For

instance, some jurisdictions require strict forensic validation and documented chain-of-custody procedures, while others adopt more flexible evidentiary thresholds based on judicial discretion (Casey 2011).

These differences create substantial procedural friction when evidence collected in one jurisdiction must be presented in another. Carrier and Spohn (2018) highlight that variations in forensic methodology and expert testimony standards can lead to exclusion of critical digital evidence, even when it is technically reliable. Furthermore, Casey and Turnbull (2017) emphasize that the lack of global forensic standardization undermines evidentiary interoperability, limiting the effectiveness of international cooperation mechanisms. As a result, digital evidence often loses probative value when transferred across jurisdictions, not because of its intrinsic unreliability, but due to incompatible legal frameworks. This fragmentation underscores the need for greater harmonization of digital forensic standards at the international level.

G. Time Sensitivity of Cybercrime Investigation

Time sensitivity represents a defining feature of cybercrime investigations and constitutes one of the most critical challenges in cross-border evidence acquisition. Digital evidence is inherently volatile and may be deleted, encrypted, or overwritten within extremely short timeframes. Cloud service providers often implement automated data retention and deletion policies, further accelerating evidence decay.

This temporal fragility creates a fundamental mismatch between the urgency of cyber incidents and the procedural timelines of international legal cooperation. Kerr (2013) and UNODC (2020) both emphasize that while cyberattacks such as ransomware or financial fraud require immediate intervention, formal mechanisms such as MLATs operate on extended timelines that are incompatible with real-time investigative needs. Brenner (2010) describes this as a "temporal disjunction" between network-speed crime and law-speed enforcement.

Consequently, delays in obtaining evidence frequently result in irreversible loss of critical data, undermining both investigative outcomes

and judicial proceedings. This reinforces the broader argument that existing legal infrastructures are not merely inefficient but structurally misaligned with the operational realities of digital crime.

EVALUATION OF EXISTING INTERNATIONAL COOPERATION FRAMEWORKS

A. Mutual Legal Assistance Treaties (MLAT)

Mutual Legal Assistance Treaties (MLATs) remain the doctrinal backbone of cross-border criminal cooperation and continue to embody the classical model of state-centric international criminal law enforcement. Their primary strength lies in their legal legitimacy, as MLATs are grounded in formally negotiated bilateral or multilateral agreements that respect the sovereignty of participating states. This sovereignty-preserving structure is normatively significant because it ensures that cross-border investigative actions are conducted through mutually recognized legal channels rather than unilateral assertions of jurisdiction. As Kerr (2013) observes, MLATs institutionalize inter-state trust by requiring judicial and diplomatic oversight, thereby protecting fundamental principles of due process and non-intervention.

However, this same structural design generates profound inefficiencies in the context of cybercrime. The procedural architecture of MLATs is inherently linear, hierarchical, and bureaucratic, requiring requests to pass through centralized authorities, translation stages, and legal vetting procedures in both requesting and receiving states. This results in systemic delays that are incompatible with the temporal dynamics of digital evidence, which may be deleted, encrypted, or relocated within minutes or hours. Brenner (2010) argues that this mismatch between "legal time" and "network time" renders MLATs structurally obsolete for many categories of cybercrime. Consequently, while MLATs preserve legal order, they often fail to preserve evidence, producing a paradox in which procedural legality undermines substantive justice.

B. Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime represents the most comprehensive international effort to harmonize substantive and procedural cybercrime law. Its primary achievement lies in establishing a shared normative and procedural framework for cybercrime offenses, investigative powers, and international cooperation. Clough (2015) emphasizes that the Convention has significantly contributed to the convergence of legal definitions and facilitated cooperation among signatory states, particularly in areas such as data preservation, expedited assistance, and transborder access to stored data with consent.

Nevertheless, the Convention's effectiveness is constrained by its limited global participation and uneven implementation. Many major cyber powers and developing states are not parties to the Convention, resulting in a fragmented global legal landscape. Moreover, even among signatories, implementation varies significantly due to differences in domestic legal systems, institutional capacity, and political priorities. Schjølberg (2017) notes that the Convention's reliance on domestic incorporation mechanisms leads to inconsistent enforcement standards, thereby weakening its harmonizing ambition. As a result, while the Budapest framework provides a normative blueprint for cooperation, it lacks universal binding force, limiting its capacity to function as a truly global cybercrime governance regime.

C. European Union Frameworks

The European Union has developed one of the most advanced regional regimes for cross-border digital evidence acquisition, particularly through the proposed E-Evidence Regulation and associated instruments for cross-border data access. These frameworks aim to streamline cooperation by enabling direct requests for electronic evidence between judicial authorities and service providers across member states, thereby bypassing traditional MLAT procedures.

From a functional perspective, the EU approach represents a significant shift toward efficiency-oriented legal design. By reducing intermediaries and

introducing standardized production orders, the system seeks to address the temporal limitations of traditional cooperation mechanisms. However, this efficiency-driven model also raises normative concerns regarding proportionality, judicial oversight, and fundamental rights protection. De Hert and Papakonstantinou (2016) argue that while the E-Evidence framework enhances operational speed, it risks weakening procedural safeguards if not properly balanced with robust accountability mechanisms.

Furthermore, the EU model remains geographically limited and cannot be easily generalized to global cybercrime governance due to its high level of legal integration and shared constitutional principles. Its success depends heavily on the existence of supranational legal authority, which is absent in most other regions.

D. United States Approach

The United States has adopted a more unilateral and extraterritorial approach to cross-border digital evidence through the Clarifying Lawful Overseas Use of Data (CLOUD) Act. This legislation authorizes U.S. law enforcement agencies to compel domestic service providers to produce data stored abroad, provided certain legal thresholds are met. From an efficiency standpoint, the CLOUD Act significantly accelerates access to digital evidence by bypassing traditional MLAT processes.

However, this extraterritorial model introduces complex tensions in international law. Schünemann (2018) argues that such unilateral data access mechanisms challenge the sovereignty of foreign states by asserting jurisdiction over data physically located outside national territory. This creates potential conflicts with local data protection laws and raises concerns about legal fragmentation. Additionally, while the CLOUD Act includes provisions for executive agreements with foreign governments, its implementation remains selective and politically contingent. Thus, the U.S. approach reflects a functional prioritization of investigative efficiency over multilateral legal harmonization, reinforcing a trend toward fragmented and power-based rather than rule-based global cyber governance.

E. ASEAN Cooperation

In contrast to the EU and U.S. frameworks, ASEAN cooperation in cybercrime investigation remains relatively underdeveloped and heavily reliant on bilateral agreements and informal coordination mechanisms. While ASEAN member states have adopted various declarations and soft-law instruments on cybersecurity cooperation, these initiatives lack binding legal force and institutional enforcement mechanisms.

The absence of deep legal harmonization within ASEAN results in significant disparities in cybercrime legislation, procedural law, and data governance standards. As Jaishankar (2019) notes, this legal diversity limits the region's capacity to respond effectively to transnational cyber threats. Furthermore, reliance on bilateral arrangements creates fragmentation, as cooperation depends on individual state relationships rather than a unified regional framework.

This structural limitation becomes particularly problematic in cases involving rapidly evolving cyber threats, where delays in coordination can significantly hinder investigative outcomes. Consequently, ASEAN remains dependent on external frameworks such as MLATs and international conventions, rather than functioning as a self-sufficient regional cybercrime governance regime.

F. Critical Assessment

A comprehensive evaluation of existing international cooperation frameworks reveals a deeply fragmented and structurally inconsistent global cyber law architecture. Despite the presence of multiple instruments—ranging from MLATs and the Budapest Convention to regional EU mechanisms and unilateral U.S. legislation—there is no coherent global system governing cross-border digital evidence acquisition. This fragmentation results in overlapping jurisdictions, inconsistent procedural standards, and competing sovereignty claims, all of which undermine investigative efficiency and legal certainty.

The absence of a unified evidentiary regime is particularly critical.

Digital evidence requires harmonized standards for collection, authentication, preservation, and admissibility, yet current frameworks diverge significantly in these domains. Casey (2011) and Carrier and Spohn (2018) emphasize that without standardized forensic and evidentiary protocols, cross-border cooperation will continue to produce legally fragile outcomes. Moreover, Swire and Hemmings (2015) argue that the lack of institutional interoperability between legal systems creates systemic inefficiencies that cannot be resolved through incremental reform alone. Ultimately, the existing international architecture reflects a transitional governance phase in which traditional sovereignty-based legal structures are increasingly misaligned with the technological realities of cyberspace. This misalignment suggests the need for a more integrated, hybrid, and possibly supranational approach to cybercrime cooperation that balances efficiency, sovereignty, and fundamental rights protection.

TOWARD AN EFFECTIVE CROSS-BORDER DIGITAL EVIDENCE FRAMEWORK

The structural inadequacies of existing cross-border evidence regimes reveal a fundamental governance gap between the pace of digital criminal activity and the procedural rigidity of international legal cooperation. As demonstrated in previous sections, Mutual Legal Assistance Treaties (MLATs), regional instruments, and unilateral legislative approaches remain fragmented, slow, and normatively inconsistent. Against this backdrop, this section develops an integrated framework for cross-border digital evidence governance that seeks to reconcile four competing imperatives: legality, sovereignty, efficiency, and technological realism. The proposed model does not aim to replace existing institutions but to recalibrate them toward a more adaptive, layered, and interoperable system of cooperation.

A. Normative Principles

Any effective framework for cross-border digital evidence must be grounded in a coherent set of normative principles that guide both state

behavior and institutional design. First, the rule of law remains the foundational principle, requiring that all data access and evidence collection activities be subject to clear legal authorization, judicial oversight, and procedural safeguards. As Kerr (2013) emphasizes, legitimacy in digital investigations depends not only on outcomes but on adherence to due process standards that ensure accountability and prevent arbitrary surveillance.

Second, sovereignty balance is essential in preserving state equality in international law while recognizing the transnational nature of digital infrastructure. Rather than absolute territorial control, sovereignty must be reinterpreted as shared and distributed authority over digital ecosystems (Schünemann 2018). Third, proportionality functions as a limiting principle to ensure that investigative powers are exercised in a manner that is necessary, suitable, and minimally intrusive, particularly in relation to privacy-sensitive data (De Hert and Papakonstantinou 2016). Finally, the urgency principle reflects the operational reality of cybercrime, where digital evidence may be lost within hours. This principle justifies accelerated procedures for evidence preservation and access in exigent circumstances, thereby bridging the gap between legal process and technological temporality (UNODC 2020).

B. Reforming Mutual Legal Assistance

The modernization of Mutual Legal Assistance frameworks is essential for maintaining their relevance in digital investigations. The traditional MLAT model, characterized by diplomatic channels and multi-layered approvals, is structurally incompatible with the speed requirements of cybercrime enforcement. A reformed system must therefore adopt streamlined procedures that eliminate redundant bureaucratic steps while preserving judicial oversight.

A key innovation is the development of a digital-first MLAT system, in which all requests are submitted, processed, and executed through secure interoperable digital platforms. This would significantly reduce processing time while improving transparency and traceability. Additionally, time-bound request mechanisms should be introduced, requiring receiving states

to respond within fixed legal deadlines, particularly for data preservation requests. As Kerr and Swire (2020) argue, procedural time limits are essential to prevent the loss of volatile digital evidence and to ensure operational effectiveness. The following table summarizes the proposed MLAT reform structure as shown on Table 1.

TABLE 1. Proposal for MLAT System

Component	Current MLAT System	Proposed Digital-First MLAT System
Request submission	Paper-based / diplomatic channels	Secure digital platform
Processing time	Weeks to months	Time-bound (24–72 hours for urgent cases)
Coordination	Central authorities only	Direct judicial + digital liaison
Transparency	Limited tracking	Real-time case tracking system
Responsiveness	Low	High (urgency-based tiers)

This transformation reflects a shift from procedural rigidity to adaptive legal interoperability, ensuring that MLATs remain relevant in the digital era.

C. Direct Data Access Mechanisms

Beyond MLAT reform, the increasing centrality of private technology companies necessitates the development of regulated direct data access mechanisms. These mechanisms allow law enforcement agencies to obtain digital evidence directly from service providers under predefined legal frameworks, thereby bypassing traditional inter-state channels.

Such lawful direct access agreements must be carefully designed to balance efficiency with sovereignty and privacy protections. The U.S. CLOUD Act provides a partial precedent for such arrangements, enabling executive agreements with foreign governments to facilitate cross-border data access. However, as Zuboff (2019) warns, unregulated direct access risks reinforcing corporate-state surveillance architectures without adequate democratic accountability.

Regulated access to cloud data should therefore include strict judicial authorization requirements, audit trails, and data minimization principles. Moreover, access should be limited to specific categories of serious crime, ensuring proportionality in enforcement. This model reflects a shift from state-to-state cooperation toward state-to-platform governance, recognizing the structural role of technology companies as custodians of critical evidentiary infrastructure (Swire and Hemmings 2015).

D. Standardization of Digital Evidence

A major impediment to cross-border digital investigations is the lack of standardized forensic and evidentiary protocols. Without harmonized standards, evidence collected in one jurisdiction may be deemed inadmissible in another, undermining transnational prosecutions. Therefore, global standardization of digital evidence practices is essential.

Global forensic standards should include uniform protocols for evidence collection, preservation, analysis, and presentation. These standards must be technologically neutral but methodologically consistent, ensuring that digital evidence maintains integrity across jurisdictions. Casey (2011) emphasizes that chain-of-custody integrity is central to evidentiary reliability and must be preserved through standardized forensic procedures.

Interoperability of evidence systems is equally important. This involves creating technical and legal frameworks that allow different national systems to exchange and verify digital evidence seamlessly. The following table outlines the proposed standardization architecture, see Table 2.

TABLE 2. Standardization of Digital Evidence

Dimension	Current System	Proposed Standardized System
Forensic protocols	Nationally fragmented	Global baseline standards
Evidence integrity	Variable	Cryptographic verification mandatory
System interoperability	Limited	Cross-border compatible platforms
Chain of custody	Inconsistent	Unified digital logging system

Such standardization would significantly reduce evidentiary disputes and enhance judicial confidence in digital evidence.

E. Strengthening Role of Technology Companies

Given their central role in digital infrastructure, technology companies must be formally integrated into cross-border evidence governance frameworks. This requires the establishment of mandatory compliance regimes that define their responsibilities in data preservation, disclosure, and transparency.

First, mandatory compliance frameworks should require platforms to respond to lawful requests within defined timeframes, particularly in urgent cybercrime cases. Second, transparency obligations should ensure that companies publish regular reports on government data requests, enhancing public accountability. Third, data preservation duties must require platforms to retain potentially relevant data upon receipt of preservation orders, preventing its deletion during ongoing investigations.

As De Hert and Gutwirth (2017) argue, private actors increasingly function as "quasi-regulators" of data access, necessitating corresponding accountability structures. However, these obligations must be carefully calibrated to avoid excessive burden and to ensure compliance with international human rights standards.

F. International Cybercrime Courts or Cooperation Bodies

An emerging conceptual proposal in cybercrime governance is the establishment of centralized international cooperation bodies or even specialized cybercrime courts. Such institutions would serve as supranational coordination mechanisms capable of resolving jurisdictional conflicts, authorizing cross-border data access, and standardizing evidentiary procedures.

While ambitious, this model reflects the increasing inadequacy of purely bilateral or regional cooperation frameworks. A centralized body could

function as a clearinghouse for urgent digital evidence requests, ensuring faster and more consistent responses. It could also develop authoritative guidelines on digital evidence admissibility and forensic standards. However, the feasibility of such institutions remains contested due to sovereignty concerns and political resistance. Nevertheless, as Schünemann (2018) suggests, the evolution of digital sovereignty may eventually necessitate partial supranational governance structures to manage transnational cyber threats effectively.

G. Proposed Integrated Model

The proposed framework integrates four interdependent layers designed to address the structural weaknesses of current systems while maintaining legal legitimacy and operational efficiency:

1. Enhanced MLAT System (Modernized Layer)
   A digital-first, time-bound, and transparent MLAT mechanism that preserves inter-state legal cooperation while improving responsiveness.
2. Direct Access Agreements (Platform Layer)
   Regulated mechanisms enabling lawful access to data held by technology companies under strict judicial and proportionality safeguards.
3. Platform Cooperation Obligations (Private Governance Layer)
   Mandatory compliance, transparency reporting, and data preservation duties imposed on digital service providers.
4. Standardized Digital Forensic Protocols (Technical-Legal Layer)
   Global harmonization of forensic methodologies, chain-of-custody standards, and evidence interoperability systems.

Collectively, these four layers form an integrated governance ecosystem that balances sovereignty, efficiency, and rights protection. The model recognizes that no single instrument—whether MLAT, unilateral legislation, or platform regulation—is sufficient on its own. Instead, effective governance requires a multi-layered architecture capable of adapting to the dynamic and transnational nature of cybercrime.

FUTURE CHALLENGES IN TRANSNATIONAL CYBERCRIME INVESTIGATION

The trajectory of cybercrime evolution suggests that cross-border criminal investigations will become increasingly complex due to the rapid transformation of digital infrastructures and emerging technologies. While existing legal frameworks already struggle with cloud computing, encryption, and jurisdictional fragmentation, future developments in cloud-native architectures, artificial intelligence, blockchain systems, and quantum computing are likely to further destabilize traditional evidentiary and jurisdictional assumptions. As Brenner (2010) argues, cybercrime is not static but structurally adaptive, continuously evolving in response to technological innovation and regulatory pressure. This adaptive nature necessitates a forward-looking legal analysis that anticipates—not merely reacts to—technological disruption.

Cloud-native crime infrastructure represents a significant shift in the operational environment of cybercriminal activity. Unlike earlier forms of cybercrime that relied on discrete servers or identifiable endpoints, cloud-native systems operate through distributed, elastic, and globally redundant architectures. Criminal actors increasingly exploit infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and anonymized cloud environments to mask attribution and fragment evidentiary trails. This decentralization complicates traditional investigative models that rely on physical server identification and territorial data localization. As Kerr and Swire (2020) note, the migration of data across jurisdictions in real time renders static legal concepts of "data location" increasingly obsolete, thereby challenging the foundational logic of cross-border evidence acquisition.

Artificial intelligence further intensifies the complexity of transnational cybercrime by enabling automation, scalability, and behavioral adaptation in criminal operations. AI-driven cybercrime systems can generate phishing content, optimize social engineering strategies, and dynamically adapt malware behavior based on defensive responses. This introduces a level of

autonomy that blurs the distinction between human intent and machine execution. Zuboff (2019) highlights that algorithmic systems not only process data but actively shape behavioral outcomes, suggesting that AI-enabled cybercrime may evolve into self-optimizing criminal ecosystems. This raises profound legal questions regarding attribution, culpability, and evidentiary interpretation, particularly when malicious actions are partially or fully generated by autonomous systems.

Blockchain-based systems introduce a different set of evidentiary and investigative challenges due to their decentralized, immutable, and pseudonymous nature. While blockchain technology is often associated with transparency, its pseudonymity creates significant obstacles for law enforcement agencies attempting to trace illicit financial flows or identify perpetrators. Cryptocurrencies and decentralized finance (DeFi) platforms enable cross-border value transfer without reliance on centralized intermediaries, thereby complicating traditional asset tracing mechanisms. Casey (2011) emphasizes that digital evidence must be both authentic and attributable, yet blockchain systems deliberately obscure attribution through cryptographic abstraction. Furthermore, the immutability of blockchain records complicates legal correction mechanisms, even when illicit activity is later identified.

Quantum computing represents a more distant but potentially transformative challenge to cybersecurity and digital evidence integrity. If realized at scale, quantum computing could undermine widely used cryptographic protocols, including those securing digital communications, financial transactions, and forensic data storage. Abelson et al. (2015) warn that cryptographic stability is foundational to digital trust systems, and any disruption to encryption standards would have cascading effects on evidence preservation and authentication. In a post-quantum environment, previously secure digital evidence may become vulnerable to retrospective decryption or manipulation, raising concerns about long-term evidentiary reliability and chain-of-custody integrity. This introduces a temporal paradox in which evidence considered secure at the time of collection may later become compromised due to technological advancement.

Collectively, these technological developments underscore the urgent need for adaptive legal frameworks capable of responding to continuous innovation in cybercrime methodologies. Traditional legal systems, which are largely reactive and territorially bounded, are increasingly misaligned with the fluid and transnational nature of digital threats. Brenner (2010) argues that cybercrime law must evolve toward a dynamic governance model that integrates technological foresight, regulatory flexibility, and international coordination. Similarly, Schünemann (2018) suggests that digital sovereignty must be reconceptualized as a shared and adaptive legal construct rather than a fixed territorial principle.

An adaptive legal framework would require several key features. First, it must incorporate anticipatory regulation, enabling lawmakers to design rules that account for emerging technologies before they are fully weaponized by criminal actors. Second, it must adopt modular governance structures capable of updating evidentiary standards and investigative procedures in response to technological change. Third, it must enhance international interoperability to ensure that legal responses remain effective across jurisdictions. Finally, it must integrate continuous risk assessment mechanisms to evaluate the evolving impact of technologies such as AI, blockchain, and quantum computing on criminal justice systems.

Therefore, the future of transnational cybercrime investigation will be defined by increasing technological sophistication and corresponding legal uncertainty. Without adaptive and forward-looking governance structures, existing legal frameworks risk becoming progressively irrelevant in the face of rapidly evolving digital threats. The convergence of cloud-native infrastructures, AI-driven automation, blockchain decentralization, and quantum cryptographic disruption signals not only an escalation in cybercrime capabilities but also a fundamental transformation in the nature of digital evidence and legal accountability.

CONCLUSION

The investigation of cross-border cybercrime reveals a structural tension

between territorially bounded legal systems and the borderless architecture of digital communication. While cybercrime operates through distributed infrastructures, cloud environments, and real-time transnational networks, existing legal frameworks remain largely anchored in sovereignty-based cooperation mechanisms such as Mutual Legal Assistance Treaties. This mismatch produces persistent operational inefficiencies, particularly in the acquisition, preservation, and admissibility of digital evidence. As demonstrated throughout the analysis, jurisdictional fragmentation, procedural delays, and divergent evidentiary standards collectively weaken the effectiveness of international criminal justice responses. In this context, the central problem is not merely the absence of cooperation, but the structural incompatibility between traditional legal timeframes and the speed of digital evidence volatility (Brenner 2010; Kerr 2013).

The study further shows that although instruments such as the Budapest Convention and emerging unilateral or regional mechanisms (such as the CLOUD Act and EU E-Evidence framework) represent important innovations, they remain partial and fragmented responses to a global problem. No single framework currently provides a coherent, universal regime capable of ensuring both efficient access to digital evidence and the protection of fundamental rights. Instead, the global governance landscape is characterized by legal pluralism, institutional asymmetry, and competing sovereignty claims. This fragmentation reinforces evidentiary uncertainty and undermines the reliability of cross-border prosecutions, particularly in urgent cybercrime cases where time-sensitive data may be lost before lawful access is completed (Swire and Hemmings 2015; De Hert and Papakonstantinou 2016).

In conclusion, the findings of this article underscore the urgent need for a reconfiguration of international cooperation mechanisms toward a more integrated, adaptive, and technologically responsive framework. Such a framework must reconcile sovereignty with operational efficiency, while embedding robust safeguards for due process, privacy, and evidentiary integrity. Without such reform, cross-border cybercrime investigations will continue to be constrained by procedural rigidity and jurisdictional

fragmentation, thereby weakening the global capacity to respond effectively to increasingly sophisticated digital threats.

ACKNOWLEDGMENTS

None.

FUNDING INFORMATION

None.

CONFLICTING INTEREST AND ORGINALITY STATEMENT

The authors state that there is no conflict of interest in the publication of this article.

GENERATIVE AI STATEMENT

None.

REFERENCES

Abelson, Harold, Ross Anderson, Steven M. Bellovin, et al. 2015. *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*. Washington, DC: MIT Press.

Brenner, Susan W. 2010. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, CA: Praeger.

Brenner, Susan W., and Leo Clarke. 2019. *Cybercrime Investigation Methods*. Aspen Publishing.

Carrier, Michael A., and Cassia C. Spohn. 2018. *Digital Evidence and Criminal Justice*. New York: Routledge.

Casey, Eoghan, and Benjamin Turnbull. 2017. *Advanced Digital Forensics Analysis*. London: Syngress.

Casey, Eoghan. 2011. *Digital Evidence and Computer Crime*. 3rd ed. Amsterdam: Academic Press.

Cassese, Antonio. 2008. *International Criminal Law*. 2nd ed. Oxford: Oxford

University Press.
Clough, Jonathan. 2015. *Principles of Cybercrime*. Cambridge: Cambridge University Press.
Council of Europe. 2001. *Convention on Cybercrime (Budapest Convention)*. Strasbourg.
Council of Europe. 2020. *Cybercrime Convention Committee (T-CY) Guidance on Mutual Legal Assistance*. Strasbourg: Council of Europe.
De Hert, Paul, and Serge Gutwirth. 2017. *Privacy and Data Protection Governance*. Springer.
De Hert, Paul, and Vagelis Papakonstantinou. 2016. "The Data Protection Regime and Cross-Border Data Flows." *Computer Law & Security Review* 32 (2): 193–210.
De Hert, Paul, and Vagelis Papakonstantinou. 2018. "E-Evidence and Digital Rule of Law." *European Law Review* 43 (3): 389–412.
Governance and Digital Evidence Report. United Nations.
Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.
Jaishankar, K. 2019. *Cyber Criminology in the ASEAN Context*. Routledge.
Kerr, Orin S. 2013. "The Next Generation Communications Privacy Act." *Texas Law Review* 92 (2): 1–45.
Kerr, Orin S., and Peter Swire. 2020. "Cross-Border Data Requests and Conflicts of Law." *Harvard Law Review Forum* 133: 1–25.
Kuner, Christopher. 2017. *Transborder Data Flows and Data Privacy Law*. Oxford University Press.
Ohm, Paul. 2010. "Broken Promises of Privacy." *UCLA Law Review* 57: 1701–1777.
Quick, Darren, and Kim-Kwang Raymond Choo. 2018. *Digital Forensics and Investigations*. Springer.
Rahmawati, Ulfah Dwi, et al. 2024. "Digital Transformation in Case Handling: A Juridical Review of Technology Utilization in the Justice System in Indonesia and Malaysia." *Unnes Law Journal* 10(1): 43-80.
Saputra, Rian, Josef Purwadi Setiodjati, and Jaco Barkhuizen. 2023. "Under-Legislation in Electronic Trials and Renewing Criminal Law

Enforcement in Indonesia (Comparison with United States)." *Journal of Indonesian Legal Studies* 8(1): 243-288.

Schjølberg, Stein. 2017. *The History of the Budapest Convention on Cybercrime*. Oslo Cybercrime Conference Papers.

Schünemann, Bernd. 2018. *International Criminal Law and Digital Sovereignty*. Berlin: Springer.

Shaw, Malcolm N. 2017. *International Law*. 8th ed. Cambridge: Cambridge University Press.

Solove, Daniel J. 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Swire, Peter, and Justin Hemmings. 2015. "Mutual Legal Assistance in an Era of Globalized Communications." *New York University Law Review* 90 (5): 123–189.

UNODC. 2020. *Cybercrime Investigation and Evidence Sharing Report*. United Nations.

UNODC. 2020. *Global Cybercrime Cooperation Report*. United Nations.

UNODC. 2021. *Global Cybercrime Governance Report*. United Nations.

Wall, David S. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Yar, Majid. 2013. *Cybercrime and Society*. London: Sage.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. New York: PublicAffairs.

This page intetionally left blank