https://doi.org/10.37420/j.mlr.2026.011

Procedural Interoperability for Cross-Border Electronic Evidence under the United Nations Convention against Cybercrime

Aisheng MA
School of International Law, China University of Political Science and Law, Beijing, China
Corresponding author, E-mail: 924008223@qq.com

Abstract
Cross-border electronic evidence is governed by an overlapping set of global, regional, bilateral and domestic mechanisms, each relying on different jurisdictional connections, institutional channels and safeguards. This article asks whether the United Nations Convention against Cybercrime can reduce that fragmentation by supplying a common procedural layer. Using doctrinal analysis and functional comparison, it develops a lifecycle model covering request formation, preservation and acquisition, sovereign and rights-based review, and post-transfer governance. The article argues that the Convention does not allocate exclusive jurisdiction over data and should not be evaluated as a substitute for the Budapest Convention system, the European Union e-evidence package or the United States CLOUD Act. Its more plausible contribution is to connect legally heterogeneous systems through central authorities, a 24/7 network, expedited preservation, expedited disclosure of routing-related traffic data and differentiated cooperation for stored, traffic and content data. That contribution remains partial because conflict-of-law review, provider-facing procedures, notification, evidentiary integrity, retention, onward transfer and remedies are left substantially to domestic implementation. The Convention can therefore operate as a minimum global interoperability framework only if States coordinate the complete lifecycle of evidence requests and clarify how its State-mediated procedures interact with more specialized provider-oriented regimes. The article closes with implementation priorities across the evidence lifecycle and applies them to China, where treaty-based cooperation would have to be reconciled with approval requirements for foreign governmental requests, cybersecurity regulation and personal-information protection.

Keywords
Cross-border electronic evidence; International cooperation; Jurisdictional conflict; Procedural interoperability; Service providers; United Nations Convention against Cybercrime

1 Introduction

Electronic evidence rarely corresponds to a single territorial connection. A criminal investigation may concern conduct initiated in one State, victims or suspects located in another, a service provider incorporated in a third, and data stored or replicated through infrastructure distributed across several jurisdictions. Each connection may support a legitimate investigative, regulatory or rights-protective interest. The difficulty is not an

absence of territorial connections, but their coexistence and the fact that their legal significance varies with the measure sought, the actor compelled and the interests affected. Territoriality remains relevant because States exercise coercive authority over persons, infrastructure and public functions within their territory. Storage location, however, may result from a provider's technical or commercial choices rather than any meaningful relationship with the offence or user. Daskal accordingly shows that data may be divided, replicated or relocated without the user's knowledge and that the place of storage can be an unstable proxy for regulatory authority [3].

A provider-control-based model responds to part of this problem by using the provider's possession, custody or control over data as the operational connecting factor. It does not eliminate overlapping jurisdiction. A multinational provider may be subject to legal authority in several States, and an order valid under the issuing law may conflict with disclosure restrictions, secrecy rules, privilege or data-protection requirements elsewhere. Other connections also remain relevant: the place of criminal conduct, the place of harmful effect, the nationality or residence of the suspect and victim, the provider's establishment and the market in which the service is offered. The resulting disputes are not adequately described as a binary choice between territoriality and extraterritoriality. They involve the coordination of several plausible jurisdictional claims and several institutions capable of asserting them [4-6].

Existing evidence-access mechanisms embody different solutions, and their temporal status matters for any comparison among them. Mutual legal assistance relies principally on cooperation between States and the use of the requested State's coercive powers. The United States Clarifying Lawful Overseas Use of Data Act, commonly known as the CLOUD Act, uses possession, custody or control as the operational connection for obligations imposed on covered providers, while supplementing that rule with a limited statutory comity mechanism and bilateral executive agreements [12, 19]. The European Union e-evidence package creates European Production and Preservation Orders addressed to designated establishments or legal representatives in another Member State, supported by notification, enforcement and fundamental-rights rules. Regulation (EU) 2023/1543 entered into force on 17 August 2023 but does not apply until 18 August 2026; it had therefore entered into force but had not yet become applicable by the factual cut-off date used in this article [10, 11, 24]. The Second Additional Protocol to the Budapest Convention combines expedited State-to-State cooperation with defined forms of direct cooperation involving providers and domain-name registration entities. As at 18 July 2026, four ratifications had been recorded, and the five-Party threshold in article 16(3) had not yet been met [9, 25, 26, 29]. These regimes differ not only in speed but also in who receives the demand, when another State participates, which authority reviews proportionality and how conflicts of law are managed.

The United Nations General Assembly adopted the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (the Convention) by consensus on 24 December 2024 through resolution 79/243. The Convention opened for signature in Hanoi on 25 and 26 October 2025 and remains open for signature at United Nations Headquarters until 31 December 2026. As at 18 July 2026, the United Nations Treaty Collection

recorded 79 signatories and three parties, namely Azerbaijan, Qatar and Viet Nam, with Canada the most recent signatory on 16 July 2026 and China among the States that signed in Hanoi on 25 October 2025. Article 65 requires forty instruments of ratification, acceptance, approval or accession and a further ninety days before entry into force [1, 2]. The Convention had therefore not entered into force by the factual cut-off date used throughout this article. The analysis concerns normative design and prospective implementation; subsequent ratifications, implementing legislation and practice fall outside its temporal scope.

Scholarship has mapped the declining sufficiency of storage location as an exclusive nexus, classified competing reforms and documented delay, legal heterogeneity and communication failures in cross-border investigations [3, 4, 7, 8]. It has also examined sovereignty, data protection and the institutional position of providers [5, 6, 15, 19]. The unresolved question is how the United Nations Convention fits within this field. This article answers through procedural interoperability: the capacity of legally distinct systems to connect at each stage of an evidence request without complete harmonization. It argues that the Convention supplies a minimum global layer rather than a complete evidence code. Sections 2-5 develop the framework, examine the Convention, compare specialized regimes and identify implementation priorities, including for China.

2 Jurisdictional Fragmentation and Procedural Interoperability

The Convention must be evaluated against a problem broader than the contrast between data location and provider control. Cross-border electronic evidence is governed by multiple jurisdictional connections and overlapping instruments, none of which supplies a universally preferred route. The difficulty is therefore not only concurrent jurisdiction, but the absence of shared procedures for formulating, reviewing, executing and supervising requests across legal systems. This section explains why single-nexus theories are insufficient and develops procedural interoperability as a lifecycle-based response that preserves legitimate differences in criminal procedure, sovereignty and rights protection.

2.1 Jurisdictional Fragmentation and the Electronic-Evidence Regime Complex

Cross-border data disputes are often organized around a contrast between location and provider control. The location-based model gives priority to the State in which data is stored, while the provider-control-based model uses an intermediary's possession, custody or control over data as the operational connection for compulsory production. Each captures a genuine legal interest, but neither supplies a general solution. Storage connects data to territorial regulation and may identify the State capable of carrying out a search or compelling a local custodian. Yet cloud architecture can replicate or allocate data for operational reasons unrelated to the investigation, and the user may have no knowledge of that allocation. In Microsoft Ireland, the Second Circuit held that the pre-CLOUD Act Stored Communications Act did not authorize enforcement of a warrant for email content stored in Dublin. After Congress enacted the CLOUD Act and the Government obtained a new warrant under the amended statute, the Supreme Court vacated the judgment and remanded with instructions to dismiss the case as moot [13, 14]. Provider control is more operational, but its apparent simplicity conceals difficult questions concerning corporate structure, encryption, contrac-

tual authority and technical capacity. It also privileges the State able to regulate a global intermediary and may expose that intermediary to inconsistent obligations. The proper issue is not which single connection should always prevail, but how the legal relevance of several connections should be translated into procedures of notice, review, execution and accommodation.

This problem requires a distinction between jurisdiction to prescribe and jurisdiction to enforce. A State may criminalize and adjudicate conduct linked to its territory, nationals or protected interests without acquiring an unrestricted right to perform investigative functions abroad. Conversely, a domestic order to a provider may affect foreign-stored data without foreign officers entering the storage State. The legality of such an order therefore depends on its addressee, required act, place of compliance, affected rights, competing regulatory interests and available conflict-management procedures. Woods and Ryngaert accordingly treat digital enforcement as the accommodation of overlapping sovereign authority rather than the search for a single territorial answer [5, 6].

The institutional environment is equally plural. Mutual legal assistance treaties, police networks, the Budapest system, the United Nations Convention, EU legislation, CLOUD Act agreements, domestic production powers and data-protection rules operate without a general hierarchy. Together they form an electronic-evidence regime complex: partially overlapping, non-hierarchical instruments governing the same issue area [18, 20]. Plurality can combine urgent preservation, deeper regional cooperation and a global baseline, but it also permits forum selection, duplicate demands and uneven safeguards. The objective is therefore to build interfaces through which distinct regimes can interact while subjecting their differences to legally structured review.

2.2 Procedural Interoperability: Lifecycle and Cross-Cutting Dimensions

In this article, procedural interoperability is developed as an analytical framework for evaluating cross-border electronic-evidence regimes. It denotes the capacity of legally distinct authorities to recognize, transmit, review, execute and supervise cross-border measures through sufficiently compatible procedures. Unlike harmonization or mutual recognition, it accepts continuing legal differences. It asks whether a request can be translated into another system, reviewed under that system's legality and rights standards, and governed after disclosure. Operational compatibility therefore requires identifiable institutions, shared legal categories, authenticated channels and procedures for disagreement.

The evidence lifecycle has three stages. Request formation identifies the issuing authority, legal basis, offence, relevant facts, account or person, data category, period, purpose and urgency. Preservation and acquisition address authentication, authorization, proportionality, confidentiality, feasibility, objections and conflicts with foreign law; preservation separates urgent protection against deletion from the more intrusive decision to disclose. Post-transfer governance covers purpose limitation, access, retention, deletion, onward transfer, security, evidentiary integrity, supervision and remedies. These stages are interdependent: vague requests impair review, accelerated acquisition may shift risk to later use, and lawful transfer does not ensure lawful retention or onward disclosure.

The lifecycle is the primary organizational axis; three cross-cutting dimensions evaluate each stage. Semantic interoperability concerns consistent understanding of data categories and procedural terms. Institutional interoperability concerns identification, authentication and allocation of responsibility among central authorities, contact points, courts and providers. Normative interoperability concerns the management of differences in proportionality, privilege, notification and data protection. A regime may perform well on one dimension and poorly on another: standardized forms can improve semantic clarity without resolving rights conflicts, while secure transmission cannot substitute for a procedure addressing foreign privilege claims.

Interoperability is a matter of degree and institutional distribution. States may cooperate effectively in preservation yet apply incompatible standards to content; providers may authenticate orders but lack standing to raise user privilege; and requested States may impose use limits without monitoring compliance. Evaluation should therefore consider legal certainty, efficiency, sovereign interests, affected persons, provider responsibility and review. Speed alone is insufficient, particularly where faster access shifts conflict-of-law judgment to private companies. Sections 3 and 4 accordingly organize analysis by lifecycle and apply the three dimensions as cross-cutting lenses.

3 The Convention as a Layered Cooperation Architecture

The Convention's cooperation chapter is best read as an evidence lifecycle. Articles 35 and 40 provide the legal and institutional basis; article 41 adds an urgent channel; articles 42 and 43 preserve evidence and identify transmission paths; articles 44-46 govern increasingly intrusive acquisition; and articles 5, 24, 36 and 40 constrain execution and subsequent use. Request contents and classifications test semantic interoperability; central authorities, the 24/7 network and execution channels test institutional interoperability; and sovereignty, safeguards, refusal, consultation and transfer rules test normative interoperability. Section 3.1 addresses formation, preservation and acquisition; Section 3.2 addresses review and post-transfer governance.

3.1 Request Formation, Preservation and Evidence Acquisition

Article 35 sets out the general basis on which States Parties are to cooperate in accordance with the Convention, other applicable international instruments and domestic law. Article 40(1) then requires them to afford one another “the widest measure of mutual legal assistance” in investigations, prosecutions and judicial proceedings relating to offences covered by the Convention. The scope also extends to the collection of electronic evidence for offences established under the Convention and for other serious crimes as defined by the treaty [1]. This relationship matters for interoperability. Specialized electronic-evidence measures do not float free from the general mutual-assistance framework. They are connected to rules on central authorities, request content, execution, confidentiality, refusal, consultation and subsequent use. At the same time, article 40 preserves existing treaties: where the States are already bound by a mutual legal assistance instrument, that instrument ordinarily governs unless they agree to apply the Convention’s procedures. Where no such treaty exists, article 40 supplies a default framework. The Convention thus fills gaps without claiming institutional exclusivity.

The request-formation interface is supported by designated central authorities. Each State must identify one or more authorities responsible for receiving requests and either executing them or transmitting them to competent domestic bodies. A request must identify the requesting authority, describe the investigation or proceeding and relevant facts, specify the assistance sought, provide available identifying information, state the applicable period and explain the purpose for which the evidence is requested. The requested State may seek additional information, and electronic transmission is permitted where authenticity and security can be ensured [1]. These requirements create a common minimum syntax, an important element of semantic interoperability, but they do not create a common form. States may differ in accepted languages, account identifiers, supporting documents, signature technologies and the level of detail required to establish necessity. The Convention therefore opens a channel while leaving much of its practical standardization to declarations, implementing legislation and operational guidance.

Article 41 supplements the central-authority route with a point of contact available twenty-four hours a day, seven days a week. The network may provide technical advice, assist in preservation and evidence collection, identify a provider's location, communicate legal information, locate suspects and supply electronic data to avert an emergency. Where the contact point is institutionally separate from the central authority, the State must ensure expedited coordination between them [1]. The network is the Convention's clearest mechanism of institutional interoperability: it can help determine which jurisdiction or provider is relevant, identify the appropriate legal procedure and prevent evidence from disappearing while formal documentation is prepared. It does not itself displace domestic authorization. A contact point can carry out coercive measures only to the extent allowed by national law and institutional competence. Effective interoperability therefore depends not only on naming a contact point but on staffing it with personnel able to understand technical identifiers, legal urgency and the relationship between provisional preservation and later disclosure.

Article 42 gives that relationship a structured form. A State may request expedited preservation of stored electronic data located in another State where it intends subsequently to seek access, seizure, securing or disclosure. The preservation request must identify the authority, offence, relevant facts, data, relationship between the data and offence, available information about the custodian or system, reasons for preservation and the intention to submit a later access request. Preservation is generally not conditioned on dual criminality, subject to a limited reservation connected to the expected later acquisition of data for offences outside those established by the Convention. Under article 42(8), preservation must remain in effect for at least sixty days so that the requesting State can submit the subsequent access request; if that request is received, the data must continue to be preserved pending a decision on it [1]. This separation of preservation from disclosure is one of the Convention's strongest design choices. It protects the evidentiary status quo without prejudging the legality of final access and permits different legal systems time to complete their own authorization procedures.

Article 43 addresses the possibility that preservation reveals a chain of providers across several States. Where the requested State discovers that a provider in another State participated in transmitting a communication, it must expeditiously disclose enough traffic data to identify that provider and the transmission

path. The disclosure is functionally limited: it is not a general transfer of traffic records but a routing device enabling the investigation to reach the next legally and technically relevant intermediary. Article 44 then permits a State Party to request another State Party to "search or similarly access," "seize or similarly secure," and disclose stored electronic data located within the requested State. The requested State responds under applicable international instruments, its domestic law and Chapter V, with expedited treatment where the data is especially vulnerable or the applicable framework so requires [1]. The coercive act remains controlled by the requested State. This protects domestic judicial authorization, privilege and constitutional limits, but it also means that similar requests may face different thresholds and timelines. The Convention achieves communicability, not equivalence.

The Convention's data definitions support this differentiated procedure but should not be treated as a formal hierarchy of sensitivity. Article 2 defines electronic data as the broader category and separately defines traffic data, content data and subscriber information [1]. The legal significance of a record depends on its function and context. An IP address used to identify an account may resemble subscriber information, while a time-stamped sequence of connections may reveal traffic patterns. Domestic implementation should therefore require the requesting authority to explain how it classified the data and why the requested procedure is appropriate. Misclassification can undermine semantic interoperability in two ways: the requested State may apply the wrong authorization standard, and the provider may produce either too much or too little information. A common vocabulary is valuable only when the factual fields sought are described with sufficient precision to support the legal category assigned to them.

Articles 45 and 46 become more deferential as the measure becomes more intrusive. Article 45 requires States to endeavour to assist in the real-time collection of traffic data associated with specified communications transmitted in their territory. Assistance is governed by domestic conditions, and States must endeavour to provide it at least where an equivalent measure would be permitted in a comparable domestic case. Article 46 requires States only to endeavour to assist with real-time collection or recording of content data to the extent permitted by applicable treaties and domestic law [1]. The text does not harmonize qualifying offences, authorization thresholds, minimization duties, duration limits or user-notification rules. This graduated structure demonstrates both the value and the boundary of the global layer. Preservation and routing disclosure can be standardized relatively strongly because they are provisional or narrowly functional. Content interception remains dependent on domestic constitutional and surveillance traditions. Chapter IV's domestic investigative powers ensure that national authorities possess relevant capabilities, but those powers do not substitute for the Chapter V procedures governing cross-border execution.

3.2 Sovereign Review, Human Rights and Post-Transfer Governance

Procedural compatibility cannot be assessed only by the speed at which data is obtained. A foreign request must remain subject to constraints that the requested legal order can recognize and apply. Article 5 requires States to perform Convention obligations consistently with sovereign equality, territorial integrity and non-intervention. It also provides that the Convention does not authorize one State to exercise in another State's territory jurisdiction or functions reserved to the latter's authorities. The provision does not establish a general rule that the storage State possesses exclusive authority over data, nor does it resolve every

dispute concerning a domestically served order with foreign effects. Its function within the interoperability framework is narrower and more important: it prevents procedural compatibility from becoming a licence for unilateral execution of another State's reserved enforcement functions. Sovereignty operates as a boundary condition, not as a refusal to cooperate.

Article 40 makes that boundary operational. The requested State normally executes assistance under its own law while following a procedure specified by the requesting State where possible and not contrary to domestic law. Assistance may be refused where the request fails to satisfy the Convention's requirements, threatens sovereignty, security, public order or other essential interests, asks for an act prohibited in a comparable domestic case, or conflicts with the requested State's mutual-assistance system. It may also be refused where substantial grounds indicate a discriminatory purpose or prejudicial effect. Reasons must be given, and consultation is required before refusal under article 40(21) or postponement under article 40(27) to determine whether assistance can be supplied subject to conditions [1]. Consultation is an underappreciated interoperability device. It permits narrowing, staged disclosure, timing conditions, confidentiality arrangements or restrictions on use instead of forcing a binary choice between full compliance and refusal. The Convention does not, however, provide a detailed conflicts-of-law test that weighs investigative necessity, privacy, privilege, provider burdens and foreign regulatory interests. Domestic law remains decisive.

Article 24 provides the principal procedural safeguard for investigative powers. It requires domestic conditions and safeguards protecting human rights and incorporating proportionality. Depending on the measure, they should include judicial or other independent review, an effective remedy, legally specified grounds and limitations on scope and duration; States must also consider the rights, responsibilities and legitimate interests of third parties [1]. Article 24(4) expressly extends those domestic conditions and safeguards to the use of Chapter IV powers and procedures when the requested State renders international cooperation. The Convention therefore directly links domestic procedural safeguards to the execution of Chapter V requests, although the substantive content and institutional form of those safeguards remain largely determined by domestic law. The flexibility of the provision enables States with different procedural traditions to participate, but the phrase "as appropriate" leaves substantial variation in prior authorization, standing, notification and remedy. The risk is not merely uneven abstract standards. Where several routes are available, the choice of route may determine whether an affected person receives judicial review or whether a provider can raise privilege and freedom-of-expression concerns. The Convention therefore creates a human-rights baseline without eliminating safeguard competition among overlapping regimes.

Post-transfer interoperability depends primarily on articles 36 and 40. Article 36 requires the transferring State to comply with domestic law and applicable international obligations, permits refusal where lawful transfer is impossible and allows conditions to be imposed to achieve compliance. The receiving State must provide effective and appropriate safeguards, and onward transfer to a third country or international organization requires notification to and authorization from the original transferring State [1]. Article 40 separately limits the use of information or evidence to the investigations or proceedings identified in the request unless the requested State consents. These rules preserve some control after disclosure, but they are not a complete evidence-lifecycle code. The Convention does not harmonize retention periods, deletion, access

logs, breach notification, data-subject information, chain-of-custody documentation or remedies in the receiving State. Nor does it provide a standing supervisory mechanism through which the transferring State can verify compliance with conditions. Across the three dimensions, the Convention supplies a workable semantic vocabulary and a basic institutional network, while normative compatibility remains more dependent on domestic law and inter-State consultation. Its architecture is consequently strongest at opening communication and preserving evidence, moderately developed at acquisition, and least complete after transfer. That pattern supports the characterization of the Convention as a minimum layer whose success depends on domestic and inter-institutional implementation.

4 The Convention within the Electronic-Evidence Regime Complex

The Convention will operate within an electronic-evidence regime complex that also includes the Second Additional Protocol, the EU e-evidence package, the CLOUD Act framework and existing mutual-assistance arrangements. These mechanisms pursue similar objectives but allocate authority differently among requesting and requested States, courts and providers. The comparison uses four variables: operational addressee, foreign-State role, jurisdictional connection and allocation of safeguards. Together they illuminate institutional, semantic and normative interoperability and clarify the Convention's distinctive role as connective infrastructure.

4.1 State-Mediated and Provider-Oriented Models Compared

The Convention’s institutional position becomes clearer when its procedures are compared by function rather than by instrument. The first variable is the operational addressee. Under the Convention, coercive access is principally mediated through the authorities of the requested State. As at 18 July 2026, the Second Additional Protocol had four ratifications and was not yet in force. It nevertheless adopts a mixed design. It provides direct requests to domain-name registration entities and direct cooperation with service providers for subscriber information, while also creating procedures through which one Party can ask another to give effect to orders for subscriber information and traffic data, obtain stored data in emergencies and conduct other enhanced cooperation [9, 25, 26, 29]. The EU package places the designated establishment or legal representative of a provider at the centre of production and preservation, although notification and enforcement authorities retain important roles for sensitive data and contested execution [10, 11]. The CLOUD Act begins with the provider subject to United States process and uses possession, custody or control as the connection, while executive agreements create reciprocal direct-access channels for qualifying foreign partners [12, 19, 27].

The second variable is the role of the foreign State. The United Nations Convention gives that State a central role because domestic authorities execute the coercive measure and apply domestic refusal and safeguard rules. This can increase legal legitimacy where a request touches local privileges, constitutional rights or essential interests, but it also preserves multiple institutional steps. The Second Additional Protocol varies the foreign-State role according to the data and procedure. Its direct subscriber-information mechanism reduces full central-authority involvement, while its order-giving and emergency provisions retain

structured participation by competent authorities. The EU system relies on mutual trust but does not remove the enforcing State entirely: notification is required for certain traffic and content orders unless the case has substantial and strong links to the issuing State, and enforcing authorities may raise specified grounds for refusal [10, 24]. CLOUD Act orders issued under ordinary United States law do not ordinarily require prior approval from the State most closely connected to the user or data. Foreign-State participation becomes stronger where an executive agreement or the statutory comity mechanism applies.

The third variable is the legal connection used to justify reaching the provider. The Convention ordinarily works through territorial execution by the requested State and does not itself create a universal provider-presence or control nexus. The Second Additional Protocol relies on treaty participation combined with defined service relationships and declarations. The EU Regulation applies to providers offering covered services in the Union and requires a designated establishment or legal representative, regardless of the location of the data. The CLOUD Act relies on possession, custody or control by a provider subject to relevant United States process. These choices allocate institutional leverage differently. A service-market connection can prevent providers from avoiding obligations by locating infrastructure elsewhere, but it expands the regulatory significance of offering services. Control can provide speed and technical clarity but may externalize conflict to States with stronger links to the person or activity. Requested-State execution provides a visible place for sovereign review but may be slower and dependent on capacity.

The fourth variable is the allocation of safeguards, which follow different institutional logics. The Convention protects rights through the requested State's domestic law, article 24's general conditions and safeguards, article 40's refusal and consultation provisions, and article 36's data-transfer rules. The Second Additional Protocol combines procedure-specific conditions with a detailed data-protection article and permits declarations or reservations in defined circumstances [9, 26]. The EU Regulation differentiates data categories, restricts who may issue or validate orders, requires necessity and proportionality and creates a notification mechanism for more sensitive traffic and content data [10, 24]. It also obliges the issuing authority to inform the person whose data were requested, subject to lawful delay, restriction or omission. The CLOUD Act executive-agreement framework imposes statutory criteria concerning rule of law, privacy and targeting, but the ordinary control-based disclosure obligation and the comity motion remain narrower than a comprehensive foreign-State review [12, 15, 19]. No model simply maximizes both speed and safeguards. Each places review, and with it conflict management and post-transfer protection, at a different institutional point.

Provider participation deserves separate emphasis because direct-access reforms redistribute public-law judgment. Providers understand account identifiers, data availability and feasibility, but are not designed to decide whether a prosecution is discriminatory, privilege applies or surveillance is proportionate under another State's law. The EU Regulation assigns issuing, notification and enforcement functions to public authorities and specifies provider objections; the Second Additional Protocol confines direct cooperation to defined categories; and CLOUD Act agreements depend on certification and targeting rules. These models improve access only where technical compliance is separated from legal adjudication. The United Nations Convention leaves that boundary largely to domestic law, making provider-facing implementation essential.

The regimes should not be arranged on a simple scale from obsolete mutual assistance to modern direct access. Provider-oriented measures may accelerate transmission but can require providers to assess authority, conflicting duties and user interests under pressure. State-mediated procedures preserve public responsibility and a forum for domestic rights, but depend on central-authority capacity and technical expertise. The comparative question is which interface bears the cost of legal diversity: the Convention retains much of it at requested-State execution, whereas EU and CLOUD Act models shift more toward issuing authorities and providers while adding different notification, enforcement or comity safeguards.

4.2 Comparative Synthesis and the Convention's Institutional Role

Table 1 summarizes the institutional allocation rather than ranking the regimes. The entries identify the principal route by which an authority reaches data; each instrument contains qualifications and may coexist with other legal channels.

Table 1 Comparison of Cross-Border Electronic-Evidence Regimes

Regime	Operational addressee	Core connection	Foreign-State role and safeguards	Structural trade-off
United Nations Convention	Requested-State authorities	Treaty cooperation and domestic execution	Central role; domestic review, refusal, consultation and transfer conditions	Broad global floor, but significant variation and multiple institutional stages
Budapest Second Protocol (four ratifications; not yet in force at cut-off)	Authorities, providers and registrars, depending on procedure	Treaty participation and defined service relationships	Varies by mechanism; procedure-specific conditions and data-protection framework	Greater procedural specificity, but narrower institutional reach
EU e-evidence package (applicable from 18 August 2026)	Designated establishment or legal representative	Offering covered services in the Union	Notification and enforcement safeguards within an integrated legal order	Faster direct orders depend on mutual trust and common EU rights standards
CLOUD Act framework	Provider subject to relevant legal process	Possession, custody or control	Limited statutory comity and executive agreements with qualifying partners	Speed and control-based reach, but the statutory comity mechanism is limited and conflicts may remain outside agreements

The comparison supports two conclusions. First, the Convention's principal advantage is breadth. It creates a common channel for States lacking EU integration, Budapest participation or a CLOUD Act agreement, and its central authorities, 24/7 network and preservation procedures lower the entry cost of cooperation. Breadth also constrains design: a global instrument cannot assume uniform judicial structures or mutual trust. It therefore defers important questions to domestic law, producing variation in authorization, response time, notification and remedies.

Secondly, the Convention should operate as connective infrastructure rather than the exclusive route to evidence. Article 40 preserves existing treaties but does not determine how authorities should choose

among a Convention request, Budapest procedure, EU order, CLOUD Act agreement or domestic provider-directed process. Specialized routes may bypass safeguards, while the most formal route may sacrifice urgency without adding protection. The Convention should guarantee a minimum capacity to communicate, preserve, review and condition transfer; specialized instruments may supply faster or more detailed procedures where their assumptions and safeguards are satisfied.

States should therefore treat route selection as a reviewable procedural decision. Where several instruments are available, an authority should record why it selected one, which safeguards apply and which foreign interests may be affected. This does not privilege the slowest route; it prevents selection from becoming an unreasoned means of avoiding notification, dual criminality or privilege protections. Reasons can remain in the case file for review by a court, central authority or supervisory body, reducing the risk that legal plurality becomes safeguard arbitrage.

The three dimensions clarify the Convention's contribution and limits. Semantically, it supplies common data categories and minimum request elements, but classification remains uneven. Institutionally, central authorities, the 24/7 network and requested-State execution create a broad channel, while specialized regimes give providers and issuing authorities larger roles. Normatively, the Convention preserves review, refusal, consultation and transfer conditions but leaves provider objections, notification, monitoring and many remedies to domestic law. Interoperability must therefore be built through domestic procedure, compatible forms, secure systems and coordination among overlapping regimes.

5 Implementation Priorities and the Chinese Context

Treaty adoption alone will not make evidence-access systems interoperable. General cooperation duties must be translated into procedures for route selection, request information, provider responsibilities, foreign-law conflicts and post-transfer use. Section 5.1 proposes an implementation design across the evidence lifecycle. Section 5.2 uses China as a concrete setting because its framework combines treaty-based criminal judicial assistance, centralised approval of foreign governmental requests and sector-specific data-governance obligations. It therefore tests whether the Convention's minimum procedural layer can interface with a system retaining substantial public-authority control over cross-border evidence transfers. The proposals are normative recommendations, not obligations already imposed in full by the Convention.

5.1 Designing an Interoperable Evidence Lifecycle

The Convention does not prescribe a mandatory order among cooperation mechanisms. This article proposes instead a route-selection principle grounded in necessity and proportionality. Where several lawful routes exist, authorities should assess whether preservation is sufficient to prevent loss, whether immediate acquisition is justified and whether the selected route creates greater interference or conflict than an effective alternative. The Convention's separation of preservation and access, and the EU's distinct Preservation and Production Orders, illustrate that urgency and disclosure need not be decided together [10]. The principle neither requires preservation in every case nor creates a treaty hierarchy; it requires reasons for the chosen route, data category and intrusion.

Standardized request information is the second priority. Beyond article 40's minimum elements, interoperable forms should identify the account or system, data category, period, factual connection, authorization, urgency, confidentiality, intended use, privilege issues and review contacts. Structured metadata can expose defects early. EU e-evidence certificates and the Second Additional Protocol show how standardized fields and authenticated transmission reduce ambiguity [9-11, 25]. Standardization must not replace individualized reasoning: a form stating that a request is necessary does not demonstrate necessity. Its purpose is to make the legal basis and limits visible to every institution involved.

Provider-facing procedures also require clarity. Providers should not adjudicate inter-State legal conflict, but must be able to authenticate demands, distinguish preservation from disclosure, identify competent authorities and raise manifest invalidity, technical impossibility, privilege or conflicting duties. Domestic law should establish secure channels, deadlines, public-authority escalation and retrospective review of emergencies; costs and delayed user notification should be transparent, authorized and reviewable. The Second Additional Protocol, EU Regulation and CLOUD Act agreements offer narrower allocation models [9-12, 25, 27]. Providers may identify problems and supply technical information, but public authorities must decide whether coercion and cross-border accommodation are justified.

Domestic law should also provide structured conflict review where requests may trigger foreign prohibitions. Relevant factors include offence seriousness and territorial connection, the affected person's location and nationality, provider establishment, data sensitivity, alternative treaty routes, the specificity of the foreign prohibition and possibilities for narrowing production. The aim is not automatic precedence for foreign law, but a reasoned public accommodation of competing interests. Article 40 consultation supplies a treaty basis, while CLOUD Act comity and the EU third-country conflict procedure offer more structured examples [10, 12, 15]. Providers should not bear the conflict alone.

Post-transfer governance is the final priority. States should supplement articles 36 and 40 with rules on purpose limitation, minimization, access, retention, deletion, onward transfer, security, breach notification, audit records, evidentiary integrity and remedies. Authorities should document how data was identified, preserved, transmitted and verified. Hash values, certifications and custody records support authenticity but cannot cure unlawful acquisition or function creep. Transfer conditions should enter the case file rather than remain in diplomatic correspondence, and independent supervision should examine both the original request and compliance with subsequent-use restrictions. Interoperability must govern the full evidence lifecycle, not merely delivery.

5.2 Implications for China

China signed the Convention on 25 October 2025 but had not deposited an instrument of ratification by the factual cut-off date [2]. Under article 67(15) of the Constitution and article 7 of the Law on the Procedure of the Conclusion of Treaties, treaties and important agreements specified by law are subject to a decision of ratification by the Standing Committee of the National People’s Congress [21, 22]. Future Chinese implementation would therefore require more than designation of contact points. It would require a coordinated assessment of criminal procedure, judicial assistance, data governance and the legal authority of providers to respond to foreign demands.

The rules most directly relevant to foreign governmental requests are article 4 of the Law on International Criminal Judicial Assistance, article 36 of the Data Security Law and article 41 of the Personal Information Protection Law. Article 4 of the 2018 Law requires international criminal judicial assistance to proceed on the basis of equality and reciprocity, prohibits assistance that would undermine China's sovereignty, security or public interests or violate the basic principles of Chinese law, and bars institutions, organizations and individuals in China from providing evidentiary materials or assistance covered by the Law to foreign authorities without the consent of the competent Chinese authorities [28]. The Law also establishes the liaison and competent-authority framework through which treaty-based requests are channelled. Under article 36 of the Data Security Law, requests by foreign judicial or law-enforcement authorities for data stored in China are handled by Chinese competent authorities in accordance with relevant laws, treaties or agreements concluded or acceded to by China, or reciprocity; domestic organizations and individuals may not provide such data directly without approval [16]. Article 41 of the Personal Information Protection Law establishes a parallel rule for personal information stored in China [17]. These provisions should be distinguished from general commercial data-export mechanisms. The current Cybersecurity Law, as amended on 28 October 2025 and effective from 1 January 2026, separately requires operators of critical information infrastructure to store in China personal information and important data collected and generated domestically and subjects necessary overseas provision to the applicable security-assessment regime; the relevant provision is now article 39, formerly article 37 [23]. A Convention request could supply a treaty basis for competent-authority cooperation, but it would not automatically displace approval, security, privilege or personal-information safeguards.

Implementation should designate a central authority and technically capable 24/7 contact point and define coordination with investigative, prosecutorial, judicial, cybersecurity and data-protection bodies. Procedures should distinguish preservation, subscriber information, traffic data, stored content and real-time interception, with progressively stronger authorization and review. Providers need a uniform protocol for authentication, preservation without disclosure, referral and legal holds, while outgoing requests should support foreign proportionality and privilege review. Transfer conditions should be integrated into case-management systems. Chinese criminal procedure should also address authenticity, translation, defence disclosure and evidence obtained under materially different procedures. Courts must be able to assess provenance, integrity and compliance with conditions imposed by the transferring State. This would support cooperation without treating unrestricted direct access or categorical data isolation as the default.

6 Conclusion

Cross-border electronic-evidence disputes cannot be resolved through a single connection based on storage, provider control, service offering, conduct or affected persons. The central question is procedural: whether a measure issued in one legal order can be understood, reviewed, executed and governed in another. Procedural interoperability evaluates that question across the evidence lifecycle rather than by speed alone.

The Convention creates a meaningful but incomplete global layer. Articles 35, 40 and 41 establish channels; articles 42 and 43 separate preservation and routing disclosure from acquisition; articles 44-46 govern stored, traffic and content data; and articles 5, 24, 36 and 40 preserve review and transfer conditions. It is strongest for limited provisional measures and weakest where intrusive surveillance or post-transfer governance depends on divergent domestic law. Its value lies in broad communicability, not replacement of the Budapest, EU or CLOUD Act systems.

Ratification alone will not produce interoperability. States must build compatible forms, secure channels, provider-facing procedures, conflict-management rules and effective post-transfer controls, while clarifying how specialized direct-access routes supplement State-mediated cooperation. Without those interfaces, the Convention may add another route without resolving the conflicts created by many routes.

References

[1] United Nations General Assembly. (2024). United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, G.A. Res. 79/243, U.N. Doc. A/RES/79/243 (24 December 2024).

[2] United Nations Treaty Collection. (2026). United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (Chapter XVIII.16): Status of Signatures and Parties, status as at 18 July 2026.

[3] Daskal, J. (2015). The Un-Territoriality of Data. Yale Law Journal, 125(2), pp. 326-398.

[4] Abraha, H.H. (2021). Law Enforcement Access to Electronic Evidence across Borders: Mapping Policy Approaches and Emerging Reform Initiatives. International Journal of Law and Information Technology, 29(2), pp. 118-153.

[5] Woods, A.K. (2018). Litigating Data Sovereignty. Yale Law Journal, 128(2), pp. 328-406.

[6] Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. German Law Journal, 24(3), pp. 537-550.

[7] James, J.I., & Gladyshev, P. (2016). A Survey of Mutual Legal Assistance Involving Digital Evidence. Digital Investigation, 18, pp. 23-32.

[8] Casino, F., Pina, C., Lopez-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-Border Criminal Investigations and Digital Evidence. Journal of Cybersecurity, 8(1), Article tyac014.

[9] Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. Council of Europe Treaty Series No. 224.

[10] European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings. Official Journal of the European Union, L 191, 118–180.

[11] European Parliament & Council of the European Union. (2023). Directive (EU) 2023/1544 of 12 July 2023 Laying Down Harmonised Rules on the Designation of Designated Establishments and the Appointment of Legal Representatives for the Purpose of Gathering Electronic Evidence in Criminal Proceedings. Official Journal of the European Union, L 191, 181–190.

[12] United States Congress. (2018). Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, 132 Stat. 1213 (codified in scattered sections of 18 U.S.C.).

[13] Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016).

[14] United States v. Microsoft Corp., 584 U.S. 236 (2018).

[15] Shurson, J. (2020). Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts between EU and US Law. International Journal of Law and Information Technology, 28(2), pp. 167-184.

[16] Standing Committee of the National People's Congress of the People's Republic of China. (2021). Data Security Law of the People's Republic of China, art. 36.

[17] Standing Committee of the National People's Congress of the People's Republic of China. (2021). Personal Information Protection Law of the People's Republic of China, art. 41.

[18] Raustiala, K., & Victor, D.G. (2004). The Regime Complex for Plant Genetic Resources. International Organization, 58(2), pp. 277-309.

[19] Abraha, H.H. (2020). Regulating Law Enforcement Access to Electronic Evidence across Borders: The United States Approach. Information & Communications Technology Law, 29(3), pp. 324-353.

[20] Alter, K.J., & Meunier, S. (2009). The Politics of International Regime Complexity. Perspectives on Politics, 7(1), pp. 13-24.

[21] National People's Congress of the People's Republic of China. (1982, as amended in 2018). Constitution of the People's Republic of China, art. 67(15).

[22] Standing Committee of the National People's Congress of the People's Republic of China. (1990). Law of the People's Republic of China on the Procedure of the Conclusion of Treaties, art. 7.

[23] Standing Committee of the National People's Congress of the People's Republic of China. (2016, amended 2025). Cybersecurity Law of the People's Republic of China, art. 39 (amendment adopted 28 October 2025; effective 1 January 2026).

[24] Shurson, J. (2025). The Balance of Efficiency and Fundamental Rights in the EU e-Evidence Regulation. New Journal of European Criminal Law, 16(3), pp. 278-299.

[25] Eurojust. (2022, updated 23 January 2024). Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence. European Union Agency for Criminal Justice Cooperation.

[26] Council of Europe. (2022). Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. CETS No. 224.

[27] United States Department of Justice. (2023). CLOUD Act Resources, updated 24 October 2023.

[28] Standing Committee of the National People's Congress of the People's Republic of China. (2018). Law of the People's Republic of China on International Criminal Judicial Assistance, art. 4.

[29] Council of Europe Treaty Office. (2026). Treaty 224: Chart of Signatures and Ratifications.