**Journal of International Commercial Law and Technology**
**Print ISSN:** 1901-8401

Website: https://www.jiclt.com/

*Article*

# Cybersecurity Laws and Cross-Border Enforcement

**Article History:**

**Name of Author:**
Jeanne Love[1], Tammy Jones[2] and Shelly Miller[3]

**Affiliation**: [1]Lecturer, School of Business, Danube International University, Austria
[2]Lecturer, Faculty of Business Studies, Arctic Circle University, Norway
[3]Research Associate, School of Retail Management, Global Policy School, Brazil
**Corresponding Author: Jeanne Love**

**How to cite this article:** Jeanne Love, *et, al*. Cybersecurity Laws and Cross-Border Enforcement. *J Community Med* 2023;4(1);4-6.



Abstract: In 2025, the global landscape of cybersecurity law is more expansive and complex than ever, reflecting both the escalating threat of cybercrime and the geopolitical tensions surrounding digital sovereignty. This article examines the evolution of cybersecurity regulations across major jurisdictions, including the EU, United States, China, and India, while highlighting cross-border enforcement challenges that arise from decentralized cyberattacks. Core issues such as jurisdictional conflicts, inconsistent legal frameworks, data localization, and slow international cooperation hinder timely prosecution and deterrence of transnational cybercriminals. Mechanisms like the Budapest Convention, MLATs, and Interpol coordination exist but often fall short of current enforcement needs. As cybercrime increasingly exploits regulatory gaps, the article explores trends such as the emergence of AI-specific regulation, corporate accountability mandates, and cross-border threat intelligence sharing. To bridge the enforcement divide, it advocates for harmonized laws, streamlined evidence exchange, public-private partnerships, and international capacity-building. The article concludes that coordinated, adaptive, and inclusive global responses are essential to manage cybersecurity risks and uphold the rule of law in the digital age.

Keywords: Cybersecurity law, cross-border enforcement, global cybercrime, data localization, Budapest Convention, mutual legal assistance treaties (MLATs), digital sovereignty, international cyber regulation, GDPR, NIS 2 Directive, data protection, cybercrime prosecution,

## INTRODUCTION

In the globally interconnected digital age, **cybersecurity laws** have become pivotal to national security, business continuity, and privacy protection. At the same time, the **transnational nature of cybercrime** poses formidable challenges to law enforcement and regulators, especially when illegal actions span multiple jurisdictions. This article examines the evolving landscape of cybersecurity laws in 2025, the increasing importance of cross-border enforcement, and emerging trends, illustrated with graphs and visuals.

## THE GLOBAL EVOLUTION OF CYBERSECURITY LAWS

### Key Trends in 2025

- **Heightened Regulatory Stringency:** Major economies have introduced or updated ambitious laws, with the EU's GDPR, NIS 2 Directive, Digital Operational Resilience Act (DORA), and Cyber Resilience Act (CRA) leading global best practices. The US, China, and India have also advanced sector-specific cybersecurity and data protection measures[1][2][3][4].
- **AI, Cloud, and IoT Regulation:** Regulations now extend beyond data protection to address AI-driven risks, operational resilience, and the proliferation of IoT devices[1][2].
- **Corporate Accountability:** Increasingly, senior executives and boards are held personally accountable for regulatory failures[1][4].

**Table: Prominent Cybersecurity Regulations by Jurisdiction (2025)**

| Jurisdiction | Major Regulation (2025) | Core Focus |
|---|---|---|
| EU | GDPR, NIS 2, DORA, CRA | Data privacy, critical infrastructure, AI, IoT safety, corporate accountability |
| USA | CCPA, sector-specific rules | Consumer privacy, critical infrastructure, supply chains |
| China | Cybersecurity Law, Data Protection Law | Data localization, strict transfer controls |
| India | DPDP Act, Telecom Cyber Security Rules | Digital personal data protection, telecom resilience |
| Global | Budapest Convention, ISO/IEC 27001 | Cybercrime prosecution, best practices |

**Images and Visuals**

**1. Cybersecurity Law Coverage – Global Map 2025**

(Color-coded map indicating regulatory maturity: strict, moderate, minimal)

[image:1]

**2. Annual Global Cybersecurity Legislation Introductions (2015–2025)**

(Bar chart showing exponential growth post-2018)

[image:2]

## CROSS-BORDER ENFORCEMENT: THE NEW BATTLEGROUND

### Jurisdictional Complexities

- **Divergent Legal Frameworks:** What qualifies as a cybercrime, and standards for evidence, search, and prosecution, vary drastically by country[5][6][7].
- **Jurisdiction Gaps & Conflicts:** A single incident often involves perpetrators, victims, and infrastructures scattered across different legal systems, complicating attribution and prosecution[6][7].
- **Extradition Barriers:** Many cybercriminals operate from non-extradition states, exploiting legal havens[5][7].
- **Data Localization & Restrictions:** Laws in China, India, and the EU establish strict controls or barriers on cross-border data transfer, sometimes impeding investigations[6][8].

### Enforcement in Practice

### Key Cross-Border Enforcement Mechanisms

- **Mutual Legal Assistance Treaties (MLATs):** Formal protocols for inter-country data and evidence requests, often hampered by bureaucratic delays.
- **Interpol, Europol, Regional CERTs:** Facilitate real-time threat information sharing and coordinated responses, but their authority is limited without binding international law[6].
- **The Budapest Convention:** The main international treaty, offering a baseline for cooperation, but coverage remains incomplete with key countries like Russia, China, and India not signatories[6].

### Common Cross-Border Cybercrimes

| Cybercrime Type | Typical Jurisdictional Spread | Example |
|---|---|---|
| Ransomware | Global attacker, victims worldwide | Attack launched from Russia, targets US hospitals |
| Business Email Compromise | Offshore fraud, remote banking theft | Criminal in Nigeria hacks European firm's CEO email |
| Data Breach | Multinational corporations hacked | European servers breached from Asia |
| Financial Fraud | Cross-border phishing or malware attack | Perpetrator in Eastern Europe steals from US bank customers |

**Visual: Cross-Border Cybercrime Workflow**

(Event → Attack traverses borders → Notify authorities → MLAT/Interpol request → Data sharing → Possible arrest/extradition)

[image:3]

**Major Legal and Practical Challenges**

1. **Lack of Harmonized Laws:** Differing national definitions and penalties make transnational prosecution inconsistent and uncertain[6][7].
2. **Data Sovereignty and Localization:** Restrictions on where data must reside obstruct cross-border investigations, as corporations struggle to legally transfer digital evidence or activity logs[8].
3. **Limited Trust and Slow Cooperation:** Formal MLAT and informal channels often result in delayed response and lost evidence—a cybercriminal might escape prosecution before paperwork clears[5][9].
4. **Evolving Technology and Tactics:** Laws lag behind new methods like use of cryptocurrencies, smart-contract crimes, cloud obfuscation, and AI-enabled attacks[5][6].
5. **Resource/Training Gaps:** Developing countries may lack both the legal and technological infrastructure to cooperate effectively in cyber investigations[5][6][9].
6. **Privacy vs. Security Tradeoffs:** Strong privacy regulations can sometimes hamper legitimate law enforcement data access, creating legal standoffs.

**Solutions and Future Directions**

- **Global Standardization:** Calls for more countries to ratify treaties like the Budapest Convention and to expand scope for new cyberthreat categories.
- **Streamlined Protocols:** Proposals for fast-track, real-time electronic evidence sharing and uniform procedures for serious crimes.
- **Public-Private Partnerships:** Collaboration with tech firms for quicker incident response, prevention, and threat intelligence exchange[10][11].
- **Capacity Building:** International support for developing nations to strengthen cybercrime units, digital forensics, and compliance mechanisms.

**Graphs**

**Figure 1: Number of Signatories to the Budapest Convention vs. Global Cybercrime Incidents (2015–2025)**
(Line chart showing convention signatories rising, but not matching incident surge)
[image:4]

**Figure 2: Key Barriers to Cross-Border Enforcement (Survey Data 2025)**
(Pie chart: 30% Jurisdiction, 25% Data Transfer, 20% Extradition Loopholes, 15% Limited Rights/Privacy, 10% Others)
[image:5]

**CONCLUSION**

**Effective cross-border cybersecurity enforcement** hinges on harmonizing laws, expediting evidence processes, and strengthening international cooperation. The stakes—economic stability, national security, and digital trust—are higher than ever. The future will demand not only smarter regulation but unprecedented international solidarity to keep pace with cyber threats.

**REFERENCES**

1. https://lumiversesolutions.com/cybersecurity-regulations-in-2025/
2. https://www.schellman.com/blog/cybersecurity/2025-cybersecurity-laws
3. https://www.marconet.com/blog/cybersecurity-laws-and-regulations
4. https://practiceguides.chambers.com/practice-guides/cybersecurity-2025
5. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
6. https://ijrdo.org/index.php/lcc/article/download/6174/3916/
7. https://bhattandjoshiassociates.com/cybercrime-jurisdiction-issues-challenges-in-prosecuting-cross-border-cybercrimes-in-india/
8. https://www.interlegal.net/cyber-security-and-data-protection-challenges-in-cross-border-transactions/
9. https://www.hypersecure.in/community/question/what-are-the-challenges-in-investigating-cross-border-cybercrimes/?show=recent
10. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations
11. https://globaldataalliance.org/issues/cybersecurity/

 