International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Need for Cybercrime Regulation on A Global Scale by International Law and Cyber Conventions

Archana Johari[1], Dr. Lalit Prakash[2]

[1]Research Scholar, Institute of Legal Studies, Shri Ramswaroop Memorial University Lucknow, Uttar Pradesh, India
[2]Assistant Professor, Faculty of Law, Banaras Hindu University, Varanasi, Uttar Pradesh, India

Abstract
This paper examines the urgent need for harmonised global regulation of cybercrime through international law and specialised cyber conventions. It argues that the inherently transnational nature of cyber-dependent and cyber-enabled offences, combined with the volatility and extraterritoriality of electronic evidence, renders purely domestic responses inadequate. The analysis traces the evolution of the international legal framework from the Budapest Convention and its Second Additional Protocol on electronic evidence to the newly adopted United Nations Convention against Cybercrime, situating these instruments within broader debates on sovereignty, jurisdiction, and digital sovereignty. It further evaluates regional initiatives and domestic legislative trends, highlighting persistent fragmentation, capacity gaps, and divergent normative approaches, particularly regarding content-related offences and state surveillance. A central claim is that effective global cybercrime regulation must be explicitly grounded in international human rights law, embedding robust safeguards for privacy, freedom of expression, due process, and data protection in both substantive and procedural rules. The paper concludes by proposing a model of complementary, human-rights–centred, and multi-stakeholder governance that aligns existing instruments, strengthens mutual legal assistance, and prioritises capacity-building, especially for developing States.

Keywords: cybercrime regulation; international law; Budapest Convention; UN cybercrime convention; electronic evidence.

I. Introduction

The exponential expansion of digital technologies has radically changed the way that humans interact, trade, govern and organise. Yet this digital revolution also has a dark side: cybercrime has become one of the most important security and economic challenges of the twenty-first century. Global costs of cybercrime are expected to reach $10.5 trillion per year by 2025, which will be the largest transfer of economic wealth in history and surpass the combined gross domestic product of most countries. If calculated in terms of a country, cybercrime would be the third-largest economy in the world behind the United States and China. These staggering numbers are not just about financial losses, but also of destroyed data, stolen intellectual property, lost productivity, reputational damage and costs of post-attack's forensics and system restoration.[1]

Cybercrime is inherently transnational in nature. Offenders systematically use the jurisdictional fragmentation and route attacks to different countries, using legal discrepancies, enforcement abilities, and mechanisms for international cooperation. A single cyber incident may involve perpetrators in one State, victims in another, servers in a third and data storage infrastructure distributed across cloud platforms in multiple jurisdictions.[1] This jurisdictional complexity makes traditional territorial criminal law patterns unsuitable and calls for a coordinated international approach that lies in international law and specific international cyber conventions.

International attempt to deal with the cyber crime using legally binding instruments has led to some remarkable development in recent years. The Council of Europe's Convention on Cybercrime (Budapest Convention) adopted in 2001 is the most comprehensive and widely ratified regional treaty establishing a model for substantive criminalisation, procedural powers and cross-border cooperation which has informed national legislation across antiquity and Europe.[2] More recently, the United Nations Convention against Cyber Crime is a ground breaking achievement: the first universal treaty specifically dedicated to the fight against offences committed using information and communications technology (ICT) systems.[3] Adopted by the UN General Assembly in December 2024 and opened for signature in Hanoi, Vietnam, in October 2025, the Convention received signatures from 74 States, indicating general international acceptance of the need for a global framework.[4]

Despite this progress, the global architecture for cybercrime remains fragmented, fought over and uneven with implementation. Divergent conceptions of "cybercrime" and competing geopolitical interests, human rights issues and acute disparities in technical and institutional capacity continue to hamper the emergence of a truly coherent and effective regime. This article explores the need for cybercrime regulation at a global level and analyses the opportunities and shortcomings of current international instruments, the difficulties of dealing with sovereignty and jurisdiction issues and matters of technology, and possible avenues towards a more robust global system based on human rights.

II. The Transnational Nature of Cybercrime and the Regulatory Imperative

A. Defining Cybercrime in International Law

The international legal instruments have however tended not to use abstract definitions of "cybercrime," but instead have taken an offence-based approach, requiring States to criminalise specific categories of conduct involving ICT systems. The Budapest Convention, for example, requires the criminalisation of cyber dependent offences, such as illegal access to computer systems, illegal interception of data, data interference, system interference, and misuse of devices, as well as those cyber enabled offences, such as computer related offences of fraud and forgery, offences regarding sexual abuse of children online, as well as offences concerning copyright infringement. This pragmatic approach has led to substantial

[1] Council of Europe, *Cybercrime, Evidence and Territoriality: Issues and Options* https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98 accessed 22 February 2026.
[2] 'The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention' (Malque Publishing OJS, 18 September 2024) https://malque.pub/ojs/index.php/mr/article/view/5348 accessed 22 February 2026.
[3] United Nations Office on Drugs and Crime, 'United Nations Convention against Cybercrime' (2024) https://www.unodc.org/unodc/en/cybercrime/convention/home.html accessed 22 February 2026.
[4] Drishti IAS, 'United Nations Convention against Cybercrime' (28 October 2025) https://www.drishtiias.com/daily-updates/daily-news-analysis/united-nations-convention-against-cybercrime accessed 22 February 2026.

convergence in the domestic legislation, and enabled mutual legal assistance by creating a baseline of dual criminality.[5]

The United Nations Convention against Cybercrime is no exception to this in terms of its general definition, instead it focuses on specific offences. Its substantive provisions among others require the criminalisation of illegal access to information systems, illegal interference with data, computer-related fraud, child sexual exploitation used as a tool for spying and criminal acts, etc.[6] The Convention features also procedural measures for the investigation and international cooperation, giving a strong emphasis to electronic evidence sharing among countries. Importantly, both these instruments recognise the balance between the demands for harmonised legal frameworks and the respect for the principle of legality, and avoid overly broad or vague definitions that could be used as an excuse to stifle legitimate expression or dissent.

B. Jurisdictional Fragmentation and the Limits of Territorial Sovereignty

Cybercrime threatens the basic notions of territorial jurisdiction which form the basis of the traditional concept of criminal law. Digital attacks easily cross physical borders, yielding situations where more than one State could assert its right of jurisdiction in a particular case on the basis of territoriality, nationality, passive personality, or the protective principle. For example, a ransomware attack planned by nationals of State A (using servers in State B, where the victims are in State C and where the effects occur in State D) creates enormous jurisdictional challenges. The lack of clear international norms in regulating such overlapping claims can mean impunity -- where no State takes effective prosecutions -- or conflicts of jurisdiction as it leads to forum shopping, duplicated proceedings and diplomatic friction.[7]

The volatility of electronic evidence adds to such challenges. Digital data can be modified, deleted, or moved in seconds and cloud computing systems regularly create multiple legal agency jurisdictions of data without any consideration of legal boundaries.[8] Traditional mutual legal assistance treaty (MLAT) processes that are designed for physical evidence and more sluggish investigations are no match for the velocity and magnitude of cybercrime. Research indicates that over half of all criminal investigations must use cross-border electronic evidence to secure a conviction, yet MLAT procedures often take as long as weeks or months to fulfill requests, some of which occur too late to benefit criminal investigators, and seriously jeopardize a case.[9] This mismatch in time highlights the need for streamlined, treaty-based mechanisms for the expeditious preservation and production of electronic evidence.

C. The Economic and Social Impact of Cybercrime

The economic cost of cybercrime is enormous and growing. Global costs of cybercrime, which in 2015 is approximately $3 trillion, are projected to reach $10.5 trillion annually by 2025 (compound annual growth rate of 15 per cent. Detailed breakdowns of these costed $150 billion to $250 billion per year due to direct financial losses from ransomware, business email compromise (BEC), cryptocurrency fraud and identity

[5] Council of Europe, *Convention on Cybercrime (ETS No 185)* https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime accessed 22 February 2026.
[6] 'United Nations Convention against Cybercrime' (Wikipedia, 2025) https://en.wikipedia.org/wiki/United_Nations_Convention_against_Cybercrime accessed 22 February 2026.
[7] Study IQ, 'Cybercrime Jurisdiction in a Borderless Internet' (2 January 2026) https://www.studyiq.com/articles/cybercrime-jurisdiction-in-a-borderless-internet/ accessed 22 February 2026.
[8] Council of Europe, *Second Additional Protocol to the Budapest Convention on Cybercrime* https://rm.coe.int/2nd-additional-protocol-budapest-convention-en/1680a2219c accessed 22 February 2026.
[9] 'SoK: Cross-Border Criminal Investigations and Digital Evidence' (2022) 8(1) *Cybersecurity* https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 accessed 22 February 2026.

theft, while business downtime and lost productivity costs add another $500 billion to $1 trillion annually. Brand damage, nation state cyberattacks, and cyber insurance impacts add hundreds of billions more.[10] Ransomware attacks alone have increased to new all-time highs. In 2024, there were more than 5600 ransomware incidents made public across the world and more than 2600 victims in America alone.[11] The four quarters in the first half of 2024 saw an average of 1,827 ransomware attacks, a 33 per cent rise over the same period in 2023 and the most active quarter on record. Critical sectors such as healthcare, financial services, manufacturing, government, and critical infrastructure are still high-value targets and the attacks can lead to operational disruptions, data breaches, and in the case of healthcare systems, direct threats to human life.[12]

Beyond economic losses, cybercrime causes profound social losses. Online scams, sextortion and romance fraud victimise millions of people each year, with especially devastating consequences in the developing world where the capacity for law enforcement is low. Cyber-enabled child sexual abuse material is continuing to proliferate with the advance of encryption technologies coupled with the global reach of the internet. The psychological burden of the victims, along with the trust lessening of digital systems that are integral to modern existence is a reminder that cybercrime is not a technical or financial issue, but that of fundamental human security and dignity.[13]

III. The Budapest Convention: A Regional Model with Global Influence

A. Origins, Objectives, and Scope

The Convention on Cybercrime of the Council of Europe is commonly referred to as the Budapest Convention and was agreed upon on 23 November 2001 and entered into force on 1 July 2004. It is still the most influential and comprehensive international treaty on cybercrime with over 74 Parties as of 2025, including many States that are non-European such as the United States, Japan and Australia, Canada and countries in Africa, Latin America, and Asia-Pacific.[14] The Convention seeks to achieve the following inter-related objectives namely harmonisation of substantive criminal law, provision of sufficient procedural powers for investigation and prosecution of the offence and strengthening of international cooperation in cybercrime related matters.

The Budapest Convention has been the model for regional instrument and domestic legislation all over the world. "It has seen its substantive definitions of offences and procedural mechanisms adopted in national laws dealing with cybercrime in diverse legal traditions which has led to a certain level of global normative convergence in the law facilitating cooperation even between States not formal Parties" leaving the Council of Europe and partner organisations "[t]o contribute to a global field of normative

[10] Cyber Defense Magazine, 'The True Cost of Cybercrime: Why Global Damages Could Reach 1.2–1.5 Trillion by End of Year 2025' (12 March 2025) https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/ accessed 22 February 2026.

[11] Fortinet, 'Ransomware Statistics 2025: Latest Trends & Must-Know Insights' (14 January 2025) https://www.fortinet.com/resources/cyberglossary/ransomware-statistics accessed 22 February 2026.

[12] Cyberint, 'Ransomware Annual Report 2024' (12 January 2025) https://cyberint.com/blog/research/ransomware-annual-report-2024/ accessed 22 February 2026.

[13] INTERPOL, 'More than 300 Arrests as African Countries Clamp Down on Cyber Threats' (23 March 2025) https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats accessed 22 February 2026.

[14] EUCRIM, 'CoE Ratifications' (25 January 2026) https://eucrim.eu/documentation/ratifications/ accessed 22 February 2026.

interoperability in the framework of cybersecurity in Africa and the Global South through capacity building programmes, model laws, and technical assistance".[15]

B. Substantive and Procedural Provisions

The substantive criminal law provisions of the Budapest Convention require States Parties to criminalise four categories of offences: offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference and misuse of devices); computer-related offences (computer-related forgery and fraud); and content-related offences (child sexual abuse material); and offences related to copyright and neighbouring rights. These provisions provide common basis, as this ensures the dual criminality for the extradition and mutual legal assistance purposes.

Procedurally, the Convention gives law enforcement authorities powers of investigation adapted to the digital environment. Article 16 mandates expedited preservation of computer data stored for service providers to preserve volatile data pending production orders. Article 18 sets production orders of certain computer data in the possession or control of individuals or service providers. Articles 19 and 20 deal with the search and seizure of stored data, whilst Articles 20 and 21 deal with the real-time collection of traffic data and interception of the content data. These tools recognise the nature of digital evidence as being ephemeral and requires swift action to prevent destruction or alteration.

International cooperation mechanisms under the Convention are a 24/7 network of contact points to provide quick communication and assistance (Article 35), mutual legal assistance in the investigation and prosecution of criminal offences related to computer systems and data (Articles 23-34) and extradition provisions (Article 24). These mechanisms have proved effective in facilitating timely cross border cooperation, particularly in urgent situations where cooperation mechanisms, where the time taken is usually much longer, would take an excessive amount of time to process.

C. The Second Additional Protocol: Enhanced Cooperation and Electronic Evidence

Recognising the ongoing development in the field of technology and the growing challenges in cross-border access to electronic evidence the Council of Europe adopted the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, which opened for signature on 12 May 2022. The Protocol deals with an important gap: the tension between the territorial nature of the traditional mutual legal assistance principle and the distributed, borderless nature of cloud-based data storage.[16]

The Second Additional Protocol contains a number of innovative mechanisms. It features simplified mutual legal assistance procedures and creates new types of cooperation between competent bodies, even in cases of emergency actions which demand immediate action. Significantly, it allows for direct cooperation between law enforcement authorities and service providers or other entities with possession or control of relevant data, including expedited disclosure of subscriber information and other categories of data. Article 9 of the Protocol, for example, creates conditions under which authorities may request

[15] UNCTAD, 'Cybercrime Legislation Worldwide' (19 June 2025) https://unctad.org/page/cybercrime-legislation-worldwide accessed 22 February 2026.

[16] Eurojust, 'Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access' (26 July 2022) https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access accessed 22 February 2026.

expedited disclosure of stored data by service providers with safeguards in relation to lawfulness, necessity and proportionality.[17]

The Protocol is accompanied by strong Treaties safeguards the protection of the level of personal data, privacy and human rights of the rule of law, as they are part of the legal tradition human rights in the Council of Europe. These include requirements that intrusive investigative measures be subject to independent oversight, that data protection principles be respected in the cross-border sharing of data, and access to effective remedies for the affected persons. This way, the Protocol aims at striking a balance between the operational needs of law enforcement on one side, and fundamental rights as guaranteed under the European Convention on Human Rights and other instruments, on the other side.

IV. The United Nations Convention against Cybercrime: Towards a Universal Framework

A. Negotiation, Adoption, and Entry into Force

The origin of the United Nations Convention against Cybercrime can be traced to longstanding demands made by States, in particular from the Global South, for a universal, inclusive framework to combat cybercrime within the purview of United Nations. Pursuant to this resolution, the UN General Assembly set up an Ad Hoc Committee to draft a universal international treaty against the misuse of ICT systems for criminal offences. The Ad Hoc Committee convened several negotiating sessions between 2021 and 2024, with States, international organizations, civil society and technical experts participating in extensive consultations.[18]

The Ad Hoc Committee adopted the text of the Convention in August 2024 and it was also adopted by consensus of the UN General Assembly on December 24, 2024 by Resolution Number: 79/243. Signing and entry into force The Convention was open for signature at a high-level conference convened in Hanoi, Vietnam, from 25 to 26 October 2025, co-chaired by President Lương Cường of Vietnam and UN Secretary-General António Guterres. By January 2026, 74 States had signed the Convention signalling their intention to ratify. 6 The treaty takes effect 90 days after the fortieth instrument of ratification, acceptance, approval or accession.[19]

Hanoi was chosen as the signing location in part for its symbolism, being the first UN treaty to be signed in Vietnam, and also the first named after a Vietnamese place. The location also sparked controversy with human rights groups expressing anxiety over Vietnam's record on free speech and internet freedom, emphasizing wider tensions over the impact of the Convention on human rights.

B. Substantive Provisions and Core Obligations

The UN's Convention against Cybercrime provides an end-to-end regime of criminalisation, procedure and international cooperation. Its enactment provisions for substantive criminal law require States Parties to indict fundamental cyber-dependent offences such as unauthorized access to information systems, interception of data, data interference and computer-related fraud and also cyber-enabled crimes such as offenses involving the sexual exploitation of children and other grave crimes committed through or by

[17] Eurojust, 'Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data' (17 October 2024) https://www.eurojust.europa.eu/publication/article-9-second-additional-protocol-convention-cybercrime-expedited-disclosure-stored-computer-data accessed 22 February 2026.

[18] United Nations Office on Drugs and Crime, 'Ad Hoc Committee – Home' (25 May 2021) https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home accessed 22 February 2026.

[19] United Nations Treaty Collection, 'Convention against Cybercrime' (23 December 2024) https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en accessed 22 February 2026.

means of ICTs. 5 The Convention takes an offence-based approach, eschewing overly broad or ambiguous terms that may be misused to criminalise lawful online conduct.

In procedural terms, the Convention requires the authority to also be entrusted with investigative powers, which include expedited preservation and production of electronic evidence, seizure or closing down data (powers of search and seizure), monitoring within its territory of traffic data in real time or content data in "real time" on condition that such authorities will only carry out their duties when the competent authorities have already approved specific operations as being strictly necessary while ensuring they respect strict conditions regarding legality, necessity and proportionality. These provisions are derived from the Budapest Convention model but have been customized so as to be compatible with a broad array of legal systems and domestic constitutional structures. International cooperation is another key of the Convention. It creates a system of mutual legal assistance, extradition, and joint investigation, with the key feature being cross-border sharing of electronic evidence. The Convention also provides for the conference of states parties to be established as the monitoring body responsible for implementation, encouraging best practices exchange and technical assistance structures and capacity building measures, in particular towards developing countries.

C. Human Rights Safeguards and Contested Issues

The process of negotiating the UN Convention was characterised by major disagreements regarding its ambit and definitions and human rights protections. Civil society organisations, technology companies and many States voiced concern that overly broad definitions of offences or vague references to "public order" or "national security" could be used by authoritarian regimes to criminalise political dissent, journalism and human rights advocacy. Particular controversy exists around proposals to incorporate offence definitions based on the content of material, such as the spread of extremist or terrorist material, disinformation, and "online propaganda", which many feared could be used to facilitate censorship and repression.[20]

At the end, human rights protection to prevent these risks are incorporated into the Convention. Its provisions confirm the obligations of States Parties to international human rights law such as the International Covenant on Civil and Political Rights, and mandate that measures adopted in connection with the Convention must respect fundamental freedoms such as privacy, freedom of expression, and freedom of association.[21] Intrusive powers to investigate, collect, interview or study must be executed subject to certain other principles concerning legality, necessity, proportionality, and procedural fairness, as well as controlled by independent supervision and effective remedies.

Academic and policy analyses have warned, however, that the effectiveness of these safeguards will be dependent much on domestic implementation and enforcement. In States with weak rule of law institutions or where judicial independence is compromised, the provisions of the treaty may not give the level of protection against abuse that it should.[22] Additionally, some have criticised the Convention for lacking strong mechanisms to oversee its implementation or enforce compliance with its human rights standards.

[20] United Nations University, 'Understanding the UN's New International Treaty to Fight Cybercrime' (3 February 2026) https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime accessed 22 February 2026.

[21] Hanoi Convention, 'Viet Nam Announces Official Dates for the Signing Ceremony of the United Nations Convention on Cybercrime' (28 July 2025) https://hanoiconvention.org/viet-nam-announces-official-dates-for-the-signing-ceremony-of-the-united-nations-convention-on-cybercrime/ accessed 22 February 2026.

[22] Digital Watch Observatory, 'Ad Hoc Committee on Cybercrime' (17 February 2026) https://dig.watch/processes/cybercrime-ad-hoc-committee accessed 22 February 2026.

V. Regional Instruments and Domestic Cybercrime Legislation

A. Regional Frameworks and Their Interaction with Global Norms

Beyond the Budapest and UN Conventions, regional organisations have developed their own approaches to cybercrime, model laws and cooperative frameworks to deal with cybercrimes. The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) covers cybercrime, electronic transactions and data protection in one place with the aim of reflecting African priorities and traditions in its legal frameworks. Regional model laws in the Economic Community of West African States, known as ECOWAS, the East African Community, known as EAC, and the Association of Southeast Asian Nations or ASEAN have also taken help from the Budapest Convention whilst adapting provisions to local contexts.

These regional instruments have a number of purposes. In this regard, they "provide a legal basis for mechanisms for intra-regional cooperation and harmonisation among the States in similar stages of development and provide the platform for capacity building and knowledge sharing specific to regionally-defined problems". For example, mutual legal assistance frameworks in the EAC are designed to overcome particular challenges facing member States in accessing cross-border electronic evidence, but implementation has been uneven and procedural barriers continue to exist.[23]

The growing number of regional frameworks leads to questions of coherence and fragmentation. Where regional instruments have obligations which differ from or conflict with those found under the Budapest or UN Conventions, the States may be faced with competing commitment. Scholarly commentary emphasises the importance of making sure that a regional and global instruments are mutually reinforcing rather than contradictory and that States are able to implement a number of treaties without legal or practical conflicts.

B. National Cybercrime Legislation: Convergence, Divergence, and Implementation Gaps

International treaties and model laws have facilitated a significant amount of convergence in national cybercrime legislation. According to the United Nations Conference on Trade and Development (UNCTAD), more and more countries in all regions have adopted specific cybercrime legislation, often based on Budapest-style definitions of offences as well as procedural powers. This convergent makes it easier to cooperate through dual criminality and compatible frameworks in investigating.

Profound divergence still exists, however. Some States have adopted very broad or indefinite offences on cybercrimes, especially in relation to content, national security or public order, and this raises issues as to compliance with international human rights standards. Others lack specialised procedural instruments, effective data retention regimes, and adequate safeguards in relation to privacy and due process. In India, for example, recent legislative reforms including the Bharatiya Nyaya Sanhita (BNS) 2023, replacing Indian Penal Code and coming into force on 1 July 2024 taxa cybercrimes and new forms of fraud including organised cybercrimes organisations and recognised digital evidence including email and server logs. The Bharatiya Nagarik Suraksha Sanhita (BNSS) simplified procedures to permit electronic filing of First Information Reports (FIRs) and digital submission of evidence, while the Bharatiya Sakshya Adhiniyam (BSA) recognised the electronic records as primary evidence to ease the process of getting justice for the victims of cybercrimes.[24]

[23] 'Mutual Legal Assistance in Combating Cybercrimes in the East African Community' (2023) *International Journal of Multidisciplinary Research* https://www.ijfmr.com/papers/2023/5/8310.pdf accessed 22 February 2026.

[24] Kaushik Associates, 'Cyber Laws that are Being Updated in 2024' (24 April 2025) https://kaushikassociates.in/cyber-laws-that-are-being-updated-in-2024/ accessed 22 February 2026.

Capacity issues law enforcement, prosecution services and elimination of judiciary, leading to more implementation genitals in countries not developing. Even where legislation is appropriate, resource constraints, insufficient training and the absence of specialised units compromise the effectiveness of enforcement. This leads to "safe havens" for cybercriminals who exploit jurisdictions with poor institutional capacity and perpetuates impunity and hinders global efforts to combat cybercrime.

C. Jurisdiction and Extraterritoriality in Domestic Law

Domestic laws against cybercrime often claim jurisdiction on several grounds, territoriality (offences committed on the territory of the State or with effects on its territory), nationality (offences committed abroad by nationals of the State), passive personality (offences committed against nationals and residents of the State) and finally, the protective principle (offences against the security of the State and vital interests of the State).9 This multiplicity of jurisdictional claims can lead to overlaps and conflicts, especially where multiple States are claiming jurisdiction in the same incident.[25]

Extraterritorial jurisdiction of data enforcement has been a contentious topic. Some States have implemented measures which allow unilateral access to data located with foreign service providers beyond their national borders which raises concerns about violation of sovereignty, conflict of laws, and compatibility with international legal principles. The Budapest Convention's Article 32(b), allows States Parties to obtain access to computer data stored by a third State party that is kept in another State or country if they seek the lawful and voluntary consent of the person entitled to disclose the data, but this article does not authorise unilateral compulsory access without consent or cooperation mechanisms.[26]

Structured treaty-based mechanisms for direct cooperation with service providers are proposed by the Second Additional Protocol to the Budapest Convention as a way of addressing such tensions in the context of safeguards, oversight and respect for the rule of law. The European Union provides similar approaches through the e-Evidence Regulation-which establishes the harmonisation of procedures for cross-border production and preservation orders within the European Union, with notification obligations to the enforcing State in case of content or traffic data requests. These developments are part of a wider trend towards multilateral treaty-based solutions to the jurisdictional problems cloud computing and data localisation cause.[27]

VI. The Imperative for Global Cybercrime Regulation: Rationales and Justifications

A. Addressing Fragmentation and Normative Competition

The expansion of overlaying and even conflicting cybercrime tools have created a certain state of fragmentation in international law. The interaction of the Budapest Convention, the UN Convention, regional frameworks, bilateral agreements, and various national laws brings out a multi-faceted mosaic where some States belong to multiple norm-sets and others to none, which makes it easy to engage in forum shopping by states and serial killers.

[25] Hackers4u, 'How Are India's Cybersecurity Laws Evolving in the Digital Era?' (9 September 2025) https://www.hackers4u.com/How-Are-India's-Cybersecurity-Laws-Evolving-in-the-Digital-Era accessed 22 February 2026.

[26] 'Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts' (2023) *German Law Journal* (Cambridge University Press, 14 April 2023) https://www.cambridge.org/core/journals/german-law-journal/article/extraterritorial-enforcement-jurisdiction-in-cyberspace-normative-shifts/ accessed 22 February 2026.

[27] White & Case, 'EU Breaks Down Digital Borders: New e-Evidence Rules Facilitate Cross-Border Access' (6 November 2023) https://www.whitecase.com/insight-alert/eu-breaks-down-digital-borders-new-e-evidence-rules-facilitate-cross-border accessed 22 February 2026.

An international framework based on the principles of the international law widely accepted can help to resolve such tensions by offering a common raft of offences, definitions, procedural powers, and human rights protection. The UN Convention against Cybercrime is a significant move in that way, which provides a universal space of cooperation that embraces States not covered by the Budapest Convention but the issue is whether the two regimes will converge or diverge with time. Fragmentation can be managed by promoting compatibility between instruments, such as by standardizing definitions, cooperation practices, and protection, and by cross-regime cooperation can be promoted through those measures as well.

B. Enhancing Mutual Legal Assistance and Electronic Evidence Sharing

One of the central justifications for global cybercrime regulation is the need to overcome the limitations of traditional mutual legal assistance in securing electronic evidence. Conventional MLAT processes are often slow, bureaucratic, and ill-suited to the volatility and volume of digital data. International instruments therefore seek to streamline and modernise cooperation through expedited preservation requests, direct cooperation channels, standardised formats for requests, and 24/7 contact networks.

The Budapest Convention's 24/7 network and the Second Additional Protocol's provisions on expedited disclosure of stored data and cooperation with service providers are prominent examples of such innovations. The UN Convention similarly emphasises electronic evidence sharing and seeks to create a global framework for cooperation that does not depend on regional membership. Effective implementation of these mechanisms can significantly reduce investigation times, increase the likelihood that electronic evidence is preserved and admissible, and enable prosecutions that would otherwise fail due to evidentiary gaps.

International law enforcement operations demonstrate the potential of enhanced cooperation. INTERPOL-led initiatives such as Operation HAECHI-V (July–November 2024) resulted in the arrest of over 5,500 suspects and the seizure of more than $400 million in virtual assets and government-backed currencies across 40 countries, targeting financial cybercrimes including business email compromise, investment fraud, and online scams. Operation Red Card (November 2024–February 2025) led to 306 arrests and the seizure of 1,842 devices across seven African countries, disrupting mobile banking, investment, and messaging app scams affecting over 5,000 victims. These successes underscore that coordinated; treaty-based cooperation can deliver tangible results in disrupting transnational cybercrime networks.[28]

C. Building Capacity and Reducing Global Disparities

Global regulation is essential to address disparities in legal frameworks, technical capabilities, and institutional resources among States. Whilst many countries have adopted cybercrime laws, significant gaps remain, particularly in developing economies, and enforcement capacity is uneven. International treaties provide not only legal obligations but also a framework for technical assistance, capacity building, and information sharing.

The United Nations Office on Drugs and Crime (UNODC), the Council of Europe, INTERPOL, and regional bodies implement programmes to support legislative reform, training of law enforcement and judicial authorities, and establishment of specialised cybercrime units. These efforts are essential to avoid creating "safe havens" for cyber offenders and to ensure that all States can benefit from and contribute to global cybercrime control efforts. The UN Convention expressly envisages a conference of States Parties and related mechanisms to facilitate the sharing of best practices, funding, and technical support for

[28] The Hacker News, 'INTERPOL Arrests 5,500 in Global Cybercrime Crackdown, Seizes $400M' (1 December 2024) https://thehackernews.com/2024/12/interpol-arrests-5500-in-global.html accessed 22 February 2026.

national implementation. South–South and triangular cooperation can also promote the exchange of regionally relevant experience and solutions, including in areas such as mobile-money fraud, online financial crime, and protection of local critical infrastructures. Academic literature underscores that such cooperation is important for ensuring that global norms are not perceived as externally imposed but are adapted to local contexts and co-produced by stakeholders from all regions.

VII. Challenges and Critiques of Global Cybercrime Regulation

A. Sovereignty, Geopolitics, and Trust Deficits

Cybercrime regulation takes place against a backdrop of broader geopolitical contestation over cyberspace governance, digital sovereignty, and information control. Some States perceive global cybercrime treaties as potential instruments for imposing particular normative visions or for legitimising intrusive cross-border data access. The division between States that favour the Budapest Convention and those that pushed for a new UN instrument reflects these tensions, with debates often framed in terms of "Western" versus "non-Western" approaches to internet governance.

Trust deficits among major powers can hinder cooperation, particularly when cybercrime investigations implicate national security, state actors, or politically sensitive information. Concerns about espionage, data protection, and the potential misuse of cooperation mechanisms can lead States to limit information sharing or to insist on strict reciprocity and conditions, thereby reducing the effectiveness of global regimes. The challenge for international law is to build frameworks that accommodate legitimate sovereignty concerns whilst preventing those concerns from becoming pretexts for impunity or non-cooperation.

B. Over-Criminalisation and Human Rights Risks

Critiques of global cybercrime regulation emphasise the risk of over-criminalisation and the use of cybercrime laws to suppress expression, target journalists, human rights defenders, or political opponents. Academic commentary on the UN Convention negotiations warns that broad offence categories or references to vague concepts such as "public order" or "national security" can be exploited by repressive regimes. Civil society groups have also raised concerns about the potential for expanded surveillance and cross-border data access to undermine privacy and data-protection rights.

Ensuring that global treaties are interpreted and implemented consistently with international human rights law is therefore critical. This entails not only incorporating explicit human-rights clauses and safeguards into treaties but also establishing mechanisms for monitoring implementation, receiving complaints, and providing guidance on best practices. The absence of robust compliance mechanisms in the UN Convention has been identified as a significant weakness, as it leaves enforcement of human rights standards largely to domestic institutions, which may be inadequate in some contexts.

C. Technological Evolution and Regulatory Obsolescence

The rapid evolution of digital technologies, including artificial intelligence, the Internet of Things, quantum computing, and new forms of encryption and anonymisation, poses a challenge to legal frameworks that may quickly become outdated. The Budapest Convention was drafted before the widespread emergence of social media platforms, cloud computing, and mobile app ecosystems, necessitating subsequent updates and interpretive guidance through additional protocols. Global cybercrime regulation must therefore be sufficiently flexible and technology-neutral to accommodate future developments, whilst also providing mechanisms for periodic review and amendment. The adoption of additional protocols, interpretative notes, and soft-law guidance can help keep treaties relevant, but

these processes require sustained political will and multilateral consensus. The challenge is to strike a balance between legal certainty and adaptability, ensuring that frameworks remain effective as technology continues to evolve at a pace far exceeding that of legislative processes.

VIII. Conclusion

Cybercrime regulation on a global scale has become a necessity rather than an option. The ubiquity of digital technologies in economic, social, and political life means that cyber-dependent and cyber-enabled crimes can inflict significant harm on individuals, businesses, and critical infrastructures across borders, often with impunity in the absence of effective legal and institutional frameworks. The Budapest Convention, its Second Additional Protocol, and the new United Nations Convention against Cybercrime collectively represent substantial progress in building a global regime that harmonises laws, provides investigative tools, and facilitates international cooperation. Yet the emerging architecture is not without its challenges. Fragmentation, geopolitical tensions, human rights risks, and rapid technological change all threaten to undermine the effectiveness and legitimacy of global cybercrime regulation. Future efforts should focus on enhancing compatibility and complementarity between different instruments; embedding robust human rights and data-protection safeguards; fostering multi-stakeholder participation and accountability; and prioritising capacity building and equitable participation by States at all levels of development.

The need for cybercrime regulation on a global scale is thus best understood not merely as a technical requirement for law enforcement, but as a broader project of international law and governance. It involves reconciling security, sovereignty, and human rights in a deeply interconnected digital environment, and building institutions and norms that can adapt to continual technological transformation. The effectiveness of the new UN cybercrime convention and related instruments will ultimately depend on States' willingness to implement them in good faith, to cooperate across political divides, and to subject their use of digital powers to meaningful legal and democratic oversight. Global cybercrime costs exceeding $10 trillion annually represent not only an economic catastrophe but also a moral imperative for collective action. The international community must rise to meet this challenge through legally binding commitments, practical cooperation mechanisms, and unwavering respect for the rule of law and fundamental freedoms. Only through such a comprehensive, human-rights–centred approach can the promise of digital technologies be realised whilst mitigating their gravest risks.