*Page 1160 - 1175*

**INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES**

**[ISSN 2581-5369]**

**Volume 9 | Issue 3**

**2026**

# Cyber-Terrorism and the Changing Definition of Terrorism Prospects for India in International Law

SUNNY DIWAKER*

## ABSTRACT

*The digital revolution has expanded the frontiers of terrorism beyond physical violence into cyberspace. Cyber-terrorism—manifested through large-scale cyber-attacks, online radicalization, and digital sabotage—poses unique challenges to the existing definition of terrorism under international law. Despite several UN Security Council resolutions and sectoral conventions, international law still lacks a uniform and comprehensive definition that accommodates these emerging threats. This paper critically examines the inadequacy of traditional legal definitions of terrorism in addressing cyber operations by non-state actors. It explores whether existing frameworks, such as the Budapest Convention on Cybercrime and the UN Global Counter-Terrorism Strategy, effectively encompass the complex dimensions of cyber-terrorism. Focusing on India's role, the paper analyses how domestic laws the Unlawful Activities (Prevention) Act, 1967 and the Information Technology Act, 2000 can be harmonized with evolving international norms. It further evaluates India's participation in global counter-terrorism initiatives and its potential leadership in advancing a more inclusive international definition of terrorism that recognizes cyber dimensions. Adopting a doctrinal and comparative methodology, the study highlights the need for India to strengthen its legal preparedness while engaging proactively in international law-making processes. It concludes that India can play a pivotal role in shaping a balanced and forward-looking global framework against cyber-terrorism within the contemporary international legal order.*

***Keywords:*** *Cyber-terrorism, International Law, India, Global Security, UN Framework*

## I. INTRODUCTION

Terrorism has been transformed in the twenty first century. Traditional terrorism was characterized by direct incidences of violence, bombing, hostage taker, and assassination that were conducted in specific locations and to specific targets. In the modern world, a coordinated strike on the power grid, banking system or defence communications system of a country can

* Author has Pursued Law from University of Allahabad, Prayagraj, Uttar Pradesh, India.

 [ISSN 2581-5369]

have effects comparable or greater than a traditional terrorist strike, but can be caused anywhere on the planet by an unknown party. It is one of the greatest challenges to international law today as this physical violence has been changed into digital violence.[1]

India is in the centre of this emerging threat environment. India, which is the largest democracy in the world and one of the fastest digitising economies, has a population of about 918 million internet users as of late in 2024.[2] Attacks on critical industries, such as banking and government, increased more than twice in just two years.[3] The issue, though, is more than just technological in nature. The current international systems of countering terrorism were made in a time when terrorism implied physical violence and not cross-border intrusions into computer systems and the systematic radicalisation of youth over the internet.

The most urgent legal issue is the one of definition. There is no single definition of terrorism and it is accepted internationally at present. Firstly, the Comprehensive Convention on International Terrorism (CCIT), which was initially introduced by India at the United Nations General Assembly in 1996,[4] has not been completed almost three decades later. Without such a definition, cyber-terrorism, that is, the integration of technology in cybercrime with the ideology of terrorism, is in a very dangerous grey area of legal jurisdiction. Unless it can be defined accurately, it cannot be consistently prosecuted, and cannot be used as a foundation of consistent international cooperation.[5]

The paper, critically examines the question of whether the current international legal arrangements suffice to combat cyber-terrorism, evaluates the domestic legal effort by India in the UAPA and the IT Act and it is argued that India, as the first proposer of the CCIT and as a key digital economy, is best laid out to be the first to take the lead in ensuring the development of a comprehensive legal definition of terrorism that encompasses the cyber aspects. The paper has a doctrinal and comparative methodology, which is based on primary legal materials such

[1] Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 1–15 (2d ed. Cambridge University Press 2017); Thomas Rid, Cyber War Will Not Take Place, 35 J. Strategic Stud. 5 (2012); Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* ch. 1 (HarperCollins 2010).

[2] Telecom Regulatory Authority of India, *Telecom Subscription Data as of 31 October 2024* (2025); Press Information Bureau, Gov't of India, Curbing Cyber Frauds in Digital India (2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146 (last visited Feb. 16, 2026) (reporting 918.19 million internet users and over 86% household internet connectivity).

[3] Press Information Bureau, Gov't of India, *supra* note 2 (reporting cybersecurity incidents rising from 10.29 lakh in 2022 to 22.68 lakh in 2024); The Rising Tide: Understanding the Surge in Cyber Attacks in India, Tripwire (2024), https://www.tripwire.com/state-of-security/rising-tide-understanding-surge-cyber-attacks-india (last visited Feb. 16, 2026).

[4] G.A. Res. 51/210, Measures to Eliminate International Terrorism (Dec. 17, 1996); India, Draft Comprehensive Convention on International Terrorism, U.N. Doc. A/C.6/55/1 (Aug. 28, 2000).

[5] Ben Saul, *Defining Terrorism in International Law* 1–5 (Oxford University Press 2006); United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* 1–3 (2012).

 [ISSN 2581-5369]

as international treaties, resolutions of the UN Security Council, and domestic law, and is supported by academic literature.[6]

## II. TERRORISM AND THE PROBLEM OF DEFINITION

One of the most ancient issues of the international criminal law is the difficulty of defining the concept of terrorism in law. Since the 1920s,[7] Professor Ben Saul has noted that the international community has failed many times to establish terrorism into a category of law despite the almost unanimous denouncing of terrorism by international actors. The most significant challenge is more political than technical: states do not agree on the essentials of what actors and what actions they should be considered in any definition. This tension is reflected by the cliche that one man terrorist is another man freedom fighter. Historically, states that had gone through the colonial rule were unwilling to embrace definitions that would criminalise national liberation movements; others demanded that state-sponsored violence should be added. Such differences have meant that a global definition is yet to be reached in a century.

Without a comprehensive definition of treaties, the international law has been dependent on a piece meal approach. Thirteen sectoral conventions have been closed since the 1960s and each has an objective of a particular type of terrorist act. These are the Hague Convention of Suppression of Unlawful seizure of aircrafts of 1970,[8] the International Convention against the taking of Hostages of 1979 and the international convention on the financing of terrorism of 1999.[9] All these tools criminalise certain behaviour but do not state terrorism as an overall law. Not one of them was created to deal with acts executed through the use of computers or the internet.[10]

### A. U.N. attempts to define terrorism

The attacks of September 11, 2001 led to the most notable change in the international counter-terrorism law since the sectoral conventions. In Chapter VII of the UN Charter,[11] under an unanimously adopted resolution of the UN Security Council, Resolution 137312, on 28 September 2001, all member states were obliged under the binding force of the resolution to

[6] **See generally** Malcolm N. Shaw, *International Law* ch. 1 (9th ed. Cambridge University Press 2021); Ian Brownlie, *Principles of Public International Law* 1–15 (7th ed. Oxford University Press 2008).
[7] Ben Saul, *supra* note 5, at 1.
[8] Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 860 U.N.T.S. 105 (entered into force Oct. 14, 1971).
[9] International Convention Against the Taking of Hostages, Dec. 17, 1979, 1316 U.N.T.S. 205 (entered into force June 3, 1983).
[10] International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, 2178 U.N.T.S. 197 (entered into force Apr. 10, 2002).
[11] S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

 [ISSN 2581-5369]

criminalise terrorist financing, freeze terrorist assets, prevent the movement of terrorists across borders, and enhance mutual legal assistance. Resolution 1373 is legally binding on all the 193 member states of the United Nations because it was adopted under Chapter VII and by Article 25 of the UN Charter.[12]

However, Resolution 1373 failed to provide definition of terrorism. This was an intentional oversight - states were unable to reach a definition and settled on the expedient, and they decided to place commitments lacking any definition, and left it to each state to decide what it would classify as terrorism under its internal jurisdiction. The outcome was a mosaic of incoherent national definitions which seriously threatened the coherence of the international counter-terrorism regime. A subsequent definition, UNSC Resolution 1566 of 2004,[13] provided a more practical definition of the term terrorism: acts of crime aimed at inflicting fatalities, or grievous bodily harm, or hostages, to frighten a population or induce a government to take action. This was a political pronouncement though useful as a working rule, and made no mention of cyber means of commission.

The multilateral political framework on counter-terrorism is the most broad and comprehensive, which is the UN General Assembly Global Counter-Terrorism Strategy, adopted under Resolution 60/288 in 2006 and reviewed biennially.[14] It works on four pillars, which are dealing with conditions favoring terrorism, preventing and countering terrorism, building state capacity as well as ensuring human rights. The Strategy has been revised over the years to include the cyber aspect especially concerning the use of the internet as a means of radicalisation, recruitment, and propagation of terrorism.

The major weakness of the Strategy as a tool of fighting cyber-terrorism is its non-binding nature. It imposes no lawful duties on states, sets no crimes, and provides no apparatuses of enforcement. It is mostly useful as a framework of political value and capacity-building. Making it legally binding would not allow it to replace a binding treaty definition of cyber-terrorism.

The only multilateral treaty that is specifically put up to deal with cybercrime is the Budapest Convention on Cybercrime of 2001.[15] It demands the states to criminalize crimes against the confidentiality, integrity and availability of computer systems and data, computer-related fraud

[12] U.N. Charter art. 25; Brownlie, supra note 6, at 698–701.
[13] S.C. Res. 1566, ¶ 3, U.N. Doc. S/RES/1566 (Oct. 8, 2004).
[14] G.A. Res. 60/288, The United Nations Global Counter-Terrorism Strategy, U.N. Doc. A/RES/60/288 (Sept. 8, 2006).
[15] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (entered into force July 1, 2004).

 [ISSN 2581-5369]

and forgery, content related crimes and copyright violations. It also sets procedures on real-time collection of computer information and mutual legal aid between parties of the states.

Nevertheless, the Budapest convention has three major constraints regarding the coverage of cyber-terrorism. First, it is silent on or defines cyber-terrorism as a specific type of offence, it is concerned with the idea of cybercrime in the traditional meaning of the term, that is, without any point to political motive or terrorist purpose. Secondly, it has a limited geographic coverage in the past. Despite the fact that the Convention was open to non-Council of Europe states, only a fairly small number of the global states are parties.[16] Thirdly, and most apparent in the context of India, the provisions of the Convention that invite transborder access to stored data, in particular Article 32, brings about serious concerns about state sovereignty that India has always pointed out as a factor against accession to the Convention.[17]

The failure of India to comply with the Budapest Convention is also a major loophole in their international involvement in cyber law. The extraterritorial issues that India has raised are in part partially resolved by the 2021 Second Additional Protocol to the Budapest Convention that reinforces international cooperation in obtaining electronic evidence.[18] India must give a serious rethink upon its stance or take an active part in coming up with an alternative multilateral instrument that combats both cybercrime and cyber-terrorism by applying the relevant sovereignty.

### B. Regional organizations and definitions of terrorism

Regional organisations have tried to be more specific in definition. According to the Directive 2017/541/EU on combating terrorism by the European Union terrorist offences are acts which in the nature or circumstances of their commission may cause severe harm to a country or international organisation when used with the purpose of severely intimidating a population, coercing a government unduly or severely destabilising fundamental structures.[19] Notably, the Article 3(1)(i) of this Directive contains the attacks on information systems in the list of terrorist offences, which is why it is one of very few international instruments that denotes the cyber aspect of terrorism.

---

[16] Council of Europe, Chart of Signatures and Ratifications of Treaty 185, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (last visited Feb. 16, 2026).

[17] Convention on Cybercrime, supra note 23, art. 32; Government of India, Ministry of Home Affairs, Note on Budapest Convention (2017) (on record in Rajya Sabha Question No. 1518, Aug. 2, 2017).

[18] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, May 12, 2022, E.T.S. No. 224.

[19] Directive (EU) 2017/541 of the European Parliament and of the Council of Mar. 15, 2017 on Combating Terrorism, 2017 O.J. (L 88) 6, art. 3.

 [ISSN 2581-5369]

The Convention on Combatting Terrorism of Shanghai Cooperation Organisation of 2009 is of particular interest to India since, becoming a full party,[20] India joined the SCO as a full member in 2017. It is remarkable that the SCO Convention has incorporated in its operative text information terrorism, i.e. the terrorist use of information technologies and communication technologies, as one of its provisions. The involvement of India in SCO already links it to an international tool that partially deals with cyber-terrorism but the provisions of SCO Convention do not go as far as they need to be specific in order to have a solid enforcement tool.

## III. CYBER-TERRORISM: CONCEPT AND FEATURES

### A. Defining Cyber-Terrorism

The term "cyber-terrorism" was coined by *Barry Collin* of the Institute for Security and Intelligence in the 1980s to describe the convergence of cyberspace and terrorism.[21] The most widely cited and legally precise definition remains that of *Professor Dorothy Denning*, who defined cyber terrorism as: "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives... [Causing] enough harm to generate fear."[22]

To be used in legal terms, the definition of cyber-terrorism should encompass three separate components. **First, an act element:** an assault upon or via computer systems, computer networks, or computer infrastructure. **Second, an effect element:** the attack has to result in or have a high probability of resulting in severe damage - either physical damage, interruption of essential services, or massive economic loss. **Third**, **an intent element:** the attack should be executed with a view to terrorise a population, blackmail a government or disrupt the basic government structures towards political, ideological or some other objective.[23] All the three should be present so that an act should be considered as a cyber-terrorism but not a cybercrime or hacktivism.

[20] Convention of the Shanghai Cooperation Organisation against Terrorism, June 16, 2009 (entered into force Jan. 1, 2012), https://eng.sectsco.org/documents/ (last visited Feb. 16, 2026).
[21] Barry Collin, The Future of Cyberterrorism (paper presented at the 11th Annual International Symposium on Criminal Justice Issues, Univ. of Ill. at Chi., 1996); Gabriel Weimann, Cyberterrorism: How Real Is the Threat?, U.S. Inst. of Peace, Spec. Rep. No. 119, at 2 (2004).
[22] Dorothy E. Denning, Cyberterrorism (testimony before the Special Oversight Panel on Terrorism, H. Comm. on Armed Servs., 106th Cong. (May 23, 2000)), https://irp.fas.org/congress/2000_hr/00-05-23denning.htm (last visited Feb. 16, 2026); Dorothy E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, in *Networks and Netwars: The Future of Terror*, *Crime and Militancy* 239, 241 (John Arquilla & David Ronfeldt eds., RAND Corp. 2001).
[23] Weimann, supra note 16, at 3–5; see also Lee Jarvis & Stuart Macdonald, What Is Cyberterrorism? Findings from a Survey of Researchers, 27(4) Terrorism & Pol. Violence 657, 663 (2015).

 [ISSN 2581-5369]

Cyber-terrorism has to be differentiated with three related concepts that are closely related but have different legal definitions. **Cybercrime** is a type of crime that is perpetrated with the aid of digital technology, fraud, hacking, identity theft, etc. and is not ideologically or politically driven. The concept of cyber war denotes the state-supported **cyber warfare** activities carried out to either provide military or interstate combat in accordance with the law of armed conflict and Tallinn Manual 2.0.[24] **The use of internet by terrorists** can be described as an exploitation of the internet to recruit, propagate, fund, and plan operations which are not necessarily direct cyber-attacks on infrastructure, though these are similar.[25]

Cybercrime and cyber-terrorism are differentiated not only by the nature of the act but also by intent and purpose. The distributed denial-of-service attack that amounts to cyber-crime committed in pursuit of financial extortion is cyber-terrorism in pursuit of limited governmental emergency service paralysis due to the aim of creating terror in the community. The legal implications of this observation are as follows: the boundary between what is and what is not a terrorist act should be adjusted closely to prevent over-criminalisation of an ordinary cyber-attack, on the one hand, and to capture acts of a terrorist character, on the other hand.

The majority of legal frameworks and policy documents meet at the notion of the critical infrastructure as the differentiating line on cyber-terrorism. Once an attack becomes critical enough to affect systems the crippling of which would cause far-reaching effects on the lives of the population, the safety of a nation, or the financial viability of a state, the attack can be defined as cyber-terrorism. The UN Security Council Resolution 2341 of 2017 explicitly requested the states to defend against a terrorist attack on critical infrastructure,[26] including cyber attacks and urged states to exchange information and establish national policies in order to deter terrorist attacks. The Indian own system of protection against critical information infrastructures is provided by Section 70 of the IT Act that creates the so-called protected systems, but the statutory framework for their protection against a cyber-terrorist attack remains underdeveloped.[27]

[24] Schmitt, supra note 1, at Rules 4–7, 14–17; see also Jack Goldsmith & Tim Wu, *Who Controls the Internet?* 179 (Oxford Univ. Press 2006).
[25] U.N. Office on Drugs & Crime, supra note 5, ch. 2; S.C. Res. 2396, ¶¶ 17–19, U.N. Doc. S/RES/2396 (Dec. 21, 2017).
[26] S.C. Res. 2341, U.N. Doc. S/RES/2341 (Feb. 13, 2017).
[27] Information Technology Act, No. 21 of 2000, § 70 (India) (as amended by the Information Technology (Amendment) Act, 2008); Nat'l Critical Info. Infrastructure Prot. Ctr., Guidelines for Protection of Critical Information Infrastructure (2015).

 [ISSN 2581-5369]

## IV. LEGAL INSTRUMENTS AND CYBER TERRORISM

The only multilateral treaty that is specifically put up to deal with cybercrime is the Budapest Convention on Cybercrime of 2001.[28] It demands the states to criminalize crimes against the confidentiality, integrity and availability of computer systems and data, computer-related fraud and forgery, content related crimes and copyright violations. It also sets procedures on real-time collection of computer information and mutual legal aid between parties of the states.

Nevertheless, the Budapest convention has three major constraints regarding the coverage of cyber-terrorism. First, it is silent on or defines cyber-terrorism as a specific type of offence, it is concerned with the idea of cybercrime in the traditional meaning of the term, that is, without any point to political motive or terrorist purpose. Secondly, it has a limited geographic coverage in the past. Despite the fact that the Convention was open to non-Council of Europe states, only a fairly small number of the global states are parties.[29] Thirdly, and most apparent in the context of India, the provisions of the Convention that invite transborder access to stored data, in particular Article 32, brings about serious concerns about state sovereignty that India has always pointed out as a factor against accession to the Convention.[30]

The failure of India to comply with the Budapest Convention is also a major loophole in their international involvement in cyber law. The extraterritorial issues that India has raised are in part partially resolved by the 2021 Second Additional Protocol to the Budapest Convention that reinforces international cooperation in obtaining electronic evidence.[31] India must give a serious rethink upon its stance or take an active part in coming up with an alternative multilateral instrument that combats both cybercrime and cyber-terrorism by applying the relevant sovereignty.

### A. Structural Gaps in the International Framework

At the first glance, a critical examination of the existing international tools will demonstrate that there are at least four structural gaps in the legal regime of cyber-terrorism. **First**, terrorism and cyber-terrorism have no binding definition within the international law, which generates uneven responses among countries and hinders cooperation. **Second**, the legal and technical

[28] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (entered into force July 1, 2004).
[29] Council of Europe, Chart of Signatures and Ratifications of Treaty 185, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (last visited Feb. 16, 2026).
[30] Convention on Cybercrime, supra note 23, art. 32; Government of India, Ministry of Home Affairs, Note on Budapest Convention (2017) (on record in Rajya Sabha Question No. 1518, Aug. 2, 2017).
[31] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, May 12, 2022, E.T.S. No. 224.

 [ISSN 2581-5369]

challenge of attributing cyber-attacks to particular non-state actors, which is a necessary condition to prosecute, is unclear; international law has not established clear guidelines on how to hold states accountable in cases where they cannot control the use of their territory to carry out terrorist cyber-attacks.[32] **Third**, there is a jurisdictional complication in cyber-terrorism cases: attacks regularly cross borders in several countries, yet current mutual legal assistance treaties are slow and inefficient with investigations of cyber-attacks as they happen. **Fourth**, technology always keeps ahead of the law new threats based on artificial intelligence, autonomous systems, and quantum computing do not fit within any current system.

## V. INDIA'S DOMESTIC LEGAL FRAMEWORK FOR CYBER-TERRORISM

The core anti-terrorism law in India is the Unlawful Activities (Prevention) Act, 1967 (UAPA) that was radically reformed by the UAPA (Amendment) Act, 2008, and has been revisited in 2013 and 2019. Section 15 of UAPA defines a terrorism act as an act committed with intent to cause threat to unity, integrity, security, economic security, or sovereignty of India, or with intent to cause terror to people, done by specified means i.e. by firearms, explosives, and most importantly by any other means of whatever nature.[33]

Such residual provision as "by any other means of whatever nature" gives the hypothetical potential of classifying cyber-terrorist actions as a terrorist act under the UAPA, despite the lack of a specific provision. Nonetheless, such interpretation is yet to be firmly stipulated by the decision of a court. In *Asif Iqbal Tanha v State (NCT of Delhi)*,[34] the Delhi High Court, which allowed the bail on the condition, stated that Section 15 was of a broader and possibly unrestrictive nature and could only be used in pertaining to matters of such seriousness in the security of the country. This vagueness poses the danger of both under-enforcement (when actual cyber-terrorists avoid the UAPA) and over-enforcement (where the act is used to cover a lawful political act on the internet).

The procedures set forth by the UAPA are much harsher than standard criminal procedure: Section 43D of the UAPA permits up to 180 days of pre-trial detention without a charge sheet; the conditions of bail are more limiting; and the National Investigation Agency incurs an exclusive federal role in investigating offenses committed under the UAPA under the NIA Act

[32] Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, 125 Yale L.J. Forum 68 (2015); Articles on Responsibility of States for Internationally Wrongful Acts, art. 8, U.N. Doc. A/56/10 (2001).
[33] Unlawful Activities (Prevention) Act, No. 37 of 1967, § 15 (India) (as substituted by the Unlawful Activities (Prevention) Amendment Act, 2008 and amended by the Unlawful Activities (Prevention) Amendment Act, 2019).
[34] Asif Iqbal Tanha v. State (NCT of Delhi), 2021 SCC OnLine Del 3299 (Del. H.C.) (Sidharth Mridul & Anup Jairam Bhambhani, JJ.).

 [ISSN 2581-5369]

2008.[35] The lack of an express cyber-terrorism clause in the UAPA is not just a matter of definition, however, but has a direct impact on prosecution strategy, bailing, evidentiary standards and jurisdiction over investigation.

Another Section 66F of the Information Technology Act, 2000, inserted by the IT (Amendment) Act, 2008 and brought into force on 27 October 2009, is India's most direct statutory response to cyber-terrorism. It provides:[36]

"Whoever (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by — (i) denying or cause the denial of access to any person authorised to access computer resource; (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access... and (B) by knowingly or intentionally penetrating or accessing a computer resource... causes or is likely to cause death or injuries to persons or damage to or destruction of property... commits the offence of cyber terrorism." Punishment prescribed is imprisonment for life.

Section 66F is a significant initial move. Its definition encompasses the key components of cyber-terrorism namely the unauthorised access, infrastructure destruction, and terrorist purposes targeting national security or popular terror. Nevertheless, there are a number of limitations evident. The clause is silent on the use of internet to recruit, radicalize or even propagate, which are mentioned in UNSC Resolutions 2341 and 2396 as a main element of the cyber-terrorism threat. Nor does it discuss how terrorism is financed by use of digital resources, such as cryptocurrency. In addition, like in the case with UAPA, there is no clear mechanism to resolve the overlap of Section 66F and Section 15 UAPA, resulting in a prosecutorial choice-of-law issue that carries huge procedural implications.[37]

A number of other tools fill in the India domestic cyber-terrorist landscape. Section 69 of the IT Act provides the government with the authority to intercept,[38] monitor and decrypt information on the name of national security - a vital anti-terrorism surveillance device. The blocking of internet content in the public interest under section 69A is widely used to block terrorist propaganda and recruiting material. The National Cyber Security Policy 2013 formulates a strategic way of ensuring that the cyberspace is not threatened yet it is not legally

[35] National Investigation Agency Act, No. 34 of 2008, § 3 (India); Unlawful Activities (Prevention) Act, No. 37 of 1967, § 43D (India).
[36] Information Technology Act, No. 21 of 2000, § 66F (India) (as inserted by the Information Technology (Amendment) Act, 2008, No. 10 of 2009, § 32 (effective Oct. 27, 2009)).
[37] Pavan Duggal, *Cyber Law: The Indian Perspective* 312–318 (4th ed. Saakshar Law Publ'ns 2019); Karnika Seth, *Computers, Internet and New Technology Laws* ch. 9 (LexisNexis 2016).
[38] Information Technology Act, No. 21 of 2000, § 69 (India).

 [ISSN 2581-5369]

binding.[39] Based on the EU example of the Terrorist Content Online Regulation, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 puts considerable compliance burdens on the social media regarding the deletion of terrorist content,[40] which places India in a common direction with the EU.

## VI. CRITICAL ASSESSMENT: GAPS IN THE DOMESTIC FRAMEWORK

The domestic system of India, though having the relevant provisions in the UAPA and the IT Act, has four major weaknesses. **First**, the lack of a specific provision on cyber-terrorism in the UAPA provides interpretive ambiguity on the gravest instances. **Second**, India does not have a specific Critical Infrastructure Cyber Protection Act to the one that the US has the Critical Infrastructure Protection program or the EU the NIS2 Directive, so the designation and protection of critical information infrastructure is still done fragmentarily by Section 70 IT Act. **Third**, the Federal coordination between the CERT-In, the NCIIPC, the NIA and the state police is governed through administrative structures and not a definite statutory outline. **Fourth**, the system of mutual legal assistance in India is ill-adjusted to the pace and technical challenges of cyber-terrorism investigations, where the electronic evidence should be stored and retrieved in real-time.[41]

Previously, the Indian Penal Code (IPC) did not have any specific provision related to terrorism. The matter of terrorism was covered by means of special laws like the Unlawful Activities (Prevention) Act (UAPA). Nevertheless, since the introduction of the Bharatiya Nyaya Sanhita, the problem of terrorism is mentioned explicitly for the first time in the context of the general criminal law of India. This example demonstrates the constant development of the Indian legal system with respect to tackling new kinds of crimes and threats to national security. It should be noted that despite this step forward, there are no specific provisions concerning cyber terrorism as an independent crime under the BNS. In the era of digital attacks which can endanger national security, financial system and even physical structures of society, there appears to be a necessity to incorporate the problem of cyber terrorism into Indian criminal law.[42]

---

[39] Ministry of Communications & Information Technology (India), National Cyber Security Policy 2013 (Gov't of India 2013).

[40] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under the Information Technology Act, No. 21 of 2000, §§ 87 r/w 79 (India).

[41] Nandan Kamath, *Law Relating to Computers*, *Internet and E-Commerce* 540–555 (8th ed. Universal Law Publ'g 2021); U.N. Office on Drugs & Crime, Mutual Legal Assistance Requests for Electronic Evidence: A Practitioner's Guide 14–18 (2019).

[42] Siddhant Sinha, "Was Section 113 of the Bharatiya Nyaya Sanhita, 2023 Regarding Terrorist Act Needed in the Presence of the UAPA, 1967?" *Legal Service India* (2024), available at: [Legal Service India](https://www.legalserviceindia.com/legal/legal/article-17535-was-section-113-of-the-bharatiya-nyaya-

## VII. INDIA'S ROLE IN THE INTERNATIONAL COUNTER-TERRORISM ARCHITECTURE

The decades of first-hand experience with terrorism in its different manifestations inform the way India perceives the international counter-terrorism law. The Comprehensive Convention on International Terrorism (CCIT) was originally offered by India at the UN General Assembly in 1996 as a draft convention, which attempts to criminalise terrorism internationally with no exception given to the so-called political legitimacy of the cause.[43] The fundamental stance of India, that terrorist acts should not be criminalised with exceptions based on the motive or the target, squarely differs with the historical differences that have led to the lack of consensus over CCIT. India has lamented especially that the definition that has been advanced by UNSC Resolution 1566 (2004) may likewise make a fruitful point of contact in furthering the negotiations.

By October 2025, India still laments that the CCIT is yet to be concluded. India made this observation in a statement to the UN Sixth Committee that said that narrow geopolitical interests have remained the barrier to making meaningful progress.[44] The fact India is the original proposer of the CCIT means it has the standing and the burden to spearhead the attempt to resurrect such negotiations that may have cyber-terrorism provisions in a revised version.

In addition to the CCIT, India is actively a member of various multilateral counter-terrorism systems that are applicable to cyber-terrorism. India joined in full membership of the Financial Action Taskforce (FATF), 2010,[45] and is involved in the FATF activities on terrorist financing via digital mediums such as cryptocurrency, which is becoming an increasing source of financing cyber terrorism. In India when it hosted the 2023 G20 Presidency, the internet as a source of terrorist activities was discussed in the Counter-Terrorism Working Group, and a consensus declaration was made representing the no-tolerance policy towards terrorist content online.[46]

---

sanhita-2023-regarding-terrorist-act-needed-in-the-presence-of-the-uapa-1967-.html?utm) (last visited on May 18, 2026).

[43] India, supra note 4; Permanent Mission of India to the United Nations, Statement to the Sixth Committee on Measures to Eliminate International Terrorism (72d Sess., Oct. 3, 2017), https://pminewyork.gov.in/IndiaatUNGA?id=MzU5Mg (last visited Feb. 16, 2026).

[44] Wikipedia, Comprehensive Convention on International Terrorism (last updated Dec. 2025), https://en.wikipedia.org/wiki/Comprehensive_Convention_on_International_Terrorism (last visited Feb. 16, 2026).

[45] Financial Action Task Force, *India: Mutual Evaluation Report* (2010); Financial Action Task Force, Targeted Financial Sanctions Related to Terrorism and Terrorist Financing, Recommendation 6, in *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012, updated 2023).

[46] Convention of the Shanghai Cooperation Organisation against Terrorism, supra note 15, art. 1(1)(3); see also Nayef Al-Rodhan, The Five Dimensions of Cyberspace Threats, 3 J. Strategic Security 17 (2012).

 [ISSN 2581-5369]

India is a member of a mechanism of intelligence sharing and counter-terrorism coordination, through the SCO, the Regional Anti-Terrorist Structure (RATS), consisting of China, Russia, Pakistan as well as the Central Asian republics. The increasing emphasis of the SCO on their definition of information terrorism, which is a term in the SCO Convention designed to refer to the employment of information technologies in terrorist activity, provides India with a regional grid on which to promote the norms of cyber-terrorism in addition to its campaigning activity at the UN level. The fact that India is both a member of the G20 and the SCO places it in an excellent position to facilitate the views of both the West and non-West on cyber-terrorism law.

## VIII. SUGGESTIONS

The concept of harmonisation in international law is defined as the correlation of the domestic legal norms with the international legal requirements and standards. Harmonisation is also required in the context of counter-terrorism by UNSC Resolution 1373 which states that a state must criminalise in its local legislation acts of terrorism that are in accordance with its international obligations.[47] Article 27 of the Vienna Convention on the Law of Treaties makes this crystal clear because it provides that a state may not use the provisions of its national law as an excuse of failing to comply with an international obligation.[48] In the case of India, harmonisation needs to focus on not just making sure international counter-terrorism obligations existing under the domestic law are covered but also predicting and reflecting on the changing international consensus on cyber-terrorism.

### A. Recommended Domestic Legislative Reforms

There are three sections of legislation reforms that are suggested to cover the gaps highlighted under Section V. To begin with, the UAPA needs to be amended in order to make explicit reference to cyber means of commission, that is, attacks on computer systems, networks, and critical information infrastructure, being qualifying means to the definition of a "terrorist act". The current residual provision is not adequate; it needs to be specifically stated to provide legal inertia and confidence by the prosecutors.[49]

The IT Act, Section 66F needs to be extended to include: (i) the use of the internet to carry out radicalisation, recruitment, and facilitation of acts of terrorism, in line with the UNSC Resolutions 2341 and 2396; (ii) financing of acts of terrorism using digital tools, including

[47] S.C. Res. 1373, supra note 11, ¶ 2(e)–(f).
[48] Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, art. 27 (entered into force Jan. 27, 1980).
[49] Counter-Terrorism and Security Act 2015, c. 6, § 17 (U.K.); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, § 814 (U.S.); Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(5).

 [ISSN 2581-5369]

cryptocurrency and anonymous payment systems; and (iii) attacks on designated critical information infrastructure under Section 70 IT Act, and with heavier penalties.[50]

India needs to implement a specific Critical Infrastructure Cyber Protection Act which explicitly identifies what sectors should be the focus of protection, makes obligatory the reporting of cyber-incidents, brings about a statutory framework of the cooperation of the government and the private sector in the context of cyber-terrorism, and establishes a clear mechanism of inter-agency interdependence between CERT-In, the NCIIPC, and the NIA in the case of cyber-terrorist attack. This would take India to the best practice internationally in the form of EU NIS2 Directive and US CISA framework.

### B. Elements of a Proposed International Definition of Cyber-Terrorism

Based on the discussion in previous sections and state practice prevailing at the time, this paper puts forward the following components of a comprehensive international definition of terrorism that specifically includes the cyber aspect. A revised draft of CCIT might include such definition or may be adopted as an independent protocol to current instruments.

There should be five elements in the definition. An act element: any act, either physically or digitally, such as unauthorised access to, interference with, or damage to computer systems, networks or vital information infrastructure. An effect element: the cause, or is likely to cause, death or severe bodily injury on persons, material harm to property, violation of essential public services, or economic harm of a substantial nature. A purposeful aspect: a determined act with the purpose to threaten a population, blackmail a government, or disrupt basic constitutional, economic or social systems. Ideological qualifier: where the act is driven by political, religious, ideological or other such objectives, which differentiate it with regular crime. A non-state actor clause: applies to non-state actors but expressly excludes acts of war or legitimate activities of armed groups that may be covered under the international humanitarian law.[51]

### C. India's Leadership Role in International Law-Making

The credibility of India as an advocate of the comprehensive definition of terrorism with the cyber dimensions is based on three pillars. Its advocacy is moral because it has suffered as a victim of various forms of terrorism. It has a direct economic interest in a stable global cyberspace by virtue of being a significant digital economy. And the fact that it was the proposer

[50] S.C. Res. 2341, supra note 21; S.C. Res. 2396, supra note 20, ¶ 30.
[51] Saul, supra note 5, ch. 4; Ben Saul, *Research Handbook on International Law and Terrorism* ch. 3 (2d ed. Edward Elgar 2020); Yoram Dinstein, *War, Aggression and Self-Defence* 222–228 (6th ed. Cambridge Univ. Press 2017).

 [ISSN 2581-5369]

of the CCIT the very tool by which a new definition of cyber-terrorism would best be assimilated into the system, provides it with procedural standing and institutional permanence.[52]

India needs to submit a new draft of the CCIT before the UN General Assembly Ad Hoc Committee on Terrorism which would include the definition that consists of five elements as suggested in this paper. Concurrently, India needs to consult with the UN Group of Governmental Experts (GGE) regarding responsible state behaviour on cyberspace to promote complementary norms on state responsibility to terrorist cyber attacks launched on their soil. The G20 and SCO membership of India must be implemented in order to develop plurilateral coalitions behind these stands.[53]

## IX. CONCLUSION

This paper has argued three central propositions. **First**, the current global system of laws on counter-terrorism is fundamentally poor to contain cyber-terrorism. The patchwork of sectoral agreements, UNSC resolutions, and regional tools, which are attuned to a physical violence era, cannot offer a single definition, efficient rules of attribution, or quick cooperation arrangements when it comes to cyber-terrorism instances. Although the most pertinent existing tool, the Budapest Convention lacks the element of terrorist intent and its global scope is small; the fact that India is not a signatory undermines its power in South Asia even further.[54]

The domestic framework of India, though having the applicable provisions in both UAPA and IT Act, is rather weak in terms of the lack of definition; there is neither specific statute that regulates critical infrastructure protection, nor is there an effective inter-agency coordination; moreover, the infrastructure of mutual legal assistance is outdated. The gaps are not just technical in nature they directly translate into impunity of cyber-terrorist agents who can use the grey areas between the UAPA and the IT Act and between the Indian and international systems.

And **most importantly**, India is best placed to spearhead global advancement in addressing cyber-terrorism legislation. India as the pioneer among the digital economies that have been directly exposed to cyber-terrorism, and as a G20 and SCO member, can forge cross-regional

[52] Brahma Chellaney, India's Terrorism Challenge, 16(3) Asian Security 245 (2009); see also C. Raja Mohan, India and the Balance of Power, 85(4) Foreign Aff. 17 (2006).
[53] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Rep., U.N. Doc. A/70/174 (July 22, 2015); Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Rep., U.N. Doc. A/75/816 (Mar. 10, 2021).
[54] Convention on Cybercrime, supra note 23; see also Maura Conway, Cyberterrorism: Hype and Reality, in *Terrorism Online: Politics, Law and Technology* 97 (Lee Jarvis, Stuart Macdonald & Thomas Chen eds., Routledge 2015).

alliances that can develop a multi-dimensional international definition of the concept of terrorism that is clearly cyber-driven. The legal battle against cyber-terrorism-like all legal battles-begins with definition. India should lead the way.[55]

*****

[55] Saul, supra note 5, at 319–320; Upendra Baxi, The "War on Terror" and the "War of Terror": Nomadic Multitudes, Aggressive Incumbents, and the "New" International Law, 37(1) Osgoode Hall L.J. 7 (2005).

 [ISSN 2581-5369]