VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

EXTRATERRITORIALITY, CYBER TERRORISM, AND CYBER SOVEREIGNTY: ANALYZING THE EFFICACY OF SECTION 113 OF THE BHARATIYA NYAYA SANHITA, 2023

- K.K.Sathyaraj[1]

ABSTRACT

The rapid evolution of cyberspace has transformed the nature of terrorism, sovereignty, and criminal jurisdiction. Cyber terrorism today transcends territorial boundaries and challenges traditional legal doctrines rooted in physical geography and state-centric jurisdiction. In response to emerging digital threats, India enacted the Bharatiya Nyaya Sanhita, 2023 (BNS), replacing the Indian Penal Code, 1860. Section 113 of the BNS introduces a comprehensive definition of "terrorist acts" and extends criminal liability to acts committed both within and outside India, thereby recognizing the doctrine of extraterritorial jurisdiction. This paper critically analyzes Section 113 in the context of cyber terrorism and the evolving concept of cyber sovereignty. It examines whether the provision adequately addresses transnational cyber threats while maintaining constitutional safeguards and legal certainty.

The study adopts a doctrinal and comparative methodology by examining legal frameworks in the United States, United Kingdom, European Union, and Israel. It identifies significant regulatory gaps in India's cyber terrorism framework, including definitional ambiguity, overlap with the Unlawful Activities (Prevention) Act, 1967 and the Information Technology Act, 2000, weak international cooperation mechanisms, and lack of specialized procedural safeguards. The paper further evaluates constitutional concerns under Articles 14, 19, and 21 of the Constitution of India, particularly in relation to privacy, free speech, and due process.

The paper argues that while Section 113 represents a significant modernization of India's criminal law framework, it remains insufficient to effectively regulate cyber terrorism in the

[1] Student at School of Excellence In Law, Tamilnadu Dr. Ambedkar Law University.

age of hybrid warfare and digital sovereignty. The study concludes by proposing comprehensive legal reforms, including specialized cyber terrorism legislation, institutional restructuring, international cooperation mechanisms, and judicial oversight frameworks.

Keywords: Cyber Terrorism, Extraterritorial Jurisdiction, Cyber Sovereignty, Digital Sovereignty, Cybercrime, National Security, International Cyber Law.

INTRODUCTION

The digital revolution has fundamentally altered the relationship between sovereignty, security, and criminal law. Unlike conventional crimes confined within territorial borders, cyber terrorism transcends geographical limitations and enables non-state actors to target national infrastructure from remote jurisdictions.The emergence of cyber warfare, digital espionage, ransomware attacks, and cyber-enabled terror financing has exposed the inadequacy of traditional criminal law frameworks rooted in territorial sovereignty.[2]

India's enactment of the Bharatiya Nyaya Sanhita, 2023 represents a transformative shift in criminal jurisprudence. Section 113 of the BNS criminalizes "terrorist acts" and extends liability to acts committed both within India and outside its territorial boundaries.[3] This provision reflects the growing trend of states exercising extraterritorial criminal jurisdiction to protect national security interests in cyberspace.

The concept of "cyber sovereignty" emerges prominently in this context. States increasingly project legal authority beyond territorial borders to regulate digital spaces, cyber threats, and transnational terrorism.[4] Section 113 therefore represents more than a penal provision; it is an assertion of digital sovereignty in an interconnected world.

However, despite its significance, Section 113 raises serious constitutional and operational concerns. The provision overlaps substantially with the Unlawful Activities (Prevention) Act, 1967 (UAPA), particularly Section 15 concerning terrorist acts.[5] The broad wording of terms

[2]Yoram Dinstein, *Non-International Armed Conflicts in International Law* (Cambridge University Press 2014)
[3]Bharatiya Nyaya Sanhita, 2023, s. 113.
[4]Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006)
[5]Unlawful Activities (Prevention) Act, 1967, s. 15

such as "economic security" and "public emergency" creates interpretative uncertainty and risks of arbitrary enforcement.

Further, India lacks a dedicated legal framework specifically addressing cyber terrorism. Existing provisions under the Information Technology Act, 2000 and UAPA operate in fragmented silos, producing institutional overlap and enforcement inconsistencies.[6] The increasing frequency of cyber attacks targeting financial institutions, government databases, communication systems, and critical infrastructure demonstrates the urgency of a coherent legal framework.

This paper critically examines the efficacy of Section 113 of the BNS in addressing cyber terrorism through the lens of extraterritoriality and cyber sovereignty. It undertakes a comparative legal analysis with foreign jurisdictions and proposes reforms necessary to strengthen India's cyber terrorism framework.

NEED FOR THE STUDY

The study becomes necessary because cyber terrorism has emerged as one of the most serious threats to national security in the twenty-first century. Terrorist organizations increasingly use cyberspace for recruitment, propaganda dissemination, financing, encrypted communication, and attacks on critical infrastructure.[7] Traditional criminal law mechanisms are insufficient to address these technologically sophisticated and transnational threats.

The incorporation of terrorism within the BNS creates a new legal regime where ordinary criminal law intersects with national security legislation. This shift necessitates scholarly examination because it expands executive power and criminal jurisdiction beyond traditional limits.

The study is also necessary because India's cyber legal framework remains fragmented. Section 66F of the Information Technology Act, 2000 criminalizes cyber terrorism, while the UAPA addresses terrorist acts more broadly.[8] The addition of Section 113 of the BNS creates overlapping offences and jurisdictional ambiguity.

[6]Information Technology Act, 2000, s. 66F
[7] Bruce Hoffman, *Inside Terrorism* (Columbia University Press 2006)
[8] Information Technology Act, 2000, s. 66F; UAPA, 1967, s. 15

Moreover, India has witnessed a substantial increase in cybercrime cases. NCRB data indicates continuous growth in cyber offences, including attacks involving ransomware, digital fraud, and attacks on critical infrastructure.[9] These developments demand a modernized legal framework capable of effectively regulating cyber terrorism while preserving constitutional rights.

SIGNIFICANCE OF THE STUDY

The study is significant because it contributes to the emerging discourse on digital sovereignty and transnational criminal jurisdiction. It examines how states increasingly use criminal law as an instrument of strategic sovereignty in cyberspace.

The paper is important for policymakers because it identifies deficiencies within India's cyber terrorism framework and proposes reforms based on comparative international practices. It is equally relevant for constitutional scholars because it evaluates the implications of Section 113 for privacy, due process, and free speech.

The study also contributes to comparative legal scholarship by analyzing foreign approaches toward cyber terrorism and extraterritorial jurisdiction. It demonstrates how advanced jurisdictions combine legal regulation, institutional coordination, and international cooperation to address cyber threats.[10]

REVIEW OF LITERATURE

Dorothy Denning defines cyber terrorism as unlawful attacks against computers, networks, and information systems intended to intimidate governments or populations for political purposes.[11] Denning argues that cyber attacks targeting essential infrastructure may produce consequences equivalent to physical terrorism.

[9] NCRB, *Cyber Crime Statistics Report 2023* (Government of India 2024)
[10] Council of Europe Convention on Cybercrime, Budapest Convention 2001
[11] Dorothy E. Denning, 'Cyberterrorism' (2000) Georgetown University Testimony

Yoram Dinstein emphasizes that cyberspace challenges traditional doctrines of attribution and territorial sovereignty.[12] According to Dinstein, cyber operations blur distinctions between state-sponsored warfare and non-state terrorist activities.

Indian scholars such as Apar Gupta criticize India's cyber regulatory framework for excessive executive discretion and insufficient procedural safeguards.[13] Gautam Bhatia similarly argues that vague cyber laws risk undermining constitutional liberties, particularly freedom of speech and privacy.[14]

Contemporary scholarship on the BNS suggests that Section 113 duplicates existing provisions under the UAPA and may create parallel anti-terror regimes. However, there remains limited literature specifically examining Section 113 through the lens of cyber terrorism and cyber sovereignty.

RESEARCH STATEMENT

This research examines whether Section 113 of the Bharatiya Nyaya Sanhita, 2023 effectively addresses cyber terrorism and extraterritorial threats while preserving constitutional safeguards, legal certainty, and international compatibility.

RESEARCH PROBLEM

The principal research problem concerns the ambiguity and overbreadth of Section 113 in regulating cyber terrorism. Although the provision expands India's jurisdictional reach, it fails to clearly define cyber terrorism, establish specialized procedural safeguards, or provide effective mechanisms for international cooperation and digital evidence collection.

RESEARCH QUESTIONS

1. Whether Section 113 adequately addresses cyber terrorism and extraterritorial threats?
2. Whether Section 113 overlaps with the UAPA and IT Act in a manner creating regulatory inconsistency?

[12] Yoram Dinstein, *Cyber War and International Law* (Cambridge University Press 2018)
[13] Apar Gupta, 'Digital Surveillance and Constitutional Freedoms in India' (2019) 4 Indian Journal of Constitutional Law 112
[14] Gautam Bhatia, *The Transformative Constitution* (HarperCollins 2019)

3. How do foreign jurisdictions regulate cyber terrorism and extraterritorial criminal jurisdiction?
4. Whether Section 113 satisfies constitutional principles of legality and proportionality?
5. What reforms are necessary to strengthen India's legal framework governing cyber terrorism?

HYPOTHESIS

The study hypothesizes that while Section 113 of the BNS significantly expands India's anti-terror framework through extraterritorial jurisdiction, it remains inadequate in addressing cyber terrorism due to definitional ambiguity, overlap with existing legislation, insufficient procedural safeguards, and weak international cooperation mechanisms.

RESEARCH METHODOLOGY

The study adopts doctrinal and comparative methodologies. Primary sources include statutes, constitutional provisions, judicial decisions, international conventions, parliamentary debates, and governmental reports. Secondary sources include books, journal articles, policy papers, and academic commentaries.

Comparative analysis is undertaken with the legal systems of the United States, United Kingdom, European Union, and Israel.

AIMS AND OBJECTIVES

1. To analyze the scope and structure of Section 113 of the BNS.
2. To examine the concept of extraterritoriality and cyber sovereignty in cyber law.
3. To identify regulatory gaps in India's cyber terrorism framework.
4. To undertake comparative analysis with foreign jurisdictions.
5. To propose legal and institutional reforms.

SCOPE AND LIMITATIONS

The study primarily focuses on Section 113 of the BNS in relation to cyber terrorism and extraterritorial criminal jurisdiction. It includes comparative analysis with selected foreign jurisdictions.

However, the study does not comprehensively address military cyber warfare governed by international humanitarian law. Judicial precedents interpreting Section 113 are also limited because the legislation is recent

CHAPTER I – CONCEPTUAL FRAMEWORK OF CYBER TERRORISM AND EXTRATERRITORIALITY

The first chapter lays the theoretical and jurisprudential foundation of the study by examining the concepts of cyber terrorism, extraterritoriality, digital sovereignty, and cyber sovereignty. Cyber terrorism is fundamentally different from traditional terrorism because it operates in a borderless virtual environment where attacks may originate from one country, pass through multiple jurisdictions, and ultimately affect another sovereign state. Unlike conventional crimes confined within territorial boundaries, cyber offences undermine the classical doctrine of territorial sovereignty, which historically formed the basis of criminal jurisdiction.[15] This chapter explains how technological globalization has weakened the effectiveness of traditional jurisdictional principles and compelled states to increasingly rely on extraterritorial legal mechanisms.

The chapter further explores the evolution of extraterritorial jurisdiction under international law through principles such as territoriality, nationality, passive personality, universality, and the protective principle. Particular emphasis is placed on the protective principle because cyber terrorism directly threatens national security, economic stability, and critical infrastructure. The chapter also discusses the concept of "cyber sovereignty," where states extend their regulatory and penal authority beyond physical borders to preserve digital and strategic security interests.[16]

[15] Malcolm N. Shaw, *International Law* (8th edn, Cambridge University Press 2017)
[16] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006)

The chapter analyzes how cyberspace has transformed warfare and terrorism into hybrid and asymmetric threats. Terrorist organizations increasingly use digital technologies for propaganda dissemination, recruitment, encrypted communication, financing, and attacks on strategic infrastructure.[17] Consequently, the traditional distinction between internal security and external aggression has become blurred. The chapter therefore establishes the conceptual basis for understanding why states such as India are increasingly incorporating cyber threats within national criminal law frameworks.

The chapter also examines international instruments such as the Budapest Convention on Cybercrime, the Tallinn Manual on International Cyber Warfare, and United Nations resolutions concerning cybersecurity and terrorism.[18] It demonstrates that while international law recognizes cyber threats as serious security concerns, there remains no universally accepted definition of cyber terrorism. This absence of consensus creates significant legal uncertainty for states attempting to regulate transnational cyber offences.

The chapter concludes by emphasizing that cyber terrorism represents not merely a technological challenge but a constitutional and geopolitical challenge to state sovereignty itself. Therefore, any legal framework addressing cyber terrorism must balance national security with constitutional guarantees, international cooperation, and protection of civil liberties.

CHAPTER II – ANALYSIS OF SECTION 113 OF THE BHARATIYA NYAYA SANHITA, 2023

The second chapter critically examines the scope, structure, and implications of Section 113 of the Bharatiya Nyaya Sanhita, 2023. This chapter begins by analyzing the legislative transformation brought about by the replacement of the Indian Penal Code, 1860 with the BNS. Section 113 introduces terrorism directly into the general penal law framework, thereby normalizing anti-terror provisions within ordinary criminal law rather than treating them as exceptional legislation.

[17] Bruce Hoffman, *Inside Terrorism* (Columbia University Press 2006)
[18] Council of Europe Convention on Cybercrime, Budapest Convention 2001

The chapter examines the language of Section 113 in detail. It highlights that the provision criminalizes acts threatening the unity, integrity, sovereignty, security, or economic security of India and applies to acts committed both within and outside India.[19] This explicit recognition of extraterritorial jurisdiction demonstrates the Indian state's intention to address transnational threats in cyberspace. The provision also criminalizes conspiracy, financing, recruitment, facilitation, harboring, and organizational support relating to terrorist acts.

A significant portion of the chapter focuses on the applicability of Section 113 to cyber terrorism. It explains how cyber attacks targeting banking systems, power grids, communication infrastructure, transportation systems, government databases, and critical information systems may fall within the ambit of "terrorist acts." However, the chapter identifies a major weakness in the provision: the absence of a clear statutory definition of cyber terrorism. Unlike Section 66F of the Information Technology Act, 2000[20], Section 113 does not specifically address cyber-enabled terrorist activities.

The chapter also critically evaluates the overlap between Section 113 and the Unlawful Activities (Prevention) Act, 1967.[21] Since both provisions regulate terrorist acts using similar language, there exists a risk of prosecutorial inconsistency, forum shopping, and arbitrary exercise of discretion. The coexistence of multiple anti-terror laws may undermine legal certainty and procedural fairness.

Further, the chapter discusses constitutional concerns arising from vague terminology such as "economic security" and "public emergency." Such undefined expressions may lead to expansive interpretation by investigative agencies and potentially infringe constitutional rights under Articles 14, 19, and 21 of the Constitution of India.[22] The chapter therefore argues that while Section 113 represents an important modernization of criminal law, it remains legally ambiguous and procedurally incomplete.

CHAPTER III – COMPARATIVE LEGAL ANALYSIS OF FOREIGN JURISDICTIONS

[19] Bharatiya Nyaya Sanhita, 2023, s. 113
[20] Information Technology Act, 2000, s. 66F
[21] Unlawful Activities (Prevention) Act, 1967, s. 15
[22] Constitution of India arts 14, 19 & 21

The third chapter undertakes a comparative analysis of cyber terrorism laws and extraterritorial jurisdiction frameworks in selected foreign jurisdictions including the United States, United Kingdom, European Union, and Israel. The objective of this chapter is to identify best practices and evaluate how other democratic jurisdictions address cyber threats while balancing constitutional safeguards and national security concerns.

The chapter first examines the United States legal framework under the USA PATRIOT Act, the Computer Fraud and Abuse Act, and various federal counterterrorism statutes.[23] The United States adopts an expansive model of extraterritorial jurisdiction and treats cyber terrorism as a national security issue integrated with homeland security and intelligence operations. Federal agencies such as the FBI, NSA, and CISA possess specialized investigative and surveillance powers. The chapter highlights how the United States combines criminal law with cybersecurity policy, intelligence coordination, and international cooperation mechanisms.

The chapter then examines the United Kingdom's approach under the Terrorism Act, 2000 and the Computer Misuse Act, 1990.[24] The UK framework emphasizes preventive counterterrorism strategies, digital surveillance, infrastructure protection, and intelligence gathering. The role of the National Cyber Security Centre (NCSC) is discussed as an example of specialized institutional coordination.

The chapter further analyzes the European Union's cybersecurity framework, particularly the Budapest Convention, the NIS Directive, and GDPR-related cybersecurity obligations.The European approach prioritizes harmonization, judicial oversight, and transnational cooperation among member states. The chapter notes that unlike India, the EU framework places greater emphasis on privacy protection and proportionality.

Israel's cybersecurity framework is also examined due to its advanced cyber defense infrastructure. Israel integrates military intelligence, civilian cybersecurity agencies, and

[23] USA PATRIOT Act, 2001; Computer Fraud and Abuse Act, 1986
[24] Terrorism Act 2000 (UK); Computer Misuse Act 1990 (UK)

private sector collaboration into a unified national strategy.[25] The chapter highlights Israel's proactive cyber defense measures and sophisticated attribution mechanisms.

Through comparative analysis, the chapter identifies several deficiencies in India's legal framework, including the absence of specialized cyber terrorism legislation, inadequate institutional coordination, weak attribution mechanisms, limited forensic capacity, and insufficient international cooperation. The chapter argues that India's current approach remains fragmented and reactive when compared to advanced jurisdictions.

CHAPTER IV – REGULATORY GAPS AND CONSTITUTIONAL CHALLENGES IN INDIA

The fourth chapter identifies the major regulatory, institutional, and constitutional deficiencies in India's legal framework governing cyber terrorism. The chapter begins by examining the absence of a comprehensive statutory definition of cyber terrorism under the BNS. The vague and overbroad wording of Section 113 creates uncertainty regarding the scope of criminal liability.

The chapter explains that cyber terrorism presents unique evidentiary and investigative challenges because cyber attacks often involve anonymous actors, encrypted communication systems, proxy servers, botnets, and decentralized digital networks.[26] However, Indian law lacks specialized evidentiary standards governing attribution, digital forensics, chain of custody, and admissibility of electronic evidence in transnational cyber terrorism cases.

Another important issue discussed in the chapter concerns international cooperation. India is not a party to the Budapest Convention on Cybercrime, which limits access to effective transnational cooperation mechanisms. Mutual Legal Assistance Treaty procedures remain slow and inefficient for real-time cyber investigations, thereby weakening India's ability to prosecute cross-border cyber offences.

The chapter also examines constitutional challenges associated with Section 113. Vague and expansive anti-terror provisions may violate constitutional guarantees under Articles 14, 19, and 21 of the Constitution. The Supreme Court's judgments in *Shreya Singhal v. Union of*

[25] Israel National Cyber Directorate, Cybersecurity Strategy Reports (2023)
[26] Yoram Dinstein, *Cyber War and International Law* (Cambridge University Press 2018)

India[27] and *K.S. Puttaswamy v. Union of India*are analyzed in this context.[28] The chapter argues that excessive state surveillance and broad criminalization may produce chilling effects on speech, privacy, dissent, and digital activism.

Further, the chapter discusses institutional fragmentation among agencies such as CERT-In, NIA, intelligence agencies, cybercrime cells, and state police authorities. The absence of a centralized cybersecurity authority results in coordination failures and operational inefficiency.

The chapter concludes that India's cyber terrorism framework suffers from doctrinal ambiguity, procedural inadequacy, institutional fragmentation, and constitutional vulnerability. Without comprehensive reform, Section 113 may expand state power without effectively addressing cyber threats.

CHAPTER V – PROPOSALS FOR LEGAL REFORM

The fifth chapter proposes comprehensive reforms necessary to strengthen India's cyber terrorism framework while preserving constitutional values and democratic accountability. The chapter argues that India requires a dedicated Cyber Terrorism Prevention Act harmonizing the BNS, UAPA, and Information Technology Act into a coherent legal framework. Such legislation should provide a precise definition of cyber terrorism distinguishing it from ordinary cybercrime and cyber warfare.

The chapter recommends the establishment of specialized cyber terrorism courts staffed by judges and prosecutors trained in cybersecurity, digital evidence, and transnational investigations.[29] Specialized courts would improve consistency, expertise, and procedural efficiency in complex cyber cases.

Another major recommendation concerns international cooperation. The chapter strongly advocates India's accession to the Budapest Convention to facilitate evidence-sharing, extradition, and cross-border investigations. India must also strengthen bilateral cybersecurity agreements and real-time intelligence-sharing mechanisms.

[27] *Shreya Singhal v Union of India* (2015) 5 SCC 1
[28] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1
[29] Law Commission of India, Report No 277 on Wrongful Prosecution (2018)

The chapter further proposes the creation of a unified National Cybersecurity Authority coordinating intelligence agencies, CERT-In, NIA, cybercrime units, and private sector stakeholders.[30] Institutional integration would improve attribution, infrastructure protection, and emergency response capacity.

Constitutional safeguards also form a major focus of the reform proposals. The chapter recommends stronger judicial oversight over surveillance powers, mandatory proportionality standards, parliamentary review mechanisms, and procedural protections for privacy and free speech.[31]

Additionally, the chapter highlights the importance of strengthening digital forensic infrastructure, cybersecurity education, public-private partnerships, AI-assisted threat detection systems, and critical infrastructure resilience.

The chapter concludes that effective cyber terrorism regulation requires not merely stronger punitive laws but also institutional modernization, international cooperation, technological expertise, and constitutional accountability.

CONCLUSION

The emergence of cyber terrorism has fundamentally transformed the relationship between sovereignty, security, and criminal law in the twenty-first century. Traditional territorial models of criminal jurisdiction are increasingly inadequate in addressing transnational cyber threats capable of targeting national infrastructure, economic systems, and public institutions from remote jurisdictions. In response to these evolving threats, Section 113 of the Bharatiya Nyaya Sanhita, 2023 represents India's attempt to modernize criminal law and assert digital sovereignty through expanded extraterritorial jurisdiction.

The study demonstrates that Section 113 reflects the growing doctrine of cyber sovereignty, whereby states increasingly extend penal authority beyond territorial borders to protect national security interests in cyberspace. By criminalizing terrorist acts committed both within and outside India, the provision recognizes the borderless nature of contemporary

[30] National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India
[31] *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301

cyber threats. However, despite its significance, Section 113 suffers from substantial doctrinal, constitutional, and operational deficiencies.

The research reveals that the absence of a clear definition of cyber terrorism, overlap with the UAPA and Information Technology Act, weak procedural safeguards, limited international cooperation mechanisms, and inadequate digital forensic infrastructure undermine the effectiveness of India's anti-terror framework. The broad and ambiguous wording of the provision also raises serious constitutional concerns under Articles 14, 19, and 21 of the Constitution of India, particularly regarding privacy, free speech, and due process protections.

Comparative analysis with the United States, United Kingdom, European Union, and Israel demonstrates that effective cyber terrorism regulation requires more than expansive penal provisions. Advanced jurisdictions combine specialized legislation, institutional coordination, intelligence integration, judicial oversight, international cooperation, and technological capacity-building.[32] India's current framework remains fragmented and reactive in comparison.

The study ultimately concludes that while Section 113 represents an important step toward modernization of India's criminal law system, it is insufficient as a standalone mechanism for regulating cyber terrorism in the age of hybrid warfare and digital sovereignty. Comprehensive reform is therefore essential. India must adopt specialized cyber terrorism legislation, strengthen constitutional safeguards, improve institutional coordination, enhance digital forensic capabilities, and actively participate in international cybersecurity frameworks.

Only through a balanced approach integrating national security, constitutionalism, technological expertise, and international cooperation can India effectively combat cyber terrorism while preserving democratic freedoms and the rule of law in the digital age.

[32] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017)