UCP Journal *of* Law & Legal Education
Vol. 3, Issue 3 (July – December 2025)

Cross-Border Cybercrime Investigations: Legal Challenges and The Impact of Distinct National Laws on Digital Evidence and Admissibility

Amayal Chaudhary*, Muhammad Abdullah Asghar*

Abstract

Cybercrime has evolved into a worldwide surge that poses a threat to law enforcement agencies. Transnational operations and procedural gaps constrain states. There are traditional approaches like the Mutual Legal Assistance Treaties (MLATS), but they have proved outdated in the modern cyber investigation global regime. Divergence in national laws hinders the effective execution of a multilateral and universal approach on a global level. These data breaches and insecurities can threaten a state's sovereignty and can exacerbate capacity deficits. This research paper examines these legal and practical barriers to cross-border cybercrime investigation with a focus on the collection, preservation, transfer, and admissibility of digital evidence. Key questions discuss the impediments to developing mutual strategies and the admissibility of digital evidence, limitations to existing instruments like the Budapest Convention, which are significant to address in the modern regime. A qualitative doctrinal approach has been used, and an in-depth analysis has been made of legal instruments (including the Budapest Convention and its Second Additional Protocol), national laws, court cases (e.g., the 2018 Microsoft Ireland case), institutional reports (UNODC, INTERPOL), and scholarly literature. The paper recommends full ratification and domestic harmonisation of the Budapest Convention and its Second Additional Protocol, accelerated shifts from MLATs to direct access frameworks with timelines, enhanced public-private partnerships, substantial capacity-building investments (especially in training and forensics), and diplomatic efforts to bridge geopolitical divides

* Final Year Law Student Affiliation: University of the Punjab, Lahore, Pakistan. Email: amayalch@gmail.com
** Advocate, Associate at Ahmer Bilal Soofi & Co., Lahore, Pakistan. Email: abdullah.asghar2651430@yahoo.com
Article History: Received: 08-05-2025; Received in revised form: 29-03-2026; Accepted: 30-05-2026. Available online: 08-06-2026
DOI: https://doi.org/10.24312/ucp-jlle.03.03.546

for greater policy harmonisation. These measures are essential to strengthen transnational enforcement while upholding due process and sovereignty. Coordinated legal, technical, and diplomatic efforts are of utmost importance.

Keywords: Cybercrime Investigation, Digital Evidence, Transnational Law Enforcement, Cybersecurity Regulations, Policy Harmonisation

Introduction

A crucial report was released in the year 2019 by the institutes Accenture and Ponemon, both highly influential in the fields of business technology and cybersecurity. It very conclusively highlighted the growing economic toll of cybercrime, noting that costs were rising exponentially amid the increasing pervasiveness of attacks ("Accenture/Ponemon Institute: The cost of cybercrime," 2019). These threats were categorised into diverse actors, extending up to recognising the devastating acts of non-state terrorist groups. These were named as organised crime syndicates, state-sponsored entities and individuals driven by corporate, ideological, political, or other motives. Countries all over the world struggle to respond effectively, mainly due to the porosity in the fabric of collection, preservation, analysis and admissibility of digital evidence. It is the fabric on which the very system of prosecuting these individuals lies. It is a critical bottleneck. The law enforcement agencies, prosecutors and judges frequently lack the specialised or even the standardised skills to handle the electronic evidence reliably and effectively. Effective in such a manner that it can substantiate the evidence required for prosecution, which it lacks by far from the barest of margins. The United Nations Office on Drugs and Crime (UNODC) Comprehensive Study on Cybercrime (2013) already documented widespread capacity deficits, with nearly all respondents reporting inadequate resources in digital forensics and electronic evidence handling issues exacerbated by limited training, equipment shortages, and the practical limitations of manual processes.

These gaps persist to date. Many jurisdictions, mainly in developing countries, continue to operate with this minimal forensic

infrastructure. Recent assessments, including INTERPOL surveys and UNODC regional reports, indicate that resource and training shortages remain acute: for instance, a 2024 INTERPOL survey in Africa found that 95% of participants reported inadequate training and resource constraints for cybercrime investigations. Even in well-resourced settings, agencies face significant backlogs in processing digital evidence, with median lab backlogs of three to four weeks for examinations driven by the sheer volume of data from devices like smartphones (now involved in approximately 97% of criminal cases). Furthermore, the increasing practice of cloud computing has complicated attribution and recovery of evidence, since the data location has become fluid and multi-jurisdictional, increasing legal barriers to access and preservation.

These systematically induced difficulties have been highlighted in many scholarly reports. Specifically speaking, disparities in national legal frameworks, i.e. data retention, essential requirements for chain of custody, privacy protections, authenticity, and cross-border access procedures hinder transnational digital evidence admissibility. Hence, Global Harmonisation is very important for evidence extraction. Without greater harmonisation, evidence gathered in one jurisdiction may face exclusion or significant challenges in another, undermining prosecutions. The borderless nature of cyberspace exacerbates these problems.

Investigations into cyber-attacks remain limited by territorial jurisdiction, conflicting sovereignty claims, slow mutual legal assistance mechanisms (MLATs) and political differences. Some of the existing relevant frameworks, such as the 2001 Budapest Convention on Cybercrime, ratified in 2004, provide some structure, yet persistent mismatches in procedural rules and admissibility standards limit their effectiveness. The absence of these cross-border protocols for the effective collection and validation of digital evidence creates enforcement gaps, where the volume of violations far exceeds the pace.

It is in this paper that we examine these legal challenges surrounding cross-border cybercrime investigations, with a focus mainly on how divergent national laws shape the collection, transfer and admissibility of digital evidence. By analysing these frictions,

technical deficits, conflicts in jurisdiction and attribution barriers due to evidentiary incompatibilities, we highlight how current systems fail to provide for the operational prosecution barriers in courts.

The study contributes to existing scholarship by synthesising institutional reports with recent legal and forensic literature (including analyses of cross-border cooperation mechanisms and digital forensics admissibility standards) to propose pathways toward greater harmonisation. It offers insights for policymakers for enhanced cooperation and cross-state as well as interstate regulations built upon the international frameworks.

Research Methodology

A qualitative doctrinal approach is adopted in this paper. In-depth analysis of legal frameworks, international and cross-national treaties, court cases, and policies governing cross-border cybercrime investigations has been carried out throughout this paper. A comparative analysis has also been used to examine how some countries regulate Mutual Legal Assistance (MLA), data access and admissibility of digital evidence in cross-national operations. The jurisdictions selected for this purpose are those with relatively mature legal systems in cybercrime matters, active participation in international collaborations and significant influence on global cyber policy. Key selection criteria include ratification of major cybercrime treaties, particularly the Council of Europe's Budapest Convention on Cybercrime, high prevalence of cybercrime incidents, and availability of substantial legal precedents and digital forensics infrastructure capable of providing a substantial evidence collection portal. Jurisdictions with minimal involvement in global initiatives, limited case law, or insufficient publicly available data on forensic capacities were excluded, as their inclusion would offer limited analytical value for this study's objectives. This paper bases its analysis on evidence-based findings that deepen understanding of the nuances involved in prosecuting cross-border cybercrimes and securing digital evidence collection.

Literature Review

Cloud computing, encryption, AI, and blockchain technologies are the modern complex challenges to forensic practices. The literature has evolved substantially. Early works were key foundational premises and remain highly relevant today.

One of the earliest comprehensive explorations of cybercrime investigation focused on integrating evidence while insisting that stringent collection and preservation protocols need to be followed (Shinder & Cross, 2008). Likewise, the best practices related to cybercrime and digital forensics investigations were also compiled, providing practical guidance to law enforcement. These foundational texts highlighted the importance of combining multiple evidence types to build coherent cases. This principle continues to apply in transnational contexts (Casino et al., 2022). Subsequent research sought to formalise these practices. Vlachopoulos et al. (2012) proposed a model linking digital and physical evidence procedures. Their objective was to simplify investigation procedures by taking into consideration the peculiarities of each evidence type (Vlachopoulos et al., 2012). Such models, however, exhibit limited applicability in modern distributed settings (Pichan et al., 2015). Evidence within cloud servers, encrypted networks, and decentralised systems is often fragmented and volatile (Ahmad, 2018). This makes traditional seizure methods practically inapplicable.

With the transition of cyber-activities to mobile and multimedia platforms, major gaps in current forensic capabilities were identified. Research has provided practical tutorials on multimedia evidence analysis (video, audio, and images), which is essential when dealing with incidents of misinformation, child exploitation, and deepfakes (Li & Ho, 2015). Nevertheless, rapid advances in adversarial Artificial Intelligence and deepfake creation require constant revision of forensic identification procedures. Similarly, the extraction of digital evidence in instant messaging apps was investigated, with relevance to cyberstalking, financial fraud, and terrorism cases (Ashawa & Ogwuche, 2017). This analysis is constrained by its limited coverage of ephemeral

messaging features in apps such as Telegram's secret chats and Signal's disappearing messages.

Carvalho et al. (2015) employed semantic technologies to improve banking fraud investigations by using automated data analysis (Carvalho et al., 2015). However, this solution does not suffice with regard to a critical problem, namely, AI explainability, which directly influences judicial acceptance of machine-generated evidence. Furthermore, K. et al. (2018) investigated deep learning applications in forensic analysis and developed an adversarial testing framework for AI-driven models. Despite being innovative, their results imply critical vulnerability to manipulation by malicious actors and to the reliability and legal status of AI-aided evidence. The recent comparative analysis indicates that to be used satisfactorily in court, AI-generated evidence should correspond to a high level of accuracy, reliability, and legality of its collection, as found in the UK Criminal Evidence Act or the UAE Electronic Transactions Law (Faqir, 2024).

Besides, blockchain technology has been suggested as a remedy to preserve the chain of custody in cross-border contexts. Lone and Mir (2019) presented a blockchain-based protocol to authenticate digital evidence documentation and chain-of-custody in cross-border prosecutions by tackling the challenge of authentication. This approach was extended by the suggestion of a blockchain-based forensic model using grey hash techniques to detect tampered images (Ali et al., 2022). Evidence authenticity is advanced in both contributions, yet the practical barriers have not been explored in depth. These barriers include implementation costs, scalability, and integration with existing legal systems.

Collectively, the literature reveals a consistent pattern. The rapid progress in digital forensics hasn't been matched by corresponding procedural reforms. What this means is that though the digital forensics technology has continued to advance, it is purely technological. This advancement has not been matched by the introduction of reliable and efficient frameworks. Such as techniques for evidence collection, preservation and analysis. States' national policies lag far behind. And even if it is quite satisfactory in some states, the execution is nowhere near the

practical domain. Thence, the evidence collected can be subject to tampering, substitution and contamination, which ultimately proves fatal to the results achieved. Policy hasn't been able to cope with such advancements. This incoherence causes a loss to the effectivity. While technology has improved detection and preservation capabilities, pragmatically, they frequently encounter obstacles related to admissibility, jurisdictional compatibility and international cooperation. These gaps underscore the need for legal coherence and effective policy that can accommodate evolving systems without compromising legal standards or due process.

Cross-Border Law Enforcement: Gathering of Stored Electronic Evidence

At the very outset, it is pertinent to ask whether a law enforcement agency has the authority to make territorial companies retrieve information located on international servers where such data provides evidence, though not substantive. The answer is that the traditional jurisdiction model, which grants states prosecutorial authority, is largely ineffective in cyberspace, where criminal activities traverse multiple national borders. The European Union recognised the importance of cloud computing in 2012, making policies and devising strategies to implement regulations and enforce them across sectors. Cloud computing is a paradigm for enabling access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand, according to the International Organisation for Standardisation. However, cross-border and multinational access remains a policy challenge.

A 2015 study by the Centre for European Policy Studies stated concerns regarding the EU rule of law and fundamental rights in the context of third-country law enforcement access to electronic data, particularly in EU-U.S. legal cooperation (Carrera et al., 2015). These issues were central to the 2018 case of Microsoft Corporation V. United States of America (the "Microsoft-Ireland" case), a landmark case regarding the extraterritorial reach for gathering stored data through international servers. The case had far-reaching impacts on the right to privacy and cloud computing regulations.

Internationally, it has been a state practice and standard to limit a state from exceeding a certain domain set. Article 32 of the 2001 Budapest Convention on Cybercrime allows the extraction or access to data where access has been publicly granted. The Convention's 2014 Guidance Notes clarify that service providers, as mere holders of data, cannot provide valid consent. They don't hold the authority to declare such access (Santos et al., 2021; Council of Europe, 2001). Consequently, Mutual Legal Assistance Treaties (MLATs) remain the primary framework for cross-border data requests. These treaties help provide a set of legal statements that a nation can work within the bounds of when dealing with data access between two distinct operating points (Efrat & Newman, 2017). But recognising its limitations, several states have pursued alternative agreements (De Busser, 2018).

The United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act in 2018, which enables direct data access agreements with foreign governments, streamlining access to data held by U.S.-based providers.

Meanwhile, the Council of Europe has been negotiating an additional protocol to the Budapest Convention (second additional protocol), the aim of which is to legislate such provisions that expand the horizon for direct access to subscriber data (Spiezia, 2022). The European Commission is also developing an intra-EU framework for data access (Silva & Duarte, 2025; Council of Europe, 2022). Within the European Union, the e-Evidence Package (Regulation (EU) 2023/1543 and Directive (EU) 2023/1544) establishes a harmonised intra-EU framework for European Production and Preservation Orders, allowing faster direct access to electronic evidence across Member States.

The Budapest Convention, while remaining the only effective and comprehensive international treaty which deals with cross-border electronic evidence collection, has a limited and constrained scope since it doesn't cover the sub-subjects. It allows unilateral access where the data is publicly available or with the consent of a lawful authority (Art.32, Budapest Convention, *202*0). Key cyber powers China, Russia and India have refused to ratify the convention, thus reducing its universal character and limiting its

enforceability (Amarachi F. Ndubuisi, 2023). Thence, the non-cooperative states, non-ratifying states, are not bound by its execution, and since the bigger and developing countries have more data access points, a lack of it can leave devastating impacts on the system. The system thus cannot compel such states. Since its adoption in 2001, a real change in global-level security threats has been seen with ransomware-as-a-service, dark web marketplaces, and cryptocurrency-based laundering schemes emerging as dominant cybercrime trends (Nshimiyimana, 2026). The Convention has not been updated to address these evolving threats, rendering some of its provisions obsolete. Meanwhile, cyberwarfare doctrines such as the Tallinn Manual remain focused on state-on-state conflict, neglecting the reality that most cyber threats originate from non-state actors, decentralised criminal networks, or rogue operations within state apparatuses. It is very difficult for such host states to identify such channels and to stop them, since they are part of a larger proxy scheme adopted by hostile states towards each other to hamper the channels.

The most complex segment of the cybercrime investigation process includes digital forensics. The scientific practice in electronic media regarding data preservation enables court evidence by performing acquisition and analysis of digital information (Pedapudi & Vadlamani, 2023). A traditional digital forensic investigation contains four sequential phases. These phases contain different work streams that occasionally share identical activities, although they represent distinct operational areas: *(1) Collection, (2) Examination, (3) Analysis, (4) Reporting* (NIST, 2006; Carrier, 2006).

Digital Evidence as a Means of Proof before the International Court of Justice

Evidence is such information which establishes or disproves alleged facts, whereas proof is a conclusive result which is derived from examining that evidence. Data stored in binary form, called digital evidence, has become increasingly important in courts (Joshi et al., 2025). This subsection focuses on the treatment of digital evidence before the International Court of Justice (ICJ), the principal judicial organ of the United Nations for resolving disputes

between states. Due to the ICJ's distinct procedural framework, these findings cannot compel states to adopt these procedures.

Digital evidence is inherently volatile and susceptible to tampering, manipulation, deletion, or unauthorised access (Prayudi & SN, 2015). Courts, therefore, impose strict safeguards, including chain-of-custody protocols, authentication requirements, and verification of integrity, to ensure reliability before admission (Ridder, 2009). Jurisdictions are different in their approaches. Their prioritisation is unique. Some prioritise authentication and hearsay exceptions, while others emphasise data integrity and privacy protections (Brantes Ferreira & Gromova, 2024).

Cross-border data-sharing regulations and privacy laws (e.g., GDPR in Europe) add further complexity. It is often a conflict between interstate disputes and the need for rapid cybercrime detection. The ICJ statute doesn't address digital evidence explicitly. There are no standard measures defined, such as lists for acceptable proof forms or uniform evaluation methods. Instead, the courts interpret it broadly, linking it with evidence and determining its admissibility and probative value (Roscini, 2016). This also slows down the process remarkably.

Limited Guidance in Recent Practices

Practice Direction IX *bis* accommodates digital documents readily available in the public domain, while Practice Direction IX *quarter* requires audiovisual or photographic material like the cause of creation, time, place of initiation, etc (Brantes Ferreira & Gromova, 2024). In practice, the ICJ has admitted open-source electronic materials (Brantes Ferreira & Gromova, 2024). This includes social media statements by officials of the state, as seen in cases such as *South Africa v. Israel*, *Gambia v. Myanmar*, and *Ukraine v. Russia*. However, the court, in carrying out its functions, counterchecks the authenticity of this evidence strictly and in strict compliance with the standardised rules set up in the legislation or MLATS of the states involved or any universal practices of a character where a legal vacuum or paucity exists (Brantes Ferreira & Gromova, 2024).

This flexibility offers advantages in adapting to the modern technological regime but creates uncertainty. The evidentiary rules must be clear. Without them, anyone can manipulate the system, tailor or produce them to cause great risk to the other party. Metadata manipulation is one such risk. Hence, judicial integrity requires looking into this matter indiscriminately and trying to balance this flexibility with robust safeguards. While the Court's interstate focus limits direct applicability to criminal cybercrime prosecutions, its discretionary model highlights the global absence of harmonised standards for digital evidence admissibility, an issue that directly affects cross-border cybercrime investigations.

Progress in Fostering International Cybercrime Cooperation: Formal and Informal Methods of Cooperation

MLATs and MLAAs can help to facilitate cooperation on cybercrime investigations and prosecutions by allowing for the collection and sharing of evidence across national borders (European Commission, 2019). The typical provisions of international agreements require member nations to gather requested documents and evidence, summon witnesses, and issue warrants according to pre-established procedures when foreign governments request assistance in criminal cases.

The Council of Europe's Convention on Cybercrime (Budapest Convention, 2001) remains the most comprehensive binding multilateral instrument. As of 2025, it has 81 parties. It standardises substantive offences (e.g., illegal access, data interference, computer-related fraud) and procedural powers while promoting international cooperation. A Second Additional Protocol on enhanced cooperation and disclosure of electronic evidence has seen slow ratification (Davies & Kennedy-Mayo, 2026). The newly adopted United Nations Convention against Cybercrime (2024), opened for signature in October 2025 in Hanoi, aims for a broader global reach and has already attracted around 76 signatories (UNODC, 2026). It seeks to strengthen electronic evidence sharing for serious crimes while co-existing with the Budapest framework, though concerns persist regarding potential impacts on human rights and surveillance powers (Tropina, 2024).

Informal mechanisms, such as Interpol's networks, Europol, the Five Eyes alliance, and the G8 24/7 network, complement formal treaties by enabling faster operational collaboration among trusted partners (Madnick et al., 2011).

Barriers to Cooperation

Although several bilateral and multilateral cooperation instruments have been developed, some issues remain that hinder cooperation and effectiveness:

Treaties Enforcement Mechanism Deficiencies

The Budapest Convention, in relation to other cybercrime treaties, fails to include any sort of enforcement procedures. These procedures will help in providing a standard that ratifying states must follow in addressing their deficiencies. The bigger problem is its outdated provisions, which enable governments to neglect their commitments and treaty obligations.

Similarly, there are other models that fail in the same domain, like Interpol's *Global Complex for Innovation (IGCI)* and *Mutual Legal Assistance Treaties (MLATs)*. It suffers from bureaucratic inefficiencies and limitations in its jurisdictions; its reliance on state-to-state diplomacy and protracted procedural formalities impedes real-time law enforcement responses, rendering them largely ineffective in addressing time-sensitive cyber threats (Sarkar & Shukla, 2026).

Misalignment between Cybercrime Governance Models

Other regional instruments and policy documents, particularly the *Shanghai Cooperation Organisation's 2009 Agreement on Cooperation in the Field of Ensuring International Information Security***,** which is not a binding treaty, embody different principles from the Budapest Convention regarding cybercrime and prioritise state control of information and communications technologies (ICTs) rather than emphasising enforcement cooperation, which results in fragmentation of global cybercrime governance procedures (Goldsmith, 2011). The lack of harmonisation of national laws with bilateral and multilateral

instruments on cybercrime and electronic evidence, or the complete lack of these laws to begin with, has proven to be a major impediment to progress on cooperation (Watney, 2012).

Limited Global Adherence to Binding Cybercrime Instruments

As of 2013, less than half of the countries around the globe have even signed or ratified a binding multilateral cybercrime instrument, which means they have no international obligation to align their national laws with these provisions, if they even have the national laws in place to begin with, and ensure they have the architecture in place to comply with cooperation requests (United Nations, 2013, p. 202). These states need to establish one-on-one treaties with each nation individually because they are not signatories to these instruments, thus requiring significant diplomatic resources and time. The evolving needs in cyber-related cases remain outside the scope of other multilateral and bilateral instruments in criminal matters, which some of these countries may have ratified (United Nations, 2000). This has been the case for countries in the *Gulf Cooperation Council (GCC)* that have acceded to the broader UN Convention against Transnational Organised Crime.

Geopolitical Disputes and the Challenge of Achieving Global Consensus

The Budapest Convention faces opposition from several different countries, especially Russia and China, because they want to create a fresh international cybercrime treaty, which could take multiple years of negotiation (Embassy of the Russian Federation, 2018). The achievement of a broad global consensus for a new agreement remains highly uncertain due to the differences in geopolitical interests.

Challenges Posed by Unilateral and Regional Regulatory Frameworks

Unilateral instruments such as the *Clarifying Lawful Overseas Use of Data (CLOUD) Act (2018),* empowering U.S. authorities to compel the disclosure of electronic data from foreign

entities, yet it provoked contentious debate over extraterritorial data sovereignty, particularly in light of stringent European data protection jurisprudence. Reference can also be made to the *EU e-Evidence Package (2021),* a novel regulatory framework that envisages the establishment of European Production and Preservation Orders to streamline evidence collection or to the *EU Investigation Order (EIO),* which was established to speed up investigative measures (Tosza, 2024). But then again, these co-operation protocols are highly dependent on judicial scrutiny of the competent authorities to lawfully retrieve information. There seems to be a fragmentation of global cybersecurity efforts, wherein nations impose unilateral data localisation requirements and privacy regulations that restrict cross-border collaboration and digital evidence-sharing (Hasan, 2024).

Legal and Procedural Obstacles to Mutual Legal Assistance and Extradition

Multiple issues are present in the execution phase of MLA and extradition procedures. Most countries face long and complex administrative responsibilities to establish MLA agreements, alongside no regulations for time constraints in agreement processing (De Busser, 2018). Due to the high-risk nature of electronic evidence alongside its potential alterations, deletion, or damage, the MLA request process demands swift actions from investigators who must maintain evidence sovereignty and acquire specialised abilities to collect, preserve and distribute this evidence for valid court presentation (Buono, 2019). Furthermore, extradition demands that crimes identified for extradition be dual criminal offences between the requesting and requested countries, which is not always the case at present.

State Sovereignty and Jurisdictional Conflicts

One of the most intractable dilemmas facing cybercrime jurisprudence is how to determine which legal authority should manage the case when digital offenders use distributed networks that surpass traditional territorial rules and operate across decentralised digital ecosystems (Kleijssen & Perri, 2017). Conventional doctrines fail to consider these extraterritorial dynamics of cyber offences (Kleijssen & Perri, 2017). This results

in a paradox where nations advocate for digital sovereignty, yet their infrastructure remains inherently dependent on transnational networks, creating a complex situation because their networks still depend on international digital connections despite their claims towards sovereignty (Hollis & Waxman, 2018). The inadequacies of self-reliance models, where states assume such responsibility for defending their cyber infrastructure, became evident during the WannaCry (2017) and NotPetya (2017) ransomware attacks, where widespread damage occurred despite the existence of national cybersecurity frameworks, details of which are mentioned in the famous Hollis & Waxman 2018 report.

Mutual Trust and the Enforcement Problem in Intelligence Cooperation

Even where intelligence is shared, there is then the "enforcement problem"; that is, how to enforce any agreement on intelligence sharing since breaches, either through intention or accidental circumstances, remain difficult to address. These challenges present two main points for analysis:

First, mutual trust is an essential element which finds its expression through agencies such as *the Five Eyes Network* and regional bodies like the *European Union* that use formal oversight systems ("Unpacking the principle of mutual trust: Five building blocks," 2020). The requirement to work with states holding strained relations in cyber investigations becomes easier through mutual interest-based cooperation.

Second, the process of information exchange becomes difficult in disruptive operations since the exchange terms are uncertain and anxiety about security risks can prevent agencies from reciprocating. For example, extradition may be refused on account of political offence exceptions or dual criminality requirements.

The level of flexibility in intelligence sharing may be more anarchic between close and trusted allies, yet it needs formal protocols to prevent intelligence leaks during low-trust situations. International criminal investigations take place through both unstructured relations and formal links between law enforcement agencies like *Interpol*, *Europol* (Fedorov et al., 2025), the *Five Eyes*

(Givens et al., 2018) and the *G8 24/7 Network groups* (Madnick et al., 2011). A great example would be the Australian data retention legislation under the Telecommunications Act of 1979, which grants the Australian Federal Police the power to authorise intelligence disclosure to foreign law enforcement agencies for uses that include criminal investigations, ICC prosecutions and war crime investigations. Although limited to authorisation, disclosure requirements must be determined by officers as both "appropriate" and "reasonably necessary" to meet the intended purpose (Telecommunications Act, 1979, §180A (3) -(4)).

In addition to this, the state-sponsored cyber operations, in matters of extrajudicial hacking, digital surveillance and data exfiltration, further intensify the moral dilemmas in an already corrupted module. These operations are primarily carried out by state agencies.

There are cases such as the Pegasus spyware revelations that bring up the perils of unregulated state surveillance in state operations (Antal, 2026). The need for balancing investigations is stressed, since these can lead to worldwide data breaches and violations of fundamental rights (Van Roomen & De Jonge, 2024). Fundamental rights breaches have been experienced a lot in these domains, which further leads to online harassment.

Role of the Budapest Convention and Illegal Digital Evidence Processes

As we highlighted at the very start of this paper, it is very important to look at the cybercrime issues in the context of transnational boundaries. We can find better outcomes and legislate better outcomes with this approach. Transnational analysis can raise complex questions. One of which we are going to discuss here is the admissibility of evidence obtained through unauthorised cross-border access. State sovereignty is an important concept. It relates to the right of the state to make decisions for itself, and no third party must infringe on this decision. These decisions can be made at the domestic and international levels. This right extends to the act of restricting a foreign party from accessing its data and using it for illegal matters, such as creating circumstances that can put the

state's sovereignty at risk. Proxy wars are included in this. Access to its data without consent is illegal, except for the data provided publicly.

Article 32 of the Budapest Convention permits access to this data or the data within lawful bounds and areas of consent provided by the states themselves in explicit terms, but its scope remains debated and is applied only among the states consented (Wessel & Nascimento Heim, 2023). This can complicate the system for its successful execution. Further, the Budapest Convention seeks to harmonise the offences relating to cyberspace into four distinct categories.

(1) Offences against confidentiality, integrity, and availability of computer systems and data;

(2) Computer-related offences (forgery and fraud);

(3) Content-related offences (e.g., child pornography, with a 2002 Protocol on racist/xenophobic material); and

(4) Offences related to copyright infringements, including aiding/abetting and corporate liability.

Critically, the convention has limitations. It doesn't fully resolve extraterritorial jurisdictional issues for which it was partly designed. The amendment processes are slow, risking obsolescence amid rapid technological change (e.g., cloud computing, encryption, blockchain, and AI-generated deep fakes). The practical impact is reduced due to these enforcement gaps. Geopolitical resistance adds further to the restrictions.

The emerging UN Convention against Cybercrime may complement or compete with this framework, but the effectiveness will depend on ratification rates, the quality of implementation and safeguards against abuse. Current advancements are therefore unreliable. Greater harmonisation is required; quick procedures and enhanced trust-building measures are very important to bridge these gaps.

In light of the problems discussed above, the following solutions are proposed.

Full ratification of the Budapest Convention and its Second Protocol

Europe's Budapest Convention is the only multilateral treaty which binds most states, if not all. Ratified and designed for 81 parties, most of which are connected in Europe and some big powers, in addition, such as the US, Japan, and Australia. Its full ratification will be the ideal step, but not possible for obvious reasons. Harmonising domestic cybercrime laws in accordance with it will make domestic investigations smoother and quicker.

Article 35 of the Budapest Convention states the requirement of a 24/7 network of points of contact. This enables real-time assistance in cases of emergencies. This fast network was very productive in cases such as the GozNym malware case and in many general cases of child pornography and bomb attack prevention (United States Department of Justice, 2019).

A shift from MLATs is required. It's a very slow process. Instead, the states must focus on direct requests for subscriber information and data traffic. The need for a legal framework in extension can make the system inefficient, on which the whole premise is built. Timeline improvement is very necessary in crimes of such nature.

In addition to this, there is a need for full ratification of the Second Additional Protocol, opened for signature in May 2022. Negotiations for the Second Protocol began in 2017 under the Cybercrime Convention Committee (T-CY). It was adopted by the Committee of Ministers on 17 November 2021 and opened for signature in Strasbourg on 12 May 2022 with 22 initial signatories. This convention is specifically designed to supplement the Budapest Convention. It addresses, though narrowly, enhanced cooperation and electronic data disclosures (Mishra, 2026). Quite fundamentally important is the need for cooperation when disclosing data, given the nature of the crime. 5 sections have been given in Chapter II. Section 2 deals with direct cooperation with

private entities. The section states that MLATs are used for data of low sensitivity on a large scale. Direct orders to service providers for access to data are a key introduction in this. Investigators thus no longer need to wait for rigorous legal frameworks to be provided before the execution of data access. Section 3 talks about enhanced cooperation between governments, and sections 4-5 about emergency and procedural enhancements.

It is a pragmatic framework, a sort of evolution of the Budapest Convention.

Recommendations

Enhancing Funding and Capacity

Donor governments and international organisations should substantially increase financial support for cybercrime capacity-building programs, aligning budgets with those allocated to counterterrorism. Programs must incorporate clear, measurable objectives, independent monitoring and evaluation frameworks, and explicit safeguards for human rights and civil liberties. Greater efforts are needed to collect and publicly disseminate reliable cybercrime statistics to inform policy and build political will.

Strengthening Public-Private Cooperation

Governments should actively engage the private sector, which possesses advanced technologies and firsthand experience as frequent victims of cybercrime, through structured partnerships. Discussions should focus on overcoming barriers to collaboration, building trust, incentivising information sharing, and addressing legal uncertainties that deter private entities from assisting law enforcement.

Promoting Legal Harmonisation and Procedural Standardisation

States should prioritise alignment of national laws on digital evidence admissibility, chain-of-custody requirements, data retention, and privacy protections. This shall strengthen the process and clearly mark the investigations from slowing down in the most

urgent of state investigations. Accelerated ratification and effective implementation of the Budapest Convention (currently with 81 parties) and the UN Convention against Cybercrime (opened for signature in 2025 with approximately 72–75 signatories) are critical. Complementary bilateral and regional agreements should reduce reliance on slow, bureaucratic mutual legal assistance processes.

Addressing Geopolitical and Sovereignty Challenges

International forums should facilitate dialogue to reconcile differing governance models for multiple projects diversified in nature (e.g., between Western emphasis on criminal justice cooperation and other states' focus on information sovereignty). The protocols for sharing must be reliable.

Investing in Training and Technological Integration

Sustained investment is required to train law enforcement, prosecutors, and judges in digital forensics. This should help fill the clear gap in efficient tool handling in matters of evidence collection and add to the professional sub-investigations that can add value to the state investigations. Private channels must be supported by the state, which in the long run would benefit itself.

Conclusion

The limits are then larger than the possibilities for cross-border investigations. As more and more data move to the cloud, law enforcement is hindered. The limits thus must be renegotiated on international forums, primarily focused on devising strategies for decreasing the timeline in criminal cyber cases. A lot of work is needed at a preliminary level to bring about such a change on a common level. As pernicious a system as this can be, key advancements have been proposed in certain aspects. Firstly, the need for expeditious cross-border access to data in the cloud era needs to be formally recognised at the international level. Secondly, the problems need to be conceptualised carefully and explicitly. Stakeholders should be aware of the effect of metaphors employed in debates, and care should be taken to use the most appropriate metaphors. Framing cyberspace as 'space' (a more abstract area) rather than as 'place' (a physical area) can make a difference in

terms of thinking about solutions, as does conceiving of cross-border searches as the sending and receiving of messages rather than as 'going to' a server. The fact that the location of data is hard to identify in cloud-computing contexts should be conceptualised as a loss of knowledge of location rather than a loss of location itself. And defining legal authority in terms of effective control rather than controlling territory within national boundaries may also help to understand jurisdiction in relation to 'space' instead of being uniquely connected to 'place'. Thirdly, both the community of cyber-investigation and the community of international law must become acquainted with the other community's language, concepts, and assumptions at a much deeper level than is currently the case.

Reference

Ali, M., Ismail, A., Elgohary, H., Darwish, S., & Mesbah, S. (2022). A procedure for tracing the chain of custody in digital image forensics: A paradigm based on grey hash and blockchain. Symmetry, 14(2), 344. https://doi.org/10.3390/sym14020334

Accenture/Ponemon Institute. (2019). The cost of cybercrime. Network Security, 2019(3), 4. https://doi.org/10.1016/S1353-4858(19)30032-7

Ahmad, M. B. (2018). Provocations open problems encountered by digital forensics, ensuing trends in the near future. International Journal of Trend in Scientific Research and Development, 2(5), 879–883. https://doi.org/10.31142/ijtsrd16955

Antal, H. S. (2026). Surveillance without borders: Pegasus, regulatory failure, and constitutional accountability in India and the Global South. https://doi.org/10.33774/coe-2026-vn095

Buonoawa, M., & Ogwuche, I. (2017). Forensic data extraction and analysis of left artefacts on emulated Android phones: A case study of instant messaging applications. Circulation in

Computer Science, 2(11), 8–16. https://doi.org/10.22632/ccs-2017-252-67

Brantes Ferreira, D., & Gromova, E. A. (2024). Digital evidence in disputes involving states. AJIL Unbound, 118, 51–56. https://doi.org/10.1017/aju.2024.4

Buono, L. (2018). The genesis of the European Union's new proposed legal instrument(s) on e-evidence. ERA Forum, 19(3), 307–312. https://doi.org/10.1007/s12027-018-0525-4

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SOK: Cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 8(1). https://doi.org/10.1093/cybsec/tyac014

Carvalho, R., Goldsmith, M., & Creese, S. (2015). Applying semantic technologies to fight online banking fraud. In 2015 European Intelligence and Security Informatics Conference (pp. 61–68). https://doi.org/10.1109/EISIC.2015.42

Council of Europe. (2001). Convention on cybercrime (ETS No. 185). https://rm.coe.int/1680081561

De Busser, E. (2018). The digital unfitness of mutual legal assistance. Security and Human Rights, 28(1–4), 161–179. https://doi.org/10.1163/18750230-02801008

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

Efrat, A., & Newman, A. L. (2017). Divulging data: Domestic determinants of international information sharing. The Review of International Organizations, 13(3), 395–419. https://doi.org/10.1007/s11558-017-9284-1

Faqir, R. S. (2024). The exclusionary rule of AI-enhanced digital evidence in the United States and UAE: A comparative analysis. Journal of Southwest Jiaotong University, 59(1). https://doi.org/10.35741/issn.0258-2724.59.1.7

Fedorov, V., Antoshyna, I., & Biriukov, R. (2025). Theoretical and legal foundations of law enforcement collaboration in combating economic crime in Europe. Baltic Journal of Economic Studies, 11(4). https://doi.org/10.30525/2256-0742/2025-11-4-177-185

Givens, A., Busch, N., & Bersin, A. (2018). Going global: The international dimensions of U.S. homeland security policy. Journal of Strategic Security, 11(3). https://doi.org/10.5038/1944-0472.11.3.1689

Goldsmith, J. (2011). Cybersecurity treaties: A skeptical view. Hoover Institution. https://www.hoover.org/research/cybersecurity-treaties-skeptical-view

Hasan, M. T. (2024). Cross-border cybercrimes and international law: Challenges in ensuring justice in a digitally connected world. IJRDO Journal of Law and Cyber Crime, 4(1), 1–7. https://www.ijrdo.org/index.php/lcc/article/view/6174

Hollis, D. B., & Waxman, M. C. (2018). Promoting international cybersecurity cooperation: Lessons from the Proliferation Security Initiative. Temple International & Comparative Law Journal, 32(2), 147–178. https://sites.temple.edu/ticlj/files/2020/02/32.2_Hollis_Article04-header-deleted.pdf

Joshi, N., Kumar, R., & Patel, P. (2025). The role of electronic evidence in the civil case evidence process. Rechtsnormen: Journal of Law, 3(1), 80–90. https://doi.org/10.70177/rjl.v3i1.2090

K., A., Grzonkowski, S., & Lekhac, N. A. (2018). Enabling trust in deep learning models: A digital forensics case study. In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE

International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (pp. 1250–1255). https://doi.org/10.1109/TRUSTCOM/BIGDATASE.2018.00172

Kleijssen, J., & Perri, P. (2017). Cybercrime, evidence and territoriality: Issues and options. Netherlands Yearbook of International Law, 147–173. https://doi.org/10.1007/978-94-6265-207-1_7

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44–55. https://doi.org/10.1016/j.diin.2019.01.002

Li, S., & Ho, A. T. (2015). Digital forensics laboratories in operation. In Handbook of digital forensics of multimedia data and devices (pp. 1–37). https://doi.org/10.1002/9781118705773.ch1

Madnick, S., Choucri, N., & Ferwerda, J. (2011). Institutional foundations for cyber security: Current responses and new challenges. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2338649

Mishra, N. (2026). The second additional protocol-2022: Relevance and significance in contemporary world. International Journal of Science and Research (IJSR). https://doi.org/10.21275/SR26209112254

National Institute of Standards and Technology. (2020). NIST cloud computing forensic science challenges (NISTIR 8006). https://doi.org/10.6028/NIST.IR.8006

Nshimiyimana, F. R. (2026). Adapting the Budapest Convention to address emerging cyber threats. Belügyi Szemle, 74(1), 183–204. https://doi.org/10.38146/bsz-ajia-ajia.2026.v74.i1.pp183-204

Ndubuisi, A. F. (2023). The impact of international cybersecurity treaties on domestic cybercrime control and national critical

infrastructure protection. World Journal of Advanced Research and Reviews, 20(3), 2285–2304. https://doi.org/10.30574/wjarr.2023.20.3.2549

Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation, 13, 38–57. https://doi.org/10.1016/j.diin.2015.03.002

Prayudi, Y., & SN, A. (2015). Digital chain of custody: State of the art. International Journal of Computer Applications, 114(5), 1–9. https://doi.org/10.5120/19971-1856

Pedapudi, S. M., & Vadlamani, N. (2023). Digital forensics approach for handling audio and video files. Measurement: Sensors, 29, 100860. https://doi.org/10.1016/j.measen.2023.100860

Roscini, M. (2016). Digital evidence as a means of proof before the International Court of Justice. Journal of Conflict and Security Law, 21(3), 541–554. https://doi.org/10.1093/jcsl/krw016

Ridder, C. K. (2009). Evidentiary implications of potential security weaknesses in forensic software. International Journal of Digital Crime and Forensics, 1(3). https://doi.org/10.4018/jdcf.2009070105

Santos, C., Nouwens, M., Toth, M., Bielova, N., & Roca, V. (2021). Consent management platforms under the GDPR: Processors and/or controller. In The principle of mutual trust in EU criminal law (pp. 47–69). Springer. https://doi.org/10.1007/978-3-030-76663-4_3

Sarkar, G., & Shukla, S. (2026). Policing transnational cybercrime: A critical assessment of the anticipated impact of the United Nations convention against cybercrime in India and worldwide. https://doi.org/10.2139/ssrn.5899223

Silva, T. C., & Duarte, E. P. (2025). E-evidence regulation 1544/2023 in the European Union: A paradigm shift from

judicial to "direct" cooperation. Observatório de la Economía Latinoamericana, 23(8), e10987. https://doi.org/10.55905/oelv23n8-038

Shinder, L., & Cross, M. (2008). Understanding cybercrime prevention. In Scene of the cybercrime (pp. 505–554). https://doi.org/10.1016/B978-1-59749-276-8.00012-1

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime. ERA Forum, 23(1), 101–108. https://doi.org/10.1007/s12027-022-00707-8

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

Trans-border access to stored computer data under article 32 of the Budapest Convention on cybercrime and extraterritorial powers. (2020). Eurojust & Council of Europe. https://www.eurojust.europa.eu/publication/trans-border-access-stored-computer-data-under-article-32-budapest-convention

United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

United Nations Office on Drugs and Crime. (2026). The United Nations convention against cybercrime: Status of adherence and signatories. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

Unpacking the principle of mutual trust: Five building blocks. (2020). In The principle of mutual trust in EU criminal law. https://doi.org/10.5040/9781509924578.ch-009

United States Department of Justice. (2019, May 16). GozNym cyber-criminal network operating out of Europe and

targeting American entities dismantled. U.S. Department of Justice Archives.

Van Roomen, T., & De Jonge, B. (2024). Balancing privacy and public interest in the fight against illicit financial flows: Lessons from a European case study. Journal of Economic Criminology, 5. https://doi.org/10.1016/j.jeconc.2024.100093

Vlachopoulos, K., Magkos, E., & Chrissikopoulos, V. (2012). A model for hybrid evidence investigation. International Journal of Digital Crime and Forensics, 4(4), 47–62. https://doi.org/10.4018/jdcf.2012100104

Wang, X. (2024). Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers? Leiden Journal of International Law, 38(2), 235–261. https://doi.org/10.1017/S0922156524000402

Watney, M. (2012). The way forward in addressing cybercrime regulation on a global level. Journal of Internet Technology and Secured Transactions, 1(3), 61–67. https://doi.org/10.20533/jitst.2046.3723.2012.0009

Wessel, R. A., & Nascimento Heim, T. (2023). The various dimensions of cyberthreats: (In)consistencies in the global regulation of cybersecurity. Anales de Derecho, 40. https://doi.org/10.6018/analesderecho.546921

Wiles, J., & Reyes, A. (2007). Digital forensics. In The best damn cybercrime and digital forensics book period (pp. 53–82). https://doi.org/10.1016/B978-1-59749-228-7.00002-3