American Journal of Engineering Research (AJER) 2025
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-14, Issue-11, pp-48-54
www.ajer.org
Research Paper Open Access

# The Role of Conventions in Cybersecurity and Digital Evidence

Ashwathi. S
*LLM CYBER LAW & SECURITY*
*SRM INSTITUTE OF SCIENCE AND TECHNOLOGY*
*"SCHOOL OF LAW"*
*CHENNAI*

***ABSTRACT***
*The proliferation of digital technologies has redefined how crimes are committed, investigated, and adjudicated. Conventions formal, often international agreements and normative frameworks play a crucial role in shaping legal responses to cyber threats, harmonizing rules for cross-border cooperation, and setting standards for handling digital evidence[1]. This article examines the multifaceted role of conventions in cybersecurity and digital evidence: their functions (standard-setting, facilitation of cooperation, capacity building), the types of conventions that affect cyber law, how conventions intersect with domestic legal systems and investigative practice, their impact on digital evidence collection and admissibility, and the challenges and limitations they face. The paper concludes with practical recommendations for policymakers, practitioners, and researchers to strengthen the positive role of conventions while addressing their shortcomings. In an increasingly interconnected world, cyber threats no longer respect geographical boundaries, making international cooperation and harmonized legal frameworks indispensable. Conventions such as the Budapest Convention on Cybercrime (2001), the UN Convention against Transnational Organized Crime (2000), and various regional cyber protocols have emerged as essential tools in combating offenses that exploit digital networks[2]. These instruments not only define cybercrimes but also prescribe mechanisms for mutual legal assistance, expedited data preservation, and standardized digital forensics. For countries like India, though not a signatory to the Budapest Convention, many domestic provisions within the Information Technology Act, 2000[3], and the Indian Evidence Act, 1872, mirror its spirit by addressing offenses such as hacking, identity theft, and data breaches, while ensuring the authenticity and admissibility of electronic records through Sections 65A and 65B. The increasing reliance on digital evidence ranging from emails and call records to blockchain logs and social media data demands stringent safeguards to prevent manipulation or loss of integrity[4]. Therefore, conventions serve not only as legal frameworks but also as moral and procedural compasses guiding national systems toward transparency, accountability, and technological resilience in the pursuit of cyber justice.*

Date of Submission: 05-11-2025 Date of acceptance: 16-11-2025

## I. Introduction

Cybersecurity and digital evidence occupy an unusual legal and operational space: the subject matter is inherently technical, often borderless, fast-evolving, and deeply integrated into everyday life. National legal systems, however, remain territorially framed and characteristically slower to adapt. Conventions international agreements, model laws, and multi-stakeholder protocols serve as bridges between these realities by offering

[1] Miranda Bruce et al., Mapping the Global Geography of Cybercrime with the World Cybercrime Index, 19 (2024).
[2] KPMG, Cybercrime Survey Report, Insights and Perspectives, KPMG (Dec.14, 2017).
[3] Tanushree Basuroy, Cybercrime Cases Registered Under IT Act in India from 2012 to 2022, Statista (Dec.6, 2023).

[4]Binayak Dasgupta, Chinese hackers targeted 7 Indian power hubs, govt says ops failed, Hindustan Times.

shared legal vocabularies, procedural mechanisms for cooperation, and frameworks for evidence handling that transcend jurisdictions.

This article explores how conventions contribute to the prevention, investigation, and adjudication of cyber incidents and how they shape the lifecycle of digital evidence from collection to presentation in court. It also acknowledges the ways in which conventions fall short political resistance to harmonization, resource disparities, privacy and human-rights tensions, and technological change and proposes practical approaches to increase their effectiveness.

## II. What we mean by "conventions" in the cyber context

"Conventions" is used here as an umbrella term encompassing:

- Formal international treaties and conventions concluded between states;
- Regional conventions and agreements (e.g., regional protocols, mutual assistance frameworks);
- Model laws and instruments promulgated by international organizations (e.g., model laws, guidelines);
- Soft-law instruments, standards, and multi-stakeholder codes of conduct (industry standards, technical protocols, and best-practice guidance).

Conventions may be legally binding (treaties) or non-binding (declarations, model laws), but both categories influence domestic law and practice either through direct incorporation (treaties ratified into domestic law) or by normative and persuasive influence (model laws, standards adopted by regulators, or industry compliance).

## III. The need for conventions in cybersecurity and digital evidence

Several features of cyber incidents and digital evidence create a compelling case for conventions:

1. Transnationality of cyber operations: Data, infrastructure, and perpetrators frequently span multiple countries. Investigations often require access to servers, logs, and service providers located abroad[5].
2. Technical complexity and standardization: Digital evidence requires specialized handling, standardized forensic processes, and agreed formats to ensure integrity and admissibility across jurisdictions.
3. Divergent national laws: Substantial differences exist across countries in definitions of cyber offenses, procedural rules, privacy protections, and rules of evidence. Conventions promote harmonization or at least interoperability.
4. Speed and coordination demands: Cyber incidents can unfold quickly; timely cross-border cooperation enabled by pre-agreed frameworks can materially affect outcomes (for instance, stopping active intrusions or preserving volatile evidence).
5. Privacy, human rights, and rule of law concerns: Conventions provide space to balance investigative needs with rights protections by setting baselines and safeguards.

In short, conventions provide a predictable legal architecture upon which international cooperation and domestic capacity building can be constructed[6].

## IV. Types of conventions and normative instruments

Conventions impacting cybersecurity and digital evidence fall into several categories:

### 4.1 Formal international treaties

Treaties negotiated under the auspices of intergovernmental bodies set binding obligations for signatory states. These can cover criminalization of specific conduct, procedural cooperation, and standards for mutual legal assistance.

### 4.2 Regional agreements and protocols

Regions may adopt instruments tailored to local priorities and legal cultures these often complement or adapt global treaties to regional realities.

### 4.3 Model laws and guidelines

International organizations produce model laws (e.g., on electronic transactions, signatures) and procedural templates to aid harmonization and legislative reform. Model laws are persuasive rather than binding but frequently adopted into domestic codes.

---

[5]Finck, M., Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law? European Journal of Risk Regulation, (2018).

[6] De Hert, P., & Papakonstantinou, V., The GDPR and the Internet of Things: A Critical Analysis and Policy Recommendations. Computer Law & Security Review, 36, (2020).

4.4 Soft-law instruments and standards
Standards bodies (technical and industry consortia) publish technical specifications, accreditation criteria, and best practices for forensic processes. Although non-binding, industry adoption effectively makes these standards de facto rules for acceptable practice.

4.5 Multi-stakeholder and public-private initiatives
Conventions can take non-traditional forms cooperative frameworks involving states, industry, civil society and academia to address cyber resilience, information sharing, and incident response.

## V. Key substantive areas governed by conventions

Conventions touch on numerous substantive domains:
5.1 Criminalization and substantive offenses
Conventions often encourage or require states to criminalize specific harmful uses of ICTs unauthorized access, data interference, fraud, child exploitation, etc. thereby creating a common legal vocabulary.
5.2 Procedural cooperation and MLATs
Mechanisms for mutual legal assistance, expedited preservation requests, and cross-border evidence access are central. Some conventions facilitate direct cooperation with service providers, domain registrars, and hosting entities.

5.3 Data protection and privacy safeguards
Conventions may prescribe standards to ensure investigative powers do not unduly infringe privacy rights balancing law enforcement needs and civil liberties.
5.4 Technical standards and evidence preservation
Guidance on how to preserve volatile data (memory, live forensics), collect logs, and maintain chain-of-custody is often incorporated into conventions or their accompanying guidance.
5.5 Capacity building and mutual assistance
Conventions frequently include provisions for training, information exchange, and technical assistance to help less-resourced states implement obligations.

## VI. Conventions and cross-border cooperation: mechanisms and practice

One of the primary strengths of conventions is operationalizing cross-border cooperation. Mechanisms include:
6.1 Mutual Legal Assistance (MLA)
Treaties or conventions typically require parties to provide MLA for criminal investigations, including evidence gathering, witness statements, and executing search warrants abroad. In practice, MLA can be slow and formalistic; conventions often seek to streamline procedures and establish expedited channels for time-sensitive data preservation.
6.2 Direct cooperation with service providers
Some conventions or associated protocols encourage or permit direct law enforcement requests to service providers across borders (subject to safeguards), recognizing that MLATs may be too slow for live data.
6.3 Preservation and expedited disclosure
Recognizing data volatility, conventions often create tools for preservation orders that compel providers to retain data for a limited time while formal requests are processed.

6.4 Joint investigation teams and templated procedures
Conventions may enable joint investigation teams, common formats for requests, and model forms to reduce friction.
6.5 Regional cooperation networks and points of contact
Practical cooperation is often facilitated by national contact points or computer emergency response teams (CERTs) that exchange technical indicators and coordinate incident responses within agreed frameworks.
Together, these mechanisms aim to narrow the gap between the speed of cyber incidents and the slowness of legal process[7].

[7] United Nations Convention Against Transnational Organized Crime (UNTOC), 2000.

## VII. The role of conventions in the digital evidence lifecycle

Digital evidence passes through discrete stages identification, preservation, collection, analysis, and presentation. Conventions influence each stage[8]:

7.1 Identification

Conventions promote shared definitions and typologies of evidence (what constitutes computer data, logs, metadata), enabling investigators from different jurisdictions to recognize relevant material.

7.2 Preservation

Given the transient nature of many digital artifacts, conventions emphasize rapid preservation mechanisms. Preservation orders, notice-and-preserve frameworks, and retention obligations for service providers help prevent loss of evidence.

7.3 Collection

Conventions and accompanying technical guidelines provide protocols for lawful collection that maintain integrity. This includes standardized forensic imaging, hashing practices, and documentation standards that courts are more likely to accept.

7.4 Analysis

Conventions support capacity building for accredited forensic labs, shared toolsets, and cross-border validation of analytic methods. When multiple jurisdictions rely on similar standards, expert testimony and analytic outputs become more interoperable.

7.5 Chain of custody and documentation

To ensure admissibility, conventions promote strict chain-of-custody rules, audit trails, and metadata preservation. Agreed practices for documenting seizure, transfer, and analysis are crucial in adversarial proceedings.

7.6 Presentation and admissibility

Conventions inform judicial expectations regarding forensic evidence what analytical techniques are reliable, how to interpret logs, and how expert testimony should be framed thus shaping the courtroom lifecycle.

## VIII. Conventions' influence on admissibility and procedure in courts

While conventions are not courtroom procedures per se, they exert influence in several ways:

8.1 Standard-setting that judges rely on

When international instruments or widely-accepted standards (for example, forensic best practices) exist, judges often use them to assess whether evidence collection met acceptable procedures. This affords predictability and reduces disputes over methodology.

8.2 Recognition of foreign evidence and judicial cooperation

Conventions create conditions where courts trust and accept evidence collected abroad under agreed frameworks (e.g., through MLATs or expedited preservation procedures), which reduces hearsay and authentication challenges.

8.3 Balancing rights and investigative necessity

Conventions that embed privacy safeguards and proportionality principles can shape judicial balancing tests, affecting admissibility of evidence was gathered in a way that violated rights protected under the convention.

8.4 Expert accreditation and cross-border expert reliance

Conventions that encourage accreditation and certification of forensic practitioners help courts rely on foreign experts' reports and testimony.

In short, conventions help reduce procedural obstacles that might otherwise exclude or diminish the probative value of digital evidence.

## IX. Capacity building, harmonization and technical standards

Conventions often include provisions or accompanying programs for capacity building: training prosecutors, judges, and investigators; developing accredited labs; and funding technical infrastructure. This is especially important for countries with limited resources that otherwise cannot participate fully in cross-border investigations.

The harmonization of legal definitions and technical practices reduces "forum shopping" and evidentiary friction. Technical standards regarding forensic imaging, hashing algorithms, metadata formats, and evidence packaging are critical to interoperability. When conventions are paired with widely-accepted technical standards, the result is a practical bridge between legal requirements and operational reality.

[8] Convention on Cybercrime (Budapest Convention), ETS No. 185, Council of Europe, 23 November 2001.

## X. Strategic and normative effects: deterrence, legitimacy, and rule-making

Beyond technical and procedural impact, conventions have broader strategic effects:

10.1 Deterrence

By harmonizing criminalization and enabling coordinated enforcement, conventions increase the perceived risk for cross-border cybercriminals.

10.2 Legitimacy and normative anchoring

Conventions create normative baselines what counts as acceptable investigative conduct, what safeguards should exist and increase transparency and legitimacy in state action.

10.3 Rule-making in a fragmented space

In an environment with patchwork national laws and rapidly evolving technology, conventions act as centralized rule-making processes that can be more inclusive and deliberative than purely domestic lawmaking.

## XI. Challenges, limitations, and criticisms

While conventions are indispensable, they are not panaceas. Key limitations include:

11.1 Ratification and participation gaps

A treaty's effectiveness depends on broad adoption. When major states do not participate, the utility of a convention is limited. Partial participation creates uneven enforcement and legal vacuums.

11.2 Sovereignty, conflicting norms, and political resistance

States may resist harmonization on grounds of sovereignty or divergent policy priorities especially around surveillance, encryption, and data localization.

11.3 Speed of technological change

Conventions are often slow-moving; by the time they are negotiated and adopted, technology and threat landscapes may have evolved, creating relevance gaps.

11.4 Privacy and human-rights concerns

Some conventions, if drafted without strong safeguards, can be used to justify intrusive investigatory powers or undermine privacy protections. Ensuring human-rights compliance is a persistent tension.

11.5 Resource and capacity disparities

Low-income states may lack the resources to implement obligations, diminishing the practical reach of conventions and creating imbalanced enforcement.

11.6 Formalism and procedural delays

Even with conventions, formal procedures (MLATs, judicial cooperation) can be slow, undermining their utility for time-sensitive investigations.

11.7 Standards fragmentation and proprietary tools

The multiplicity of forensic tools, proprietary formats, and vendor-specific processes complicate the promise of interoperability standards are necessary but not always sufficient.

## XII. Emerging issues and future directions

Conventions must evolve to address modern challenges:

**12.1 Cloud computing and data localization**

Modern data architectures (cloud, edge computing) complicate notions of territoriality and data ownership. Conventions need mechanisms to handle data stored in distributed environments and to reconcile competing jurisdictional claims[9].

**12.2 End-to-end encryption and lawful access debates**

Encryption debates test the balance between privacy and lawful access. Conventions that attempt to mandate access mechanisms risk undermining security or rights; those that leave policy to states risk fragmentation.

**12.3 Artificial intelligence and evidence generated by algorithms**

AI-generated content, automated decision logs, and model interpretability introduce novel evidentiary challenges. Conventions must consider standards for provenance, explainability, and validation of AI-driven forensic outputs.

**12.4 Cyber operations and state responsibility**

As states adopt offensive cyber capabilities and as attribution becomes politically sensitive, conventions addressing state behavior, norms of responsible state conduct, and attribution procedures are increasingly important.

12.5 Private sector role and public–private partnership frameworks

Conventions should explicitly map the role of private actors cloud providers, platform companies, cybersecurity firms in incident response and evidence preservation.

[9] The CLOUD Act, 18 U.S.C. 2713 (2018).

## XIII. Recommendations

To strengthen the role of conventions in cybersecurity and digital evidence, policymakers and practitioners should consider the following practical steps:

13.1 Promote inclusive, rights-respecting drafting

Convene diverse stakeholders (states, civil society, industry, technical experts) early and ensure human-rights safeguards are embedded to increase legitimacy and uptake.

13.2 Build modular, adaptive instruments

Design conventions with modular clauses and sunset/review mechanisms so they can adapt to technological change without constant renegotiation.

13.3 Expand expedited preservation and direct-request mechanisms

Create standardized, time-limited preservation orders and clear pathways for lawful, auditable direct requests to service providers in emergency situations.

13.4 Strengthen capacity-building clauses with financing

Pair obligations with sustainable capacity-building mechanisms and financing to reduce implementation asymmetries between states.

13.5 Harmonize technical standards and certify forensic methods

Support interoperable, open technical standards for evidence collection, hashing, chain-of-custody documentation, and accreditation of forensic labs and practitioners.

13.6 Foster public–private incident response frameworks

Formalize channels and legal cover for information sharing, joint incident response, and cross-border cooperation with transparency and accountability safeguards.

13.7 Encourage regional "bridging" agreements

Where global consensus is elusive, regional agreements can act as bridges compatible templates that facilitate cooperation among clusters of states with similar legal systems.

13.8 Ensure judicial and prosecutorial training

Promote judicial exchanges, shared case-law repositories, and training on digital evidence standards to reduce admissibility disputes and build mutual trust.

13.9 Monitor and review for technological relevance

Establish regular, mandated reviews of conventions to assess relevance and propose updates in response to technological change.

## XIV. Indian Legal Context and the Influence of Conventions

While India is not a signatory to the Budapest Convention[10], the IT Act, 2000[11], and the Indian Evidence Act, 1872 (as amended by Section 65B)[12] reflect its principles. The Indian judiciary has actively engaged with issues surrounding digital evidence and cross-border investigations.

**Key Case Laws**:

1. State (NCT of Delhi) v. Navjot Sandhu (Parliament Attack Case, 2005)[13]
   - The Supreme Court accepted call records as electronic evidence but emphasized the importance of proper certification under Section 65B of the Indian Evidence Act.
   - This case laid the foundation for electronic evidence admissibility.
2. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473[14]
   - The Court clarified that electronic records are admissible only if accompanied by a Section 65B certificate, ensuring authenticity and chain of custody.
   - This judgment aligned Indian law closer to international best practices on digital evidence integrity.
3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)[15]
   - Reaffirmed the mandatory nature of Section 65B certification and explained procedures for admissibility of electronic evidence, particularly from digital devices.

[10] Convention on Cybercrime (Budapest Convention), ETS No. 185, Council of Europe, 23 November 2001.
[11] Information Technology Act, 2000
[12] Indian Evidence Act, 1872, SS. 65A and 65B.
[13] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[14] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[15] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

## XV. Conventions and Cross-Border Cooperation

Cyber investigations often require rapid sharing of evidence and technical data. Conventions facilitate this through:

- Mutual Legal Assistance Treaties (MLATs)
- 24/7 contact points for expedited preservation
- Standardized request formats

For instance, under the Budapest Convention, member states must ensure that their domestic law allows expedited preservation and disclosure of stored computer data.

**Case Reference:**

- Google Ireland Ltd. v. U.S. (2018)[16] The dispute over data stored overseas led to the U.S. CLOUD Act, illustrating the challenges conventions seek to overcome.

## XVI. Indian Framework

In India, the legal framework for cybersecurity and digital evidence draws heavily from international conventions like the **Budapest Convention on Cybercrime (2001)** and global model laws, though India is not a formal signatory. The **Information Technology Act, 2000 (IT Act)** forms the primary domestic legislation addressing cyber offenses and digital evidence. Under **Section 43**[17] and **Section 66**[18], the Act penalizes unauthorized access, hacking, data theft, and other forms of computer misuse. **Section 66C**[19] deals with identity theft and fraudulent use of digital signatures, while **Section 66D**[20] punishes cheating by impersonation through electronic means. Additionally, **Section 67**[21] criminalizes the publication or transmission of obscene material in electronic form, a provision often invoked in cyberstalking and online abuse cases. When it comes to evidence, **Section 65A**[22] **and Section 65B**[23] **of the Indian Evidence Act, 1872** are pivotal, as they specifically govern the admissibility of electronic records. Section 65B(4) mandates that any electronic record presented as evidence must be accompanied by a valid certificate ensuring authenticity and integrity. The judiciary has repeatedly emphasized this requirement, as seen in **Anvar P.V. v. P.K. Basheer (2014)**, where the Supreme Court held that electronic evidence without the Section 65B certificate is inadmissible. This was reaffirmed in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)**[24], where the Court clarified that secondary electronic evidence such as CDs, emails, or CCTV footage must comply with Section 65B to be considered valid. Moreover, **Section 79A**[25] **of the IT Act** empowers the Central Government to appoint **digital evidence examiners** to authenticate and analyze electronic evidence, ensuring conformity with forensic standards. The **Code of Criminal Procedure (CrPC), 1973**, particularly **Section 91**[26], allows investigating agencies to summon digital records, while **Section 165**[27] provides powers for lawful search and seizure, which extend to electronic devices. These domestic provisions collectively align with international standards under conventions like the Budapest Convention, ensuring that digital investigations meet global evidentiary norms. The Indian legal system, therefore, integrates international best practices while safeguarding procedural fairness and data integrity. Judicial interpretation continues to strengthen the reliability of digital evidence, creating a robust balance between technological advancement, individual rights, and effective law enforcement.

## XVII. Conclusion

Conventions whether formal treaties, model laws, or soft-law instruments are central to building a predictable, interoperable framework for cybersecurity and digital evidence. They enable cross-border cooperation, harmonize definitions and procedures, and provide operational guidance that can improve evidentiary quality and judicial outcomes. At the same time, conventions face serious limitations: uneven participation, political resistance, resource gaps, and the relentless pace of technological change.

---

[16] Google Ireland Ltd. v. United States, 138 S. Ct. 1186 (2018).
[17] Information Technology Act, 2000, SS. 43.
[18] Information Technology Act, 2000, SS, 66.
[19] Information Technology Act, 2000, SS. 66C.
[20] Information Technology Act, 2000, SS, 66D.
[21] Information Technology Act, 2000, SS. 67.
[22] Indian Evidence Act, 1872, SS. 65A.
[23] Indian Evidence Act, 1872, SS. 65B.
[24] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[25] Information Technology (Amendment) Act, 2008, SS. 79A.
[26] Code of Criminal Procedure, 1973, SS. 91.
[27] Code of Criminal Procedure, 1973, SS. 165.

The path forward requires instruments that are flexible, rights-respecting, and accompanied by concrete capacity-building and technical standardization. Enhanced public–private cooperation, investment in forensic capacity, and more adaptive normative mechanisms will be essential to ensure that conventions remain effective tools for justice and security in an increasingly digital world.