



INTERNATIONAL LEGAL FRAMEWORK FOR THE PREVENTION OF CYBERCRIME

Rahul Jagtap*

ABSTRACT

Cybercrime is, by its nature, transnational: a single intrusion can originate in one State, route through servers in a second and third, and cause harm in a fourth, defeating the territorial assumptions on which most criminal law is built. Public international law has responded unevenly. The Council of Europe's Budapest Convention of 2001 has functioned for over two decades as the closest thing to a global standard, yet it remains a regional instrument that several major States, including India and Russia, have declined to join. The United Nations Convention against Cybercrime, adopted by the General Assembly in December 2024 and opened for signature in October 2025, was designed to close this gap through a genuinely universal treaty, but as of mid-2026 it had secured only a handful of ratifications against the forty required for entry into force, and has attracted criticism that its broad evidence-sharing powers may be misused for surveillance absent stronger human rights safeguards. This paper examines the architecture of the international legal framework governing cybercrime prevention, situates it within the general principles of public international law relating to sovereignty, jurisdiction and State responsibility, and evaluates whether the current, fragmented regime is adequate to the scale of the threat. It argues that prevention of cybercrime at the international level is less a matter of drafting new substantive offences than of building interoperable, rights-respecting mechanisms for cooperation, and that India's continued position outside both the Budapest Convention and the new UN Convention leaves an avoidable gap in an otherwise improving global architecture.

Keywords: Cybercrime, Budapest Convention, UN Convention, State Responsibility.

*BA LLB, FIFTH YEAR, GOVERNMENT LAW COLLEGE, MUMBAI.

INTRODUCTION

Crime has always adapted to the tools available to the criminal, but no prior technology has dissolved the link between the location of an act and the location of its consequences as completely as the internet has. A ransomware operator in one jurisdiction can encrypt hospital records in a second, route the ransom through a cryptocurrency exchange registered in a third, and never set foot in any of them. Traditional criminal law, built on the assumption that a State's writ runs to its own territory and its own nationals, is not equipped for this. International law's response to this problem has therefore been to build, piece by piece, a set of instruments that try to do two things at once: harmonise what counts as a cybercrime across borders, and create workable channels through which States can help one another investigate and prosecute it. This paper surveys that response as it stands in 2026, distinguishes prevention from mere criminalisation, and asks whether the current architecture, anchored by the Budapest Convention and now supplemented by the new UN Convention against Cybercrime, is fit for purpose.¹

The paper proceeds in three broad movements. First, it locates cybercrime within the general framework of public international law, addressing questions of sovereignty, jurisdiction and State responsibility that arise even before any treaty is considered. Second, it examines the principal international and regional instruments in turn, the Budapest Convention, the new UN Convention, and a set of regional frameworks, tracing what each contributes and where each falls short. Third, it turns to India's position specifically, since India's non-participation in the Budapest Convention and its undecided stance on the UN Convention offer a useful case study in the tension between sovereignty concerns and the practical benefits of multilateral cooperation. The paper concludes that prevention, as distinct from prosecution after the fact, depends overwhelmingly on the speed and reliability of cross-border cooperation mechanisms, and that this is precisely where the current regime remains weakest.

THE NATURE OF CYBERCRIME AS A TRANSNATIONAL PROBLEM

Cybercrime is generally understood to cover two overlapping categories of conduct: offences that target computer systems themselves, such as unauthorised access, data interference and the deployment of malware, and offences in which a computer system is merely the instrument

¹ United Nations Office on Drugs and Crime, United Nations Convention against Cybercrime, <https://unodc.org/unodc/en/cybercrime/convention/home.html> (last visited Sept. 24, 2026).

for a conventional crime, such as fraud, extortion or the distribution of child sexual abuse material. The distinction matters for domestic drafting, but for the purposes of international law the more important feature of both categories is the same, namely that the offence, the offender, the victim and the evidence rarely sit within a single jurisdiction at the same time.

This transnational character produces three distinct problems that any preventive legal framework must address. The first is a definitional problem: unless States broadly agree on what conduct is criminal, an act that is an offence in the victim State may not be an offence where the perpetrator is located, leaving that State with no obligation, and often no incentive, to cooperate. The second is a jurisdictional problem: even where conduct is criminal in both States, it is not always clear which State has the stronger claim to prosecute, and simultaneous claims can produce conflict rather than cooperation. The third, and in practice the most significant, is an evidentiary problem: digital evidence is volatile, easily moved, and frequently held by private service providers rather than by any government, so that even a State with an undisputed right to prosecute may be unable to gather the proof it needs without the timely assistance of others. International legal instruments addressing cybercrime can, in essence, be evaluated by how well each solves these three problems.

PUBLIC INTERNATIONAL LAW FOUNDATIONS: SOVEREIGNTY, JURISDICTION AND STATE RESPONSIBILITY

Sovereignty and the Territoriality of Cyberspace: It is now well accepted that general international law, including the principle of sovereignty and the prohibition on the use of force under the United Nations Charter, applies to State conduct in cyberspace exactly as it applies elsewhere.² The difficulty is not whether the rules apply, but how territorially defined rules apply to an environment that has no natural territorial boundaries. A server, a data packet and a human operator can each be physically located in a different State, and a single malicious act may pass through the territory of several States as mere transit, without any of them being a meaningful participant in the offence. The Tallinn Manual project, a non-binding but highly influential expert restatement of how existing international law applies to cyber operations, has become the standard reference point for working through these questions, even though it does not itself create binding obligations.³

² U.N. Charter arts. 2(4), 51.

³ Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2d ed. 2017).

Jurisdiction: Public international law recognises several bases on which a State may assert criminal jurisdiction: territoriality, where the conduct or its effects occur within the State; nationality, where the offender is a national of the State; passive personality, where the victim is a national; and, more rarely, universal jurisdiction for the most serious international crimes. Cybercrime instruments typically draw on the first three together, requiring or permitting States Parties to assert jurisdiction where an offence is committed on their territory, by their nationals, or against their nationals or infrastructure. The result is that a single cyber-incident can trigger overlapping and legitimate jurisdictional claims from several States simultaneously, which is precisely why cybercrime treaties devote as much attention to cooperation and consultation between States as they do to defining the underlying offences.

State Responsibility and Due Diligence: A distinct but related question is the responsibility of the State from whose territory a cyber-operation is launched, even where the State itself is not the author of the attack. Drawing on the customary international law principle that no State may knowingly allow its territory to be used for acts contrary to the rights of other States,⁴ commentators and States have increasingly argued that a due diligence obligation requires States to take reasonable steps to prevent their territory or infrastructure from being used to mount cyberattacks against others. This obligation, however, remains contested in its precise content and is complicated further by the attribution problem: identifying the true origin of a cyber-operation with the certainty international law traditionally demands before responsibility can be assigned is often technically difficult and easily disputed.⁵

THE BUDAPEST CONVENTION: THE FIRST-GENERATION FRAMEWORK

The Council of Europe's Convention on Cybercrime, concluded at Budapest in 2001 and in force since 2004, remains, more than two decades later, the most widely adopted binding instrument specifically addressed to cybercrime.⁶ Although negotiated within the Council of Europe, it was deliberately drafted to be open to accession by non-member States, and States

⁴ *Corfu Channel (U.K. v. Alb.)*, Judgment, 1949 I.C.J. 4, 22 (Apr. 9); see also Tallinn Manual 2.0, r. 6-7.

⁵ See Tallinn Manual 2.0, r. 15-20 (discussing the law of state responsibility as applied to cyber operations and the evidentiary difficulty of attribution).

⁶ Council of Europe, Convention on Cybercrime, E.T.S. No. 185, opened for signature Nov. 23, 2001 (entered into force July 1, 2004).

such as the United States, Japan, Canada and Israel are Parties alongside the Convention's European originators.⁷

The Convention operates on three levels that map neatly onto the three problems identified in Part II above. First, it requires Parties to criminalise a defined list of offences in their domestic law, including illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and fraud, and offences related to child pornography, thereby addressing the definitional problem through substantive harmonisation. Second, it obliges Parties to equip their domestic law with a common set of procedural powers, such as expedited preservation of stored data, production orders, and real-time collection of traffic data, so that evidence does not evaporate while a request for assistance is pending. Third, and most significantly for prevention in practice, it establishes cooperation mechanisms, including a designated 24/7 network of contact points that allows one Party's law enforcement authorities to secure urgent preservation of data in another Party's territory.

Two Additional Protocols have since expanded its scope: the first, opened in 2003, extends the Convention to acts of a racist and xenophobic nature committed through computer systems, and the second, opened in 2022, strengthens cooperation and the disclosure of electronic evidence, including direct cooperation with service providers and expedited channels for emergency assistance.⁸ As of August 2025, the Convention had 81 States Parties, making it, in practical terms, closer to a universal standard than its regional origin would suggest.⁹

The Convention's principal limitation is political rather than legal. Several major States, most notably Russia and India, have declined to accede to it, primarily on the ground that they had no role in its drafting despite it having become, in effect, a global template. A framework that is not joined by some of the States generating and receiving the largest volumes of cybercrime traffic has an obvious hole in its coverage, however well designed its internal mechanisms may be.¹⁰

⁷ Council of Europe, *Joining the Convention on Cybercrime: Benefits* (July 2026 ed.), <https://rm.coe.int/cyber-buda-benefits-1-july-2026-en/48802c5c24>

⁸ Council of Europe, *Milestones: 25 Years of International Co-operation Powered by the Convention on Cybercrime* (Budapest Convention), <https://www.coe.int/en/web/cybercrime/milestones> (last visited Sept. 24, 2026).

⁹ As of August 2025, 81 States had ratified the Budapest Convention, with two further signatories yet to ratify.

¹⁰ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

THE UNITED NATIONS CONVENTION AGAINST CYBERCRIME, 2024

Origins and Adoption: Dissatisfaction, particularly among States that had no part in drafting the Budapest Convention, with the existing regional framework led the UN General Assembly to establish an Ad Hoc Committee in 2019 to negotiate a genuinely global cybercrime treaty. After five years of negotiation, the Ad Hoc Committee's draft was adopted by the General Assembly on 24 December 2024 by resolution 79/243, as the United Nations Convention against Cybercrime.¹¹ It was opened for signature at a ceremony in Hanoi on 25 October 2025, where 72 States signed on the opening day alone, and will remain open for signature at UN Headquarters until 31 December 2026.¹²

Key Provisions –

- A common set of substantive offences broadly similar to those in the Budapest Convention, including illegal access, interference with data or systems, computer-related fraud, and offences involving child sexual abuse material, together with the non-consensual dissemination of intimate images, reflecting harms that have grown significantly since 2001.
- A framework for the collection, preservation and cross-border sharing of electronic evidence applicable not only to cyber-dependent offences but to serious crime generally, addressing the evidentiary problem identified in Part II on a scale the Budapest Convention did not attempt.
- A 24/7 network of national points of contact for urgent cooperation, modelled on but intended to be broader in membership than the equivalent Budapest Convention mechanism.
- Dedicated provisions on technical assistance and capacity-building for developing countries, reflecting the concern of many negotiating States that an effective cybercrime regime cannot rest solely on the resources of already well-equipped States.

Ratification Status and Emerging Criticism: The Convention enters into force ninety days after the fortieth instrument of ratification is deposited. Progress toward that threshold has, to date, been slow: the European Union and its member States authorised signature in October 2025, and States including Canada signed the Convention in mid-2026, yet by July 2026 only

¹¹ G.A. Res. 79/243, U.N. Convention against Cybercrime (Dec. 24, 2024).

¹² Apostolos Georgiadis, 72 States Sign First Global UN Convention against Cybercrime, Help Net Security (Oct. 27, 2025), <https://www.helpnetsecurity.com/2025/10/27/un-convention-against-cybercrime/>

three States had actually completed ratification.¹³ India has not signed the Convention as of the date of this paper, although the Supreme Court of India has, in the course of proceedings concerning online financial fraud, directed the Union Government to take a considered decision on whether to ratify.¹⁴

The slow pace of ratification is not solely bureaucratic. Civil society organisations raised concerns during negotiation that the Convention's broad cross-border evidence-sharing powers, if not matched by robust human rights safeguards in every Party's domestic law, could be used by some States to compel assistance in investigations that are, in substance, directed at political dissidents, journalists or human rights defenders rather than at genuine cybercrime. This tension between the Convention's core purpose, which is to make cooperation faster and less discretionary, and its critics' fear that faster, less discretionary cooperation is precisely what enables abuse, is likely to shape how States implement and, in some cases, whether they ratify the Convention at all.¹⁵

REGIONAL AND SECTORAL INSTRUMENTS

Alongside the two global-facing instruments discussed above, a number of regional and sectoral frameworks contribute to the broader architecture of cybercrime prevention, and are worth noting briefly for the different institutional models they represent.

The African Union's Malabo Convention, adopted in 2014, addresses cybercrime alongside personal data protection and electronic transactions in a single instrument, reflecting a deliberate choice to treat cybersecurity and data governance as connected rather than separate problems. It has, however, struggled to secure the fifteen ratifications required for entry into force, illustrating that regional political will does not automatically translate into treaty participation even where the underlying need is widely acknowledged.¹⁶

The Commonwealth Secretariat's Model Law on Computer and Computer Related Crime offers a different model entirely: rather than a binding treaty, it is a template statute that member

¹³ Global Affairs Canada, Canada Signs United Nations Convention against Cybercrime (July 16, 2026), <https://www.canada.ca/en/global-affairs/news/2026/07/canada-signs-united-nations-convention-against-cybercrime.html>

¹⁴ <https://www.thehindu.com/news/national/digital-arrest-scams-what-has-the-supreme-court-directed-to-protect-victims/article71332091.ece>.

¹⁵ United Nations Convention Against Cybercrime, Vajiram & Ravi, <https://vajiramandravi.com/current-affairs/united-nations-convention-against-cybercrime/> (last visited Sept. 24, 2026).

¹⁶ African Union Convention on Cyber Security and Personal Data Protection, adopted June 27, 2014, opened for signature at Malabo, Equatorial Guinea.

States may adopt or adapt into domestic legislation, easing the definitional harmonisation problem without requiring any State to accept binding international obligations.¹⁷ Within the European Union, the NIS 2 Directive takes yet another approach, focusing less on criminalisation and more on mandatory cybersecurity risk-management and incident-reporting obligations for critical infrastructure operators, reflecting a preventive strategy centred on resilience rather than prosecution.¹⁸

Taken together, these instruments show that there is no single accepted model for international cybercrime prevention. States have variously pursued binding regional treaties, a binding global treaty, non-binding model legislation, and sector-specific resilience regulation, often simultaneously. This diversity has produced useful experimentation, but it has also produced the fragmentation that Part VII below argues is the framework's central weakness.

INTERNATIONAL COOPERATION: EXTRADITION, MUTUAL LEGAL ASSISTANCE AND EVIDENCE SHARING

Whatever substantive offences a treaty defines, prevention in practice depends on the speed of the cooperation mechanisms behind it. The traditional tool for cross-border evidence gathering, the mutual legal assistance treaty, built on the United Nations Model Treaty on Mutual Assistance in Criminal Matters, typically operates through formal diplomatic or central-authority channels that were designed for a world of paper records, not perishable digital evidence.¹⁹ A request that takes months to process is of limited use against evidence that a service provider may routinely delete within weeks. This mismatch between the pace of traditional mutual legal assistance and the volatility of digital evidence is precisely the gap that the expedited preservation mechanisms in both the Budapest Convention and the new UN Convention are designed to close, and it is arguably the single most consequential innovation either instrument offers.

Extradition presents a related but distinct difficulty. Most extradition treaties require dual criminality, meaning that the conduct alleged must be an offence in both the requesting and the requested State. Where domestic cybercrime legislation has not kept pace with the treaty's substantive definitions, or where a State has simply chosen not to criminalise a particular form

¹⁷ Commonwealth Secretariat, Commonwealth Model Law on Computer and Computer Related Crime (2002, rev. 2017).

¹⁸ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive), 2022 O.J. (L 333) 80.

¹⁹ UN Model Treaty on Mutual Assistance in Criminal Matters, G.A. Res. 45/117, annex (Dec. 14, 1990).

of conduct, extradition can fail even where the treaty framework otherwise applies, which is a further argument for the definitional harmonisation that both the Budapest Convention and the UN Convention attempt to achieve.

INDIA'S POSITION: DOMESTIC LAW AND INTERNATIONAL ENGAGEMENT

India's principal domestic legislation, the Information Technology Act, 2000, criminalises a range of conduct including unauthorised access, data theft, the introduction of computer viruses, cyber terrorism and identity theft, and has been amended over the years to address emerging harms. Its national computer emergency response function, CERT-In, coordinates incident response and issues binding directions on cybersecurity practices to regulated entities.²⁰

Despite this reasonably developed domestic framework, India remains outside the Budapest Convention and has not yet signed the UN Convention against Cybercrime. India's stated reason for declining the Budapest Convention, that it was excluded from the drafting process, carries real institutional weight, but it leaves India dependent on a patchwork of bilateral mutual legal assistance treaties for cross-border cooperation, each negotiated separately, rather than the standardised, faster channels available to Parties of a multilateral instrument. The UN Convention, having been negotiated through a UN Ad Hoc Committee in which India participated as of right, does not carry the same objection, and, notably, the Supreme Court of India has itself pressed the Union Government to take a considered position on ratification in the context of the rising volume of cyber-enabled financial fraud reaching Indian courts.

Whether India ultimately ratifies the UN Convention will depend on a familiar balance: the practical benefit of faster, more predictable cooperation against the sovereignty and privacy concerns that similarly animate the human rights critique discussed in Part V above. Given the current scale of the threat facing Indian citizens and institutions, however, continued non-participation in both major instruments risks leaving India reliant on cooperation channels that are slower than those available to States that have joined.

²⁰ Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, framed under Section 70B of the Information Technology Act, 2000.

CRITICAL ANALYSIS: GAPS AND COUNTERARGUMENTS

Three structural weaknesses in the present framework deserve emphasis, alongside the counterarguments each has attracted.

First, fragmentation. The coexistence of the Budapest Convention, the new UN Convention, and various regional instruments means that no single treaty commands universal membership, and a request for cooperation between two States that are not both Parties to the same instrument still falls back on slower, ad hoc bilateral arrangements. The counterargument is that this diversity reflects genuine and legitimate differences in regional legal traditions and political circumstances, and that a single universal instrument negotiated by consensus, such as the new UN Convention aspires to be, was itself only achievable because States could point to years of prior experimentation, including under the Budapest Convention, as a template to build on.

Second, the tension between speed of cooperation and human rights protection. The evidence-sharing mechanisms that make these treaties effective for prevention are the same mechanisms that critics fear could be misused for surveillance. The counterargument, advanced by the Convention's proponents, is that the UN Convention includes express grounds for a requested State to refuse cooperation where a request is politically motivated or inconsistent with human rights obligations, and that the alternative, namely no binding framework at all, leaves victims of genuine cybercrime with even less protection while doing nothing to prevent the abuses critics fear.

Third, the attribution and enforcement gap. Even where the applicable law is clear, and cooperation channels function well, identifying the true perpetrator of a sophisticated cyber-operation, particularly one plausibly linked to a State or a State-tolerated non-state actor, remains technically difficult, and no cybercrime treaty currently in force provides a binding mechanism for resolving contested attribution. The honest response to this gap is that it may be unrealistic to expect any criminal-law instrument to solve what is, in substance, a problem of international security law and evidence, and that this task is more appropriately left to the separate, evolving body of practice around State responsibility for cyber operations discussed in Part III.

CONCLUSION

The international legal framework for the prevention of cybercrime has moved, within a little over two decades, from a single regional treaty of uncertain global reach to a layered structure encompassing that treaty, a newly adopted universal convention, and an array of regional and sectoral instruments alongside it. This represents genuine progress: the substantive offences that States are expected to criminalise have become broadly standardised, and the procedural tools available for urgent cross-border evidence preservation are considerably faster than the mutual legal assistance channels they supplement. Prevention, however, remains only as strong as the weakest link in this cooperative chain, and that chain currently has real gaps: major States, India among them, sit outside both principal instruments; the new UN Convention has, as of mid-2026, secured only a small fraction of the ratifications needed to enter into force; and unresolved questions about attribution and the risk of misuse for surveillance mean that the framework's next phase of development is likely to be as much about building trust and safeguards as about drafting further substantive rules.

No treaty framework, however carefully drafted, can by itself eliminate a threat as adaptive as cybercrime. What the framework can do, and what its next stage of evolution should prioritise, is narrow the gap between the speed at which cybercrime crosses borders and the speed at which the law is able to follow it. Universal ratification of the UN Convention, accompanied by credible human rights safeguards in its implementation, along with India's participation in at least one of the two major instruments, would represent the most concrete steps available toward that goal in the near term.