CYBER TERRORISM AND THE LIMITS OF INTERNATIONAL LAW: RETHINKING GLOBAL LEGAL RESPONSES IN THE DIGITAL AGE

Riya Sahni, Bhartiya Vidyapeeth University, Delhi

ABSTRACT

The advent of modern information and communication technology has dramatically changed the world's security scenario thereby helping terrorist groups leverage cyberspace for propagation of ideologies, planning operations, financial transactions and to launch operations targeting the infrastructure of key states. Cyber terrorism faces challenges that have never been present for conventional forms of terrorism; this stems from its international nature, the problems with identifying the culprits, jurisdictional divisions, and no universally agreed upon legal definition. Although international law has expanded with conventions on cybercrime, the United Nations and various other bodies on cyber terrorism, these initiatives are too disconnected. This article analyses whether the existing international legal frameworks on cyber terrorism are sufficient and the impact of Indian domestic legal framework under the global framework of cyber governance. By employing the doctrinal and comparative legal methods, it is argued that the existing legal frameworks have been largely reactive and the modern technological environment has left the current laws in inadequacy. Hence, the author emphasizes for the need of a coordinated legal framework through, establishing a widely accepted definition of cyber terrorism, efficient attribution regime, improved international cooperation and protected critical digital infrastructure.

Keywords: Cyber Terrorism; International Law; Cybersecurity; Budapest Convention; State Responsibility; Critical Infrastructure; India.

I. Introduction

The internet and the digital age have made cyberspace an integral part of our contemporary lives playing host to government, business, communication, healthcare, banking and national security. But with dependence on interlinked digital infrastructure also grows the avenues available to those who seek to capitalize on technical weaknesses. Among the emergent threats, cyber terrorism has been a great focus of concern on a global scale due to the ability of terrorist actors to create disruption on a large scale without the traditional geographical limitation. While it has been acknowledged that organizations use cyberspace as a means of conducting propaganda, recruitment, fundraising and intelligence, a terrorist operation within a cyberspace realm is seen as a reality.[1]

A key difference from terrorism more broadly is that cyber terrorism is not limited by borders and uses the internet's de-centralized structure to perpetrate an attack, sometimes from a remote location and involving the criminal acts of many in different jurisdictions, thereby making identification, attribution, evidence capture and international collaboration significantly more difficult than would be faced by ordinary criminals. This, in addition to a lack of a harmonized definition of cyber terrorism between jurisdictions, has created some practical and regulatory difficulties.

International law has, in recent years, developed to address the threat of cybercrime: the cybercrime conventions, UN-sponsored actions, various regional arrangements, and developing norms on State conduct in cyberspace all exist. However, these largely developed independently and, as noted previously, are tailored to address cybercrime, cyber warfare or counter-terrorism rather than specifically cyber terrorism. As such, a considerable lack of certainty exists as to what regime of law applies: issues such as jurisdiction, state responsibility, attribution and international cooperation remain largely unresolved.[2]

An interesting and important example of this development within legal frameworks is India. Given its scale as a major digital economy, India has criminalized the activity of cyber terrorism under its IT Act, 2000, and is building capabilities at the institutional level, while dealing with

[1] Saman Iftikhar, *Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures*, 10 PeerJ Comput. Sci. e1772 (2024).
[2] United Nations Office on Drugs and Crime (UNODC), Cybercrime Module 14: Cyberterrorism, E4J University Module Series, https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html.

cross-border issues in a limited fashion.

In this article we ask whether current international legal regime sufficiently govern cyber terrorism in the modern age. In this context, it asserts that whereas current instruments constitute an important regulatory normative base, their conception remains incoherent and operationally weak. It further claims that a properly regulated world necessitates a coherent, harmonious international legal order which circumvents definitional concerns, issues of attribution, extraterritoriality, preservation of critical digital infrastructure, while upholding international law basic principles.

II. Conceptualizing Cyber Terrorism: Definitional Ambiguity and Legal Implications

The Contested Nature of Cyber terrorism Despite its increased prominence in security discourse in the international arena, one thing which stands out regarding cyber terrorism is that it is one of the most contentious areas of the study of international law. Although other international crimes like piracy and genocide can rely upon relatively established definitions under the criminal law, cyber terrorism is not amenable to the same level of consensus across the board.[3] The debate concerning a precise definition is not confined to mere academic arguments[4] but can indeed have substantial impact on the question of criminalisation and also the issues related to international co-operation, extradition and criminal prosecution of offenders.[5]

This lack of agreement stems from the larger problem of defining terrorism. Disagreement over the politically sensitive topics of self-determination movements, state sponsored violence, and ideological struggles has kept states from agreeing to an all-encompassing convention on terrorism. This struggle intensifies in the cyber sphere, where the advantages of anonymity afforded by the internet, cross-border applicability, and evolving means of attack makes any definition difficult to codify under the law. Thus far, cyber terrorism is only implicitly covered under international law through existing counter-terrorism regimes, conventions on cybercrime

[3] Maura Conway, *Reality Bytes: Cyberterrorism and Terrorist "Use" of the Internet*, First Monday (2002), https://firstmonday.org/ojs/index.php/fm/article/view/1001.
[4] Jarvis L., Stuart Macdonald & Lella Nouri, *The Cyberterrorism Threat: Findings from a Survey of Researchers*, 37 Stud. Conflict & Terrorism 68 (2014).
[5] Yaroslav Shiryaev, *Cyberterrorism in the Context of Contemporary International Law*, 14 San Diego Int'l L.J. 139 (2012), https://digital.sandiego.edu/ilj/vol14/iss1/5/.

and international law in general principles.

However, within the context of academia, cyber terrorism typically refers to politically or ideologically motivated attacks on either governments or general populations by employing computer systems or networks and inflicting damage on either a small, moderate or large scale so as to instil societal fear, fear amongst a population group or physically cause harm to them. This is an aspect which differs cyber terrorism from cybercrime. In the instance of cybercrime, the motives generally differ with the desire being financial profit or some kind of selfish reward, as opposed to a cyber terrorist utilising technology as a device for coercion for political, religious, ideological purposes.[6]

Equally significant are the differences between cyber terrorism and cyber warfare. While cyber war broadly relates to operations that are carried out by or are attributable to states in a period of armed conflict or general geo-political conflict, cyber terrorism mostly consists in non-State groups using their cyber skills to gain their aims of ideological terrorism by threats and disruption. The evolving nature of terrorist organizations, and some evidence of indirect State support of cyber-enabled groups, has made that clear distinction a little more complicated, making its legal categorization and State responsibility more problematic.

In a same vein, we should distinguish clearly between hacktivism and cyberterrorism. Many hacktivism activities including some that are actually illegal occur, but their main objectives are related to political appeal, symbolic political performance, or expressive acts of protest and disagreement rather than spreading widespread fear or extreme anxiety, which is typically associated with terrorism. By mislabelling hacktivism and cyberterrorism, we may be overreaching antiterrorist legislation into areas that were not intended for its use, so violating individual liberties like the right to free expression and the ability to participate in political life.

This article contends that cyber-terrorism should instead be conceptualized as consisting of a confluence of cumulative factors, the presence of an ideological or political motive; a deliberate attempt to target either key infrastructure or systems with civilian uses; the ability to cause severe economic or physical damage to the societal fabric; and the intention of intimidating either the general public or governments. This interpretation better conforms to contemporary technology while better comporting to the basic tenets of criminal international law-i.e. The

[6] Dorothy E. Denning, *Cyberterrorism*, in Networks and Netwars: The Future of Terror, Crime, and Militancy 239 (John Arquilla & David Ronfeldt eds., RAND 2001).

need for an object and actus rea to establish an offense.

III. International Legal Framework Governing Cyber Terrorism

Cyberterrorism and International law, Fragmented Regulation, there are still gaps in the regulation of cyberterrorism under international law since no multilateral treaty covers this concept as an independent category of international crime. Instead, States must turn to a mix of conventions on cybercrime and counterterrorism, to customary international law and the new body of rules on State behaviour in cyberspace. Even if taken together these tools support international cybersecurity they do not offer a fully developed solution to the problem of cyber terrorism as they do not cover the specific legal issues in respect to that matter.

It may be concluded that the Convention on Cybercrime[7] (Budapest Convention) remains the main international normative act to criminalize certain cybercrimes. It was drafted in 2001 within the framework of the Council of Europe and, first and foremost, aimed to improve domestic cybercrime legislative frameworks, promote cross-border co-operation and define procedures for acquiring and exchanging of electronic evidence.[8] In essence, it criminalises, inter alia, unlawful access, data interference, system interference and computer fraud and defines a framework for mutual assistance and extradition.

Notwithstanding its role in governing many aspects of international cybercrime, however, the Convention did not, of itself, govern cyber terrorism. Its concerns related more to the misuse of computer technology itself than to the motivation or aims of terrorist activity. Therefore, a nation could find its electricity grid or emergency services put out of commission by a cyberattack that fell under the scope of the Convention, and at the same time create issues of terrorism that were well outside its intended remit. In sum, it is a vital procedural Convention but not a fully developed framework for governing cyber terrorism.

In addition to the Budapest Convention, the UN has increasingly been recognizing cyberspace as a new area of international security.[9] Through several resolutions, working groups of experts and efforts in counter-terrorism, the UN has supported member states to develop their cyber

[7] Convention on Cybercrime art. 2, Nov. 23, 2001, E.T.S. No. 185.
[8] Council of Europe, Explanatory Report to the Convention on Cybercrime, E.T.S. No. 185 (2001), https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.
[9] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015).

capacities, to share information and to work together against the use of digital technologies by terrorist groups. The United Nations Office on Drugs and Crime (UNODC) has highlighted, that terrorist organizations are utilizing cyberspace more frequently for recruitment, dissemination of information/propaganda, as well as for fundraising, training and terrorist attacks. Digital technology has become part of every modern terrorism.

However, these efforts continue to be mainly aspirational rather than legally binding. They are framed as attempts to foster cooperation but fall short of setting up globally legally binding standards for dealing with cyber terrorism. Crucially, they lack a universal definition to achieve harmonisation of domestic law among states. Thus, states continue to have different domestic definitions of and approach to cyber terrorism, posing hurdles in matters such as extradition and mutual legal assistance.

The biggest challenge facing the international law of cyberspace is arguably the attribution. This type of attacks (unlike usual ones) may be routed through a few countries, hijacked servers or an anonymous web of computer networks; it makes attributing responsibility extremely difficult. Technical attribution-which traces an attack back to what appears to be its point of origin-may be a step towards establishing legal attribution, but attribution under international law entails a much higher burden.

This division is especially critical in terms of the principles of State responsibility. Under the Articles on Responsibility of States for Internationally Wrongful Acts, only conduct that is attributable to the State and violates an international obligation gives rise to international responsibility.[10] This is difficult to do in cyberspace, as non-State actor actors can act autonomously, have decentralized technical infrastructures, and take active steps to avoid discovery. As such, even complex technical analyses do not typically meet the required standard to attribute such acts to a State and impose international responsibility.

Attribution Issues have wider ramifications for established principles of law such as sovereignty, non-intervention, and prohibition on the use of force.[11] Even if a cyberattack on critical infrastructure results in harm that would have been commensurate with that of a physical attack, doubt about attribution can inhibit States from adopting an adequate legal

[10] Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, U.N. Doc. A/56/10 (2001), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
[11] U.N. Charter art. 2, ss. 4.

posture in response to it.[12] Ambiguity undermined deterrence, hindering international cooperation and making it possible to exploit ambiguities of existing international law.

Aware of these difficulties, lawyers have more and more turn to the Tallinn Manual on the International Law Applicable to Cyber Operations for clarification of its meaning.[13] It is not binding international law, but the work represents an in-depth, scholarly analysis of the applicability of traditional principles-like sovereignty, due diligence, jurisdiction, and state responsibility-to the cyberspace context. Rather than developing new rules of law, the Manual argues that many aspects of international law remain meaningful, even in the midst of fast-paced technology development. At the same time, the Manual readily admits that consensus on when and at what level a particular type of cyberattack constitutes an illegal intervention, a prohibited use of force, or an armed attack, remains elusive.

What can be said from what has been stated about the current international system for malicious use is that the latter implies the central contradiction of cyber law: the ability to govern many activities while being incapable to address cyber terrorism properly due to definitional divergence, disparate treaty obligations, problematic attribution, and a non-homogenous international community engagement. Therefore, legal evolution should not replace the current international law system, but make it stronger, more harmonious, and less vague.

IV. India's Legal Framework: Progress and Persistent Challenges

India is one of the few jurisdictions to explicitly criminalize cyber terrorism under Section 66F of the Information Technology Act, 2000, an offense punishing hacking of secured computer or accessing these with the intent to threaten the unity, integrity, security or sovereignty of India or with intent to strike terror on the people of India.[14] In fact, a cyberattack when it goes beyond mere criminality has to be addressed as an attack on national security.

Complementing the Information Technology Act is the Unlawful Activities (Prevention) Act, 1967 (UAPA)[15] which provides the overall statutory backing for terrorist outfits and terrorist acts threatening the security of the nation. It gives police forces both the ammunition and the

[12] U.N. Charter art. 51.
[13] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2d ed. 2017), https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf.
[14] Information Technology Act, No. 21 of 2000, § 66F (India).
[15] Unlawful Activities (Prevention) Act, No. 37 of 1967 (India).

mandate to investigate and pursue digital and traditional facets of terrorist acts. Additionally, India's institutional infrastructure has been improved by policies such as the National Cyber Security Policy 2013[16] and organizations such as CERT-In that manage cyber incidents response, threat observation and multi-agency interaction.[17]

However, while there has been legislative progress in these areas, the problem of countering terrorism by and large has persisted with many of the very problems that hamper the international community's efforts at dealing with this problem. The nature of cyber terrorist attacks predominantly launched from overseas digital evidence being widely spread and a prosecution being almost exclusively reliant on cooperation between countries makes even the most rigorous domestic laws insufficient by themselves.

V. Towards a Coherent International Legal Framework for Cyber Terrorism

The preceding analysis demonstrates that the fundamental fault in the present framework of regulation is not the lack of international law, but that the regulation is fragmented. Cybercrime conventions, anti-terrorism treaties, State responsibility and cybersecurity agreements all regulate specific aspects of cyber terrorism in isolation. This lack of integration means that the interpretation, application and enforcement of these norms differ considerably and limit effective international cooperation. It is important therefore that future regulation should not build a wholly new legal regime, but rather address institutional deficiencies in harmonizing and coordinating the existing ones.[18]

One main aspect that needed reform was the use of a widely adopted cyber terrorism definition. Defining terrorism in politics was never a consensual activity, but the lack of a legal definition adds uncertainty to the issues of criminal jurisdiction, extradition, and mutual assistance. For purposes of criminalisation and transnational operations, a working international definition of cyber terrorism would differentiate cyber terrorism from cybercrime, cyber warfare, and hacktivism, by outlining cumulative components: ideology/politics driven; targeting infrastructure or civilians, intending to produce harm or mass societal impact, in order to create

[16] Ministry of Electronics & Information Technology, Government of India, National Cyber Security Policy, 2013.
[17] Indian Computer Emergency Response Team (CERT-In), *Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents* (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.
[18] Organization for Economic Cooperation and Development (OECD), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document* (2015).

political or governmental fear.[19]

Second, there's a strong need for enhanced multilateral coordination of attribution and digital evidence processes.[20] The inherent transborder nature of cyber investigations means a solo state response is rarely enough. Nations need to share live information more readily, establish consistent protocols for managing digital evidence, and streamline processes for the request and exchange of mutual legal assistance in cyber cases. Faster cross-border action by states would make it easier to find, investigate and prosecute suspects, and reduce the advantages terrorist groups might glean from fragmentation across jurisdictions.

More attention should be paid to safeguarding essential digital infrastructure.[21] Modern life depends on interconnected systems in which we are vulnerable to disruption of the energy supply, our health system, our transport networks, financial transactions, the telephone networks, or our public services. Cyberattacks in this domain can cause an impact similar to traditional terrorist actions, although they do not require weapons. Such cooperation should therefore go beyond criminal law into coordinated risk assessment, building up of cybersecurity capacity, resilience planning and sharing of information on developing threats.

Not less crucially, cybersecurity governance cannot simply be State-driven. A significant amount of digital infrastructure is in fact owned and operated by the private sector: tech firms, cloud computing providers, banks, telecoms. Preventing cyber terrorism thus demands public-private collaboration enshrined in appropriate institutions for effective data sharing, coordinated incident response and technological development that respects human rights and privacy. Such partnership-based governance should embrace the pragmatic reality that cybersecurity responsibilities are being shared by the state, industry, academia and the civil society.

Lastly, future international legislative responses should also not contradict the wider body of international human rights law.[22] Vague legislation that labels excessive online speech as cyber

[19] Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, C.E.T.S. No. 224 (May 12, 2022).
[20] Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence, C.E.T.S. No. 224 (2022).
[21] National Critical Information Infrastructure Protection Centre (NCIIPC), *Guidelines for Protection of Critical Information Infrastructure* (Gov't of India), https://www.asianlaws.org/gcld/cyberlawdb/IN/guidelines/NCIIPC_Guidelines_V2.pdf.
[22] International Covenant on Civil and Political Rights arts. 17 & 19, Dec. 16, 1966, 999 U.N.T.S. 171.

terrorism should not serve as an excuse to crack down on political opposition, limit freedom of expression or to conduct indiscriminate online surveillance.[23] Counter-terrorism responses that fail to recognize due process rights or the right to privacy pose an erosion of the rule of law they set out to uphold, and so future responses should maintain a balance between collective safety and individual liberty.

VI. Conclusion

The arrival of cyber terrorism in the international security space has indeed revolutionized the security landscape by giving politically motivated individuals the opportunity to exploit technological capacities far beyond those exploited for petty cybercrimes. Because of its transnational character, the nature of the technologies involved, and the fact that it can affect vital infrastructures, cyber terrorism has brought to light the inadequacy of legal structures created for criminal behaviour or war.

This article contends that key constraints on the ability to effectively regulate is not so much technological, but normative. The lack of an accepted definition, issues of attribution remain intractable, fractured jurisdiction and inconsistent international co-operation each erode the State's capacity to deter, prosecute and investigate the perpetrators of cyber-terrorism. India's legislative measures illustrate that reforms at the domestic level can improve domestic capacity but national legislation alone cannot cope with cyber threats that disregard jurisdiction and exploit systemic weaknesses.

To ensure the effectiveness of international law in the future, a coherent and more harmonised regime must be achieved which will mesh the existing principles of law with new realities of technology. In doing so, the existing notions of sovereignty, jurisdiction and State responsibility need not be rejected but adjusted to include better cooperation, standardized attribution and protection mechanisms for vital infrastructure and the co-ordination between States and private parties. This will have the effect not only of improving the legal response to cyber terrorism but also fostering a more secure, stable and rules based digital world.

The issue, as cyberspace becomes an indispensable site for global intercourse, is not whether cyber-terrorism should be regulated by law but whether existing institutions will have the

[23] Human Rights Council, Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27 (May 16, 2011).

flexibility and the coherence to adapt quickly enough to deal with what will undoubtedly be one of the great security challenges of the age.