Page 279 - 287

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Borders without Boundaries: Cybercrime as a Transnational Threat in the Digital Age

OJASWI VINDHYACHALAM*

ABSTRACT

The rapid digitalization of global communication and governance has simultaneously enabled unprecedented technological growth and facilitated the expansion of cybercrime as a transnational threat. Cybercriminal activity now operates beyond traditional territorial boundaries, exploiting anonymity, encrypted networks and decentralized financial systems to challenge existing legal frameworks and investigative capacities. Despite early international efforts such as the Budapest Convention, inconsistencies in national cyber laws and asymmetries in enforcement capabilities continue to create safe havens for cyber offenders. The escalating scale of cyberattacks, from ransomware operations such as LockBit and global crackdowns such as Operation Endgame to sophisticated state-linked intrusions such as the SolarWinds breach, demonstrates the borderless nature of modern cyber threats. Developing digital economies, including India, face compounded vulnerabilities, as illustrated by large-scale frauds, digital arrest scams and cross-border laundering networks. These incidents reveal persistent gaps in jurisdictional clarity, mutual legal assistance, real-time data access and digital evidence management. This paper argues that addressing cybercrime as a transnational phenomenon requires harmonized legal standards, faster cross-border cooperation mechanisms and strengthened institutional capacities, particularly in the Global South. It examines global case studies, India's emerging cybercrime landscape and the challenges posed by data sovereignty and technological complexity. The study concludes that combating cybercrime demands a collective international response grounded in legal convergence, operational collaboration and trust-based global governance frameworks. Without such coordinated efforts, cybercriminal innovation will continue to outpace regulatory progress, undermining national security, economic stability and public trust in the digital ecosystem.

Keywords: *cybercrime, transnational crime, Budapest Convention, jurisdiction, mutual legal assistance, data sovereignty, international cooperation*

I. INTRODUCTION

The digital revolution has reshaped the global landscape of communication, commerce and governance. Yet the same interconnectedness that enables innovation and technological

* Author is a Student at National Forensic Sciences University, Bhubaneswar, Odisha, India.

 [ISSN 2581-5369]

development has also facilitated the globalization of crime. Cybercrime, once considered a niche threat confined to the realm of hackers and computer experts, has evolved into one of the most pressing transnational security concerns of our time, one against which no country is immune and no individual beyond reach. The anonymity, speed and borderless nature of the internet have empowered individuals and organized groups to operate across jurisdictions, challenging traditional legal frameworks and enforcement mechanisms.

The Budapest Convention on Cybercrime (2001) was the first major international attempt to address this borderless challenge by harmonizing national laws and improving international cooperation.[1] However, even two decades after its adoption, the global legal landscape remains fragmented. Cybercrime is growing at roughly 15% each year, making it one of the fastest-growing forms of transnational crime.[2] It is estimated that by the end of 2025 the global cost of cybercrime will reach USD 10.5 trillion, up from USD 3 trillion in 2015.[3] As digital dependency deepens, the magnitude of transnational cyber threats, from ransomware to state-sponsored espionage, has multiplied, creating a critical gap between technological capability and legal enforcement.

II. Cybercrime as a transnational phenomenon

In its most generic form, cybercrime is any criminal activity that involves a computer, a networked device or a network.[4] Such crimes typically involve multiple layers of anonymity, the use of encryption and decentralized financial tools such as cryptocurrencies, making attribution and prosecution exceedingly difficult.[5]

The defining feature of cybercrime is its ability to transcend borders effortlessly. Unlike most traditional crimes, cybercrime is not bound by geography. A hacker based in one country can penetrate the servers of an institution in a second country using infrastructure hosted in a third. Such acts implicate multiple jurisdictions, each with different legal systems, privacy standards and enforcement mechanisms. Anonymity technologies such as the Tor network and encrypted messaging applications leave few digital footprints, making attribution difficult, while cryptocurrencies complicate investigations by allowing illicit financial flows to cross

[1] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
[2] BD Emerson, *Cybercrime Statistics 2025: Cost, Threats & Trends*, https://www.bdemerson.com/article/complete-cybercrime-statistics.
[3] Cybersecurity Ventures, *Cybercrime To Cost the World $10.5 Trillion Annually by 2025* (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
[4] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007).
[5] Brian Krebs, *Spam Nation: The Inside Story of Organized Cybercrime* (Sourcebooks 2014).

 [ISSN 2581-5369]

borders without conventional banking oversight. These features have turned cybercrime into a quintessential transnational crime.

The United Nations Office on Drugs and Crime (UNODC) has classified cybercrime as one of the fastest-growing forms of transnational crime, posing threats not only to individuals but also to critical national infrastructure, governance and public trust.[6] The European Union Agency for Cybersecurity (ENISA) reported in its 2024 threat landscape that cyberattacks targeting multiple jurisdictions had risen by nearly 40% over two years.[7] The cross-border character of cybercrime challenges the principle of territorial sovereignty, a cornerstone of international law. Traditional jurisdictional concepts struggle to apply effectively when neither the offender nor the infrastructure lies within the victim state.[8]

A. Factors fuelling the growth of cybercrime as a transnational crime

The rise of transnational cybercrime is not accidental but rather a product of several intertwined global developments. The foremost is digital interconnectivity, which has expanded exponentially, with over five billion internet users and billions of Internet-of-Things (IoT) devices worldwide, each connection representing a potential entry point for cyber exploitation.[9] The increasing integration of artificial intelligence (AI) across almost every sector, including defence, financial systems and healthcare, has created high-value targets that attract sophisticated criminal groups.

A second factor is anonymity, which lies at the core of the growth in cybercrime. Technologies such as encryption, virtual private networks (VPNs) and the dark web provide an operational environment in which cybercriminals can remain hidden and operate safely, while currencies such as Bitcoin and Monero facilitate untraceable ransom payments and money laundering.[10]

A third factor is the jurisdictional gap created by asymmetric legal development across nations. Advanced economies generally possess strong data protection and cyber laws, whereas developing nations often lack both legislation and enforcement capacity. These inconsistencies turn some states into safe havens for cybercriminals, who exploit weak local laws to conduct international operations.[11]

---

[6] U.N. OFFICE ON DRUGS & CRIME, *Global Programme on Cybercrime* (2023).
[7] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), *Threat Landscape 2024* (2024).
[8] Vasileios Karagiannopoulos, *Cybercrime, Jurisdiction and International Cooperation: The Challenges of Global Governance*, 42 COMPUTER L. & SEC. REV. (2024).
[9] INTERPOL, *Global Cybercrime Strategy 2022-2025* (2022).
[10] KREBS, *supra* note 5.
[11] MICHAEL CHERTOFF & PAUL ROSENZWEIG, *Exploring International Approaches to Cybersecurity* (Brookings Inst. Press 2019).

 [ISSN 2581-5369]

Finally, economic and geopolitical incentives drive much contemporary cybercriminal behaviour. Organized groups backed by state actors frequently engage in cyber-espionage to steal intellectual property, manipulate public discourse or disrupt rival economies. The WannaCry and NotPetya outbreaks of 2017 demonstrated how ransomware could cripple entire industries and national health systems.[12]

III. MAJOR GLOBAL CASE STUDIES

A. LockBit ransomware syndicate (2024)

In February 2024, a coalition of agencies led by the United States and the United Kingdom executed a coordinated takedown of the LockBit ransomware network, one of the world's most prolific ransomware-as-a-service (RaaS) operations.[13] The US Treasury imposed sanctions, and a reward of up to USD 10 million was offered for information leading to the capture of the group's Russian leader.

Figure 1: Overall distribution of LockBit victims by region.[14]

LockBit exemplified the decentralized and borderless nature of modern cybercrime. It spread across continents, targeting hospitals, corporations and government entities worldwide and demanding ransom payments in cryptocurrency. The takedown required coordination between Europol, the FBI and cybersecurity agencies from multiple nations, demonstrating that no single state can effectively address transnational cyber threats in isolation.

B. Operation Endgame (2024)

In May 2024, Operation Endgame became one of the largest global crackdowns on ransomware infrastructure. Conducted by Europol together with law enforcement agencies from Germany, the Netherlands, France, Denmark, Ukraine, the United Kingdom and the United States, it dismantled more than 100 servers and seized around 2,000 malicious domains used in ransomware distribution.[15]

The operation highlighted the crucial role of cross-border intelligence sharing and legal cooperation. It also showed how cybercrime infrastructures rely on global digital supply chains, making enforcement possible only through multilateral collaboration.

C. SolarWinds supply chain attack (2020)

---

[12] EUROPOL & INTERPOL, *Ransomware: A Growing Transnational Threat* (2022).
[13] *U.S. Issues Cyber-Related Sanction on Russian National*, REUTERS (May 7, 2024).
[14] *Understanding the LockBit Ransomware Breach*, SECURITY BLUE TEAM (Feb. 6, 2025), https://www.securityblue.team/blog/posts/lockbit-ransomware-breach-explored.
[15] *Massive Police Sweep Across Europe Takes Down Ransomware Networks and Arrests Four Suspects*, ASSOCIATED PRESS (May 30, 2024).

The SolarWinds cyberattack remains one of the most sophisticated examples of state-linked transnational cyber-espionage.[16] Attackers inserted malware into SolarWinds' Orion software, which reached more than 18,000 organizations worldwide, including US federal agencies and major corporations. The incident blurred the boundary between cybercrime and cyberwarfare, demonstrating how commercial software supply chains can be exploited through operations attributed to state-sponsored actors. It also catalysed reforms in cybersecurity governance and supply chain risk management.

IV. THE INDIAN SCENARIO

India's digital transformation has been remarkable. The country has over 850 million internet users and one of the largest fintech markets in the world, supported by vast infrastructure that is also vulnerable. The Information Technology Act, 2000, together with the Digital Personal Data Protection Act, 2023, forms the primary legal framework for cyber offences, supplemented by rules on data protection, intermediary liability and electronic evidence. Owing to the transnational nature of cybercrime, however, India faces a twofold challenge: safeguarding its citizens and addressing crimes that originate or operate across borders.

A. The Rs. 260 crore call centre scam (2023)

In 2023, the Central Bureau of Investigation (CBI) uncovered a Rs. 260 crore cyber-fraud syndicate operating out of the Delhi-NCR region.[17] The group impersonated US government agencies, such as the Social Security Administration, and targeted elderly Americans through fake call centres. It extorted payments in cryptocurrency, routing the proceeds through Dubai and other offshore networks. The case highlighted India's emerging role as both a target and an operational hub for transnational cybercrime.

B. Digital arrest fraud (2024)

In October 2024, Indian authorities reported a disturbing new trend of so-called digital arrests. Fraudsters based in Cambodia duped an Indian citizen of Rs. 1.26 crore by posing as a CBI officer and the Chief Justice of India.[18] The victim was coerced into transferring funds under the threat of arrest.

---

[16] U.S. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020).
[17] Raj Shekhar Jha, *CBI Unravels Rs. 260 Crore International Cyber Fraud Syndicate Operating from Delhi-NCR*, TIMES OF INDIA (Oct. 2023).
[18] PTI, *Cambodia-Based Fraudsters Dupe Gujarat Man of Rs. 1.26 Crore by Posing as CJI, CBI Officer*, THE WEEK (Oct. 23, 2024).

 [ISSN 2581-5369]

The case exemplified how transnational criminal networks exploit psychological manipulation and cross-border anonymity to victimize Indian citizens.

C. The Rs. 117 crore cyber fraud case (2024)

In December 2024, the CBI conducted searches across Delhi and Gurugram in relation to a cyber-fraud scheme involving fake investment platforms. Funds were routed through Indian 'mule accounts' before being withdrawn via foreign ATMs. The case revealed how global laundering operations exploit the Indian financial system.

These incidents illustrate the increasing complexity of cybercrime within India's digital economy. They also underscore the urgent need for enhanced international cooperation, faster cross-border evidence sharing and updated legal mechanisms aligned with global conventions.

V. Legal and jurisdictional challenges

A. Jurisdictional ambiguity

Determining jurisdiction is one of the greatest obstacles to effective prosecution, owing to the absence of territorial boundaries in cyberspace. Crimes committed across multiple jurisdictions may give rise to a conflict of laws, in which several countries either claim or deny the authority to investigate.

For instance, Section 75 of the Information Technology Act extends jurisdiction to offences committed outside India where they involve Indian computer systems.[19] Enforcing this extraterritorial provision, however, depends on cooperation from foreign states, which is often delayed by bureaucratic hurdles or the absence of treaties, particularly where the offender, the victim and the digital infrastructure span multiple territories.

B. Extradition and mutual legal assistance

Data localization and privacy laws frequently restrict the exchange and sharing of critical case information and evidence. Mutual legal assistance treaties (MLATs), intended to facilitate cross-border cooperation, are often slow and bureaucratic, taking months to yield access to data and thereby proving ineffective against time-sensitive cyber investigations.[20]

C. Digital evidence and data sovereignty

Cloud computing has fragmented data storage across multiple jurisdictions. Companies frequently resist disclosure, citing data protection laws or the absence of local warrants, and the resulting tension between data sovereignty and transnational enforcement remains unresolved.

[19] The Information Technology Act, No. 21 of 2000, s. 75 (India).
[20] OECD, *The Human Cost of Cybercrime: Beyond the Financial Losses* (2023).

 [ISSN 2581-5369]

From the Indian perspective, even after the establishment of specialized cybercrime cells under the state police and of the Indian Cybercrime Coordination Centre (I4C), international coordination remains a bottleneck. The lack of direct access to electronic evidence stored abroad significantly hampers investigations and prosecutions.[21]

Developing nations also face capacity gaps, including a shortage of trained cyber-forensic experts, inadequate digital infrastructure and limited funding for cyber-policing. This imbalance reinforces a digital divide in law enforcement capabilities between the Global North and the Global South.

VI. THE HUMAN AND SOCIETAL DIMENSION

Cybercrime carries a human cost as well. It undermines public trust in digital governance, jeopardizes livelihoods and corrodes institutional credibility. Victims of identity theft or ransomware often experience long-term psychological and financial trauma. When hospitals, airports or government databases are attacked, the fallout is not limited to data loss; it also disrupts lives, healthcare and national stability.

VII. INTERNATIONAL LEGAL FRAMEWORKS AND COOPERATIVE MECHANISMS

A. The Budapest Convention on Cybercrime (2001)

The Budapest Convention remains the cornerstone of international cooperation against cybercrime.[22] It standardizes definitions of cybercrime and provides mechanisms for real-time data preservation, cross-border investigation and mutual assistance. More than 60 countries, including the United States and most of Europe, have ratified it. India is not a signatory, citing concerns about sovereignty and an unequal negotiation process, although it informally aligns its domestic cyber laws with several of the Convention's provisions.

B. United Nations and regional frameworks

The United Nations Convention against Transnational Organized Crime and the Protocols thereto, administered under the United Nations Office on Drugs and Crime (UNODC), recognize cybercrime as a key form of transnational organized crime and support capacity-building initiatives for developing nations.[23] In December 2024, the UN General Assembly

[21] MARK GOODMAN, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World* (Doubleday 2015).
[22] CONVENTION ON CYBERCRIME, *supra* note 1.
[23] U.N. OFFICE ON DRUGS & CRIME, *Global Programme on Cybercrime: Annual Report* (2023).

 [ISSN 2581-5369]

adopted the United Nations Convention against Cybercrime, the first comprehensive global treaty aimed at harmonizing legal responses to cybercrime.[24]

Regional organizations such as Europol, INTERPOL and ENISA play vital roles in facilitating intelligence sharing and joint operations such as Operation Endgame. In the Asia-Pacific region, initiatives such as the ASEAN-Singapore Cybersecurity Centre of Excellence provide training and foster regional cooperation.

VIII. Recommendations and the Way Forward

Addressing cybercrime as a transnational threat demands a multilayered approach integrating legal reform, technological innovation and diplomatic collaboration. The foremost priority is the harmonization of legal frameworks. Nations should align their definitions of cybercrime to achieve uniformity and set common procedural standards for data requests and evidentiary requirements. States should also reconsider acceding to the Budapest Convention or actively participate in shaping the new UN treaty to ensure equitable representation. A second priority is cross-border data access. The international community should develop streamlined frameworks, similar to the US CLOUD Act, that enable faster data exchange between allied states.

India's forthcoming Digital India Act could incorporate comparable provisions for real-time international cooperation. A third priority is capacity-building in developing nations. Transnational operations such as LockBit exploit weaker jurisdictions by using them as safe havens, and the international community should therefore invest in building cyber-forensic capacity and investigative training in developing economies. Because most cyber infrastructure is privately owned, collaboration between governments, corporations and cybersecurity firms is crucial; joint threat-intelligence sharing and early-warning mechanisms can help prevent attacks. Finally, India must strengthen its domestic framework by modernizing its cyber laws to address emerging threats such as ransomware and cryptocurrency laundering. Adjudication can be accelerated through dedicated cybercrime courts and specialized prosecutors, and enhanced cooperation between CERT-In, the CBI and global agencies will be key.

IX. Conclusion

The rise of cybercrime as a transnational phenomenon represents one of the most profound legal and security challenges of the twenty-first century. It compels a rethinking of the notions of territory, jurisdiction and sovereignty, demanding forms of cooperation between states that are

[24] United Nations Convention against Cybercrime, G.A. Res. 79/243 (Dec. 24, 2024).

 [ISSN 2581-5369]

not traditionally provided for in existing criminal law. Global frameworks such as the Budapest Convention and regional initiatives such as Operation Endgame have made progress, yet the pace of cybercriminal innovation continues to outstrip legal reform. India faces the twofold challenge of safeguarding its vast digital ecosystem while contributing to global cyber governance.

Ultimately, the fight against cybercrime cannot be won in isolation. It requires a shared global vision rooted in legal harmonization, technological collaboration and mutual trust. As cyberspace becomes the new frontier of both commerce and conflict, the transnational evolution of cybercrime will determine not only the safety of networks but also the integrity of nations themselves.

*****

 [ISSN 2581-5369]