
SAFEGUARDING BHARAT: A CONSTITUTIONAL AND STRATEGIC FRAMEWORK FOR COMBATING TERRORISM AND STRENGTHENING NATIONAL SECURITY IN THE 21ST CENTURY

Sonali Maind, Maharashtra National Law University Chhatrapati Sambhajinagar

ABSTRACT

Terrorism in contemporary India has evolved from localized insurgencies to a complex, hybrid threat that merges traditional violence with cyber-warfare, transnational financing, ideological radicalization, and digital propaganda. The recent Pahalgam ambush of 2025 has once again exposed the inadequacies in India's legal, intelligence, and institutional apparatus. This research paper critically examines India's counter-terrorism framework from a constitutional and strategic lens. It analyses the role of core legislation such as the Unlawful Activities (Prevention) Act, the functioning of institutions like the National Investigation Agency, the implications of surveillance on civil liberties, and the inadequacy of current mechanisms to deal with cyber-terrorism. The study contends that while India has made commendable efforts through international cooperation, FATF compliance, and bilateral intelligence exchanges, there exists a pressing need for a codified national security doctrine rooted in constitutional values. Drawing from global best practices and Indian jurisprudence, this paper proposes a holistic model that reinforces operational efficiency without sacrificing democratic ethos. In conclusion, it argues that national security must not merely be a function of state power, but an embodiment of the republic's foundational ideals. Only through a constitutionally aligned, technologically empowered, and ethically accountable framework can India truly safeguard Bharat in this era of asymmetrical warfare.

Keywords: Terrorism in India, National Security Doctrine, Unlawful Activities (Prevention) Act (UAPA), Cyber-Terrorism and Surveillance, Constitutional Rights and Internal Security, Counter-Terrorism Strategy and Legal Reform

Introduction:

Terrorism has historically been understood as a calculated form of political violence aimed at civilian populations to achieve ideological or strategic outcomes. In India, this understanding was largely shaped by experiences such as the Khalistan movement, insurgency in Kashmir, and Naxalite extremism. However, the dawn of the 21st century, particularly in the post-9/11 and post-26/11 eras, heralded a dramatic shift in the structure, sources, and methods of terrorism. India's current security paradigm must contend with a hybrid form of terrorism—one that marries traditional violence with digital propaganda, economic sabotage, bio-warfare, and cyberattacks. The 2025 Pahalgam attack, where militants ambushed an army convoy using encrypted communications and drone surveillance, serves as a harrowing illustration of this new threat spectrum¹. What is particularly alarming is the convergence of ideological, religious, and digital fronts in modern terrorism. Radical ideologies are now spread through encrypted platforms like Telegram, and weaponization of social media has enabled real-time mobilization of supporters and miscreants across the globe². Lone wolf actors, indoctrinated online, pose greater detection challenges than organized cells³. Moreover, state-sponsored terrorism remains a persistent challenge—India continues to suffer from Pakistan-backed networks that operate through a complex web of militant outfits, digital fund-raising campaigns, and foreign-based sympathizers⁴. These networks not only threaten national security but also erode public confidence in democratic institutions and the justice system⁵. In this milieu, it becomes imperative to re-examine our national security and counter-terrorism framework from a multidimensional perspective: legal, constitutional, technological, and diplomatic.

Legal and Institutional Framework for Combating Terrorism in India

The Indian legal system, guided by the Constitution, seeks to harmonize the competing demands of individual liberty and national security. While the fundamental rights enshrined in

¹ Ministry of Home Affairs, Government of India, “*Annual Report 2024–2025*,” (New Delhi: MHA, 2025), pp. 34–36

² Kabir Taneja, *The ISIS Peril: The World's Most Feared Terror Group and Its Shadow on South Asia* (New Delhi: Penguin Random House, 2020), p. 101

³ Sameer Patil, “*Lone Wolf Terrorism in India: A Growing Concern*,” ORF Occasional Paper, No. 293 (Observer Research Foundation, 2022), p. 4

⁴ Arvind Gupta, “*State-Sponsored Terrorism and India's Strategic Options*,” IDSA Journal, Vol. 48, No. 3 (2023), pp. 11–15

⁵ Ronojoy Sen, “*India's Democracy under Siege: Terrorism and the Erosion of Institutions*,” Economic and Political Weekly, Vol. 58, No. 5 (2023), p. 18

Part III of the Constitution offer citizens robust protections, the extraordinary threat of terrorism has often compelled the legislature and judiciary to carve out exceptions. Article 19(1)(a) guarantees the right to freedom of speech and expression, but this is subject to “reasonable restrictions” in the interests of the sovereignty and integrity of India, public order, and national security⁶. Similarly, Article 21 protects life and personal liberty, but the phrase “procedure established by law” has become the battlefield for contesting preventive detention, surveillance, and custodial practices in anti-terror operations⁷. Notably, Article 355 casts a constitutional obligation upon the Union to protect every State against external aggression and internal disturbance, providing a foundational justification for central intervention in terrorism cases⁸. The Supreme Court, through landmark cases such as *A.K. Gopalan v. State of Madras* and later *Maneka Gandhi v. Union of India*, has gradually shifted towards a rights-protective interpretation of liberty, yet counter-terror laws have often operated at the margin of these protections⁹.

Among the most powerful weapons in India’s legislative arsenal against terrorism is the Unlawful Activities (Prevention) Act, 1967 (UAPA), which has undergone multiple amendments to expand its scope. Originally designed to deal with secessionist tendencies, it now criminalizes terrorist activities, bans organizations, and empowers the National Investigation Agency (NIA) to arrest and detain suspects under stringent conditions¹⁰. The 2019 amendment to UAPA, which allowed individuals (not just organizations) to be declared terrorists, has raised serious constitutional concerns regarding due process and presumption of innocence¹¹. The law allows for detention up to 180 days without filing a charge sheet and makes bail extraordinarily difficult, especially when the mere accusation of terrorism invokes Sections 15–19 of the Act¹². Despite criticism, the government defends UAPA as a necessary evil, citing national security exigencies and operational difficulties in counter-terrorism.

The institutional framework for enforcing these laws is led by the National Investigation Agency (NIA), established under the NIA Act, 2008. The NIA functions as a centralized body with powers to investigate and prosecute offences listed in the Act’s Schedule, including those

⁶ The Constitution of India, Art. 19(2)

⁷ *Maneka Gandhi v. Union of India*, AIR 1978 SC 597

⁸ The Constitution of India, Art. 355

⁹ *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27; *Maneka Gandhi v. Union of India*, AIR 1978 SC 597

¹⁰ Unlawful Activities (Prevention) Act, 1967, as amended in 2019, §§ 2, 15–19

¹¹ Gautam Bhatia, “Due Process and the UAPA,” The Hindu, August 22, 2019

¹² UAPA, 1967, §43D(2), (5)

under UAPA, Explosive Substances Act, and Atomic Energy Act¹³. It enjoys pan-India jurisdiction and can even investigate cases outside India with prior approval. However, its functioning has invited debate about federalism and Centre-State relations, particularly when the NIA assumes control of cases without consulting State police forces¹⁴. This centralization, while operationally efficient, risks bypassing local intelligence and alienating State agencies that play a critical role in early detection of radicalization and insurgency.

Another contentious statute is the Armed Forces (Special Powers) Act, 1958 (AFSPA), which gives the military sweeping powers in “disturbed areas” such as parts of Jammu & Kashmir and the North-East. The Act allows armed forces to use force, shoot to kill, and arrest without warrant based on mere suspicion¹⁵. While AFSPA is justified as necessary in insurgency-prone zones, human rights organizations have criticized it for providing blanket immunity to security personnel, thereby contributing to a culture of impunity¹⁶. Judicial pronouncements such as *Extra Judicial Execution Victim Families Association v. Union of India* have attempted to balance the operational needs of the army with the human rights of citizens, but legislative reform remains elusive¹⁷.

Despite the wide arsenal of legal tools, enforcement remains problematic. According to reports, UAPA cases have a dismally low conviction rate of less than 3%, indicating that either charges are poorly framed or evidentiary standards are not met¹⁸. Prolonged pre-trial detentions, delay in forensic analysis, and the lack of special anti-terror courts exacerbate the situation. Bail jurisprudence in such cases has evolved cautiously, with courts often prioritizing state narratives over individual liberty. Yet, in recent judgments such as *Union of India v. K.A. Najeeb*, the Supreme Court emphasized that statutory bars on bail should not override constitutional guarantees under Article 21, especially where trial is likely to take years¹⁹.

What emerges from this complex interplay of statutes, institutions, and judicial oversight is a fragmented and reactive system that often responds to crises rather than anticipates them. The need of the hour is not just more stringent laws, but smarter legal frameworks that uphold

¹³National Investigation Agency Act, 2008, §6

¹⁴V. Venkatesan, “*Jurisdictional Overreach by NIA*,” *Frontline*, Vol. 37, Issue 15 (2020), pp. 14–16

¹⁵Armed Forces (Special Powers) Act, 1958, §4

¹⁶Amnesty International, *Denied: Failures in Accountability for Human Rights Violations by Security Force Personnel in Jammu and Kashmir*, (2015), pp. 12–14

¹⁷*Extra Judicial Execution Victim Families Association v. Union of India*, (2016) 14 SCC 536

¹⁸National Crime Records Bureau, *Crime in India 2022 Report*, Ministry of Home Affairs, p. 147

¹⁹*Union of India v. K.A. Najeeb*, (2021) 3 SCC 713

constitutional values while being responsive to modern threats. This requires procedural reform, specialized legal training, digital evidence admissibility enhancement, and accountability mechanisms for investigative agencies.

Emergence of Cyber-Terrorism and India's Digital Vulnerability

The 21st century has not only redefined the modalities of terrorism but also revolutionized its mediums. Terrorism has moved from guerrilla warfare in forests and mountainous terrains to coded communication across social media channels, dark web marketplaces, and encrypted virtual chat rooms. In India, the emergence of cyber-terrorism and digital radicalization has added an alarming dimension to national security. Unlike conventional terrorism, which is often identifiable through physical movements, border crossings, or weapons trade, cyber-terrorism is invisible, instantaneous, and borderless. The digital space has become a recruitment ground, propaganda engine, and even a battlefield where data theft, misinformation, and psychological warfare are deployed to weaken the internal fabric of the nation²⁰. From anonymous threats on Telegram channels to radical content shared on WhatsApp groups in Kerala and Kashmir, the proliferation of cyber-radicalization among Indian youth poses a structural threat that existing legal systems are not adequately equipped to handle²¹.

The legal tools available in India to counter cyber-terrorism are outdated and fragmented. The Information Technology Act, 2000, though pioneering in its time, was enacted before the digital revolution fully bloomed. It defines cyber-terrorism under Section 66F, which criminalizes acts intending to threaten the unity, integrity, security, or sovereignty of India through computer resources²². However, this section is narrow in scope and lacks clarity on preventive policing, digital evidence standards, and transnational data cooperation. Moreover, its application is limited by jurisdictional challenges, especially when servers are hosted abroad or perpetrators operate from foreign soil²³. There is no dedicated legislation that comprehensively deals with digital radicalization, algorithmic hate speech, or use of virtual private networks (VPNs) for terror operations.

²⁰ Vinay Kaura, "Cyber Terrorism and India's Security Architecture," *Journal of Defence Studies*, Vol. 15, No. 1 (2021), pp. 5–9

²¹ Praveen Swami, "Islamic State and the Digital Caliphate: India's Challenge," *The Hindu*, March 17, 2023

²² Information Technology Act, 2000, § 66F

²³ Apar Gupta, "Reforming the IT Act in the Era of Cyber Terror," *Indian Journal of Law and Technology*, Vol. 16 (2020), p. 92

The digital radicalization that led to the formation of IS modules in Kerala or the lone-wolf attackers in Delhi and Maharashtra highlights a failure not just of technology, but of policy, policing, and education²⁴. Platforms such as YouTube, Instagram, and anonymous forums on Reddit have become vectors for ideological indoctrination. Yet, India lacks a robust mechanism to monitor and moderate such content without infringing upon the right to free speech under Article 19(1)(a)²⁵. The Supreme Court's landmark judgment in *K.S. Puttaswamy v. Union of India* (2017) elevated privacy to the status of a fundamental right under Article 21. Consequently, any state surveillance, even if justified on grounds of national security, must now pass the tests of legality, necessity, and proportionality²⁶.

This has complicated the task of intelligence agencies that often require real-time interception capabilities, especially during high-risk threats. The debate on surveillance versus privacy intensified after the Pegasus spyware revelations, where prominent journalists, activists, and political figures were allegedly targeted through sophisticated malware. While the government denied unlawful surveillance, the absence of a statutory data protection framework left citizens vulnerable²⁷.

Despite several draft bills and reports, India still awaits a comprehensive personal data protection law. The proposed **Digital India Act**, expected to replace the IT Act, must integrate terrorism-related digital threats, especially in areas of content moderation, encrypted communications, and AI-based monitoring²⁸. There is also a pressing need for capacity building in digital forensics, ethical hacking, and counter-algorithmic techniques among law enforcement agencies. Without such reforms, even the most stringent laws will remain ineffective in preventing cyberterrorist attacks.

India must also navigate international cooperation more effectively. Terrorist outfits often operate through transnational channels, using cryptocurrencies, anonymous browsers, and foreign-based sympathizers²⁹. Mutual Legal Assistance Treaties (MLATs) are cumbersome and slow, and India's limited influence over global tech giants impairs its ability to demand

²⁴ National Investigation Agency, "Case Reports on ISIS Modules in India," NIA Annual Digest 2022, p. 28

²⁵ The Constitution of India, Art. 19(1)(a)

²⁶ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1

²⁷ Amnesty International and The Wire, Pegasus Project: Global Investigation into Targeted Surveillance, July 2021

²⁸ Ministry of Electronics and IT, Government of India, "Digital India Act 2023 (Draft White Paper)," December 2023

²⁹ Sandhya Devanathan, "Cryptocurrency and the Terror Finance Nexus," Indian Express, April 2, 2024

timely access to data. The European Union's *General Data Protection Regulation (GDPR)* and the United States' *CLOUD Act* serve as examples of balancing data protection with law enforcement. India must negotiate its own sovereign framework in line with constitutional values and national interests³⁰.

The digital battlefield is not a mere extension of physical warfare—it is its most volatile and invasive form. The ideological seeds of terrorism are now sown through memes, tweets, and hashtags, often cloaked under the guise of freedom. A nuanced, legally fortified, and technologically agile framework is essential to counter these threats. Without it, India's national security remains exposed not only to external enemies but also to internal digital contagions that rot the spirit of unity from within.

India's Counter-Terrorism Strategy—Institutional, Intelligence, and Global Dimensions

India's battle against terrorism is as much a struggle of intelligence and strategy as it is of legislation. Over the past two decades, the country has progressively fortified its counter-terrorism architecture through a combination of institutional reforms, centralization of investigative agencies, and international collaboration. However, this architecture is still marred by a lack of coordination, bureaucratic inertia, and structural asymmetries between central and state authorities. At the heart of India's counter-terrorism operations lie agencies like the Intelligence Bureau (IB), Research and Analysis Wing (R&AW), National Investigation Agency (NIA), National Technical Research Organisation (NTRO), and the National Security Guard (NSG)³¹. Each has specific roles, yet the absence of a unified national intelligence doctrine continues to hinder seamless cooperation.

The Intelligence Bureau, functioning under the Ministry of Home Affairs, is tasked with internal intelligence gathering and counter-intelligence³². While it has served as India's oldest and most important domestic intelligence body, it suffers from outdated surveillance techniques, lack of transparency, and political influence. R&AW, India's external intelligence agency, modeled loosely on the lines of the CIA and Mossad, has seen notable successes in cross-border surveillance, particularly in surgical strikes and drone tracking.³³ Yet, the absence

³⁰Sandhya Devanathan, "Cryptocurrency and the Terror Finance Nexus," Indian Express, April 2, 2024

³¹Ministry of Home Affairs, Manual of Security Agencies in India, 2022 Edition, p. 43

³²A.S. Dulat, Kashmir: The Vajpayee Years (New Delhi: HarperCollins, 2015), p. 102

³³B. Raman, The Kaoboy of R&AW (New Delhi: Lancer Publishers, 2007), pp. 64–70

of parliamentary oversight over R&AW operations remains a glaring gap in a constitutional democracy.

Similarly, NTRO, responsible for technical surveillance, has been instrumental in intercepting satellite communications and cyber operations³⁴. However, its coordination with state police departments is almost negligible. The National Investigation Agency (NIA), established under the NIA Act, 2008, was envisioned to be India's apex terror-investigation body. It has been granted powers to investigate terror offences across India without prior consent of states—a provision that has sparked federal tensions³⁵. While NIA has achieved breakthroughs in high-profile cases, delays in trial and a lack of adequate regional presence undermine its national reach³⁶.

At a broader level, India's counter-terrorism strategy has struggled with the "silo problem"—where information is hoarded by agencies and not shared across platforms in real time. The establishment of the National Intelligence Grid (NATGRID) aimed to resolve this issue by integrating data from 21 agencies including banks, airlines, and police systems³⁷. However, implementation delays and data privacy concerns have slowed its rollout.

The global dimension of India's counter-terrorism approach has seen significant evolution. India has increasingly aligned itself with global counter-terrorism initiatives, especially through organizations like the Financial Action Task Force (FATF), INTERPOL, and the United Nations Counter-Terrorism Committee³⁸. India has persistently lobbied for the Comprehensive Convention on International Terrorism (CCIT), a global Indian-led effort to define and outlaw terrorism universally³⁹. However, the lack of global consensus—especially from countries differentiating between "freedom fighters" and "terrorists"—has stalled its adoption.

Extradition of terror suspects is another challenge. Although India has signed treaties with over 45 countries, extradition processes are delayed due to weak evidence, dual criminality clauses,

³⁴ National Security Council Secretariat, "Technical Surveillance Framework in India," NSCS Paper Series, Vol. 5, No. 2 (2021), p. 6

³⁵ National Investigation Agency Act, 2008, §6(5)

³⁶ Suhas Chakma, "The Inefficiency of India's Terror Courts," *South Asia Human Rights Monitor*, Vol. 8, Issue 3 (2023), pp. 12–15

³⁷ Nidhi Razdan, "NATGRID and India's Security Future," *India Today*, March 12, 2022

³⁸ Ministry of External Affairs, *India's FATF Compliance Report*, 2023, p. 9

³⁹ United Nations Counter-Terrorism Committee, "India's Proposal on the CCIT," CTC Reports Archive, 2023

or political asylum⁴⁰. The case of David Headley—despite his confession and role in the 26/11 attacks—is an example of India’s limited legal access due to U.S. jurisdiction⁴¹. To counter such barriers, India must insert fast-track clauses in its treaties, backed by strategic intelligence partnerships.

Regionally, SAARC remains ineffective due to Pakistan’s obstruction, but BIMSTEC has emerged as a promising alternative. Through coordinated military exercises and cyber-security dialogues, India has engaged constructively with Bangladesh, Nepal, and Myanmar⁴². Counter-terrorism cooperation with Israel, France, and Australia has also advanced, particularly in cyber-threat mapping and naval security⁴³.

Globally, examples like Israel’s pre-emptive security doctrine, France’s de-radicalization campaigns, and the U.S. PATRIOT Act provide varied lessons⁴⁴. While India must draw from their tactical strengths, it must carefully adapt them to its democratic, multicultural, and constitutional ethos. What India needs is not a security state—but a secure democracy.

The Way Forward—A Democratic and Defensible National Security Model

As India stands on the threshold of global leadership amid a volatile international order, the urgency to recalibrate its national security paradigm cannot be overstated. The country can no longer afford to view terrorism solely through the lens of violence and retaliation; it must approach it as a multifaceted challenge that attacks the nation's sovereignty, disrupts its social cohesion, exploits its legal grey zones, and undermines its democratic institutions. The current landscape demands the articulation and implementation of a comprehensive *National Security Doctrine 2.0*, a doctrine that is not only operationally robust and technologically advanced but also rooted in constitutional morality, human dignity, and institutional accountability⁴⁵.

Such a doctrine must begin with the codification of a formal national security policy—a strategic blueprint ratified by Parliament that delineates the responsibilities of each security

⁴⁰ K.P.S. Gill, “Extradition and International Obstacles in Terrorism Prosecution,” *Indian Police Journal*, Vol. 70, No. 4 (2022), p. 23

⁴¹ Praveen Swami, “David Headley and the Jurisdictional Maze,” *Frontline*, Vol. 36, Issue 5 (2021), p. 14

⁴² BIMSTEC Secretariat, “Joint Military Exercise: MILEX-II Outcomes,” Official Statement, November 2023

⁴³ Ministry of Defence, “India-Israel Defence Cooperation Report,” MoD Annual Report 2024, pp. 55–58

⁴⁴ Suhas Chakma, “The Inefficiency of India’s Terror Courts,” *South Asia Human Rights Monitor*, Vol. 8, Issue 3 (2023), pp. 12–15

⁴⁵ Ajai Sahni, “Why India Needs a National Security Doctrine,” *South Asia Intelligence Review*, Vol. 20, No. 1 (2022), pp. 2–3

agency, the protocols for inter-agency data sharing, the standards for surveillance, and the frameworks for judicial oversight⁴⁶. A centralized *National Counter-Terrorism Authority (NCTA)*, akin to models in the U.K. or Australia, can help resolve India's silo-based intelligence infrastructure⁴⁷.

Legal reforms must walk hand in hand. India's anti-terror laws must be refined not through blanket criminalization, but through precise procedural safeguards. As held in *Maneka Gandhi v. Union of India*, the "procedure established by law" must be just, fair, and reasonable⁴⁸. Time-bound investigation, digitized FIR systems, forensic-ready evidence procedures, and AI-powered suspect profiling should become the norm.⁴⁹ A specialized cadre of judicial officers, trained in anti-terror law and cyber jurisprudence, is essential to ensure expedited and just trials. Laws like the UAPA should be periodically reviewed by a bipartisan parliamentary committee and subject to judicial scrutiny to prevent executive overreach⁵⁰.

The ethical question of surveillance, amplified in the digital era, also demands attention. The *Pegasus spyware controversy* showed that national security must not be weaponized to suppress democratic dissent⁵¹. India needs a **Security Oversight Ombudsman**—independent of the executive—with power to audit, investigate, and report on surveillance orders under the new *Digital India Act*, expected to replace the IT Act, 2000⁵².

Terrorism cannot be fought only through weapons or codes—it must also be countered with ideas, education, and civic consciousness. Counter-radicalization strategies must focus on ideological inoculation at the grassroots. Programs in schools and colleges that promote constitutional patriotism, digital hygiene, and critical thinking must replace the vacuum in which extremist ideologies flourish⁵³. Youth de-radicalization programs, rehabilitation initiatives for returnees from terror networks, and digital literacy missions must become cornerstones of the new security doctrine.

⁴⁶National Security Advisory Board, "*Recommendations for National Security Policy*," NSAB Report (2023), p. 11

⁴⁷Ministry of Home Affairs, Government of India, "*Draft Proposal for NCTA*," Internal Document, 2024

⁴⁸*Maneka Gandhi v. Union of India*, AIR 1978 SC 597

⁴⁹Arghya Sengupta, *Due Process and the Rule of Law in India* (Oxford: OUP, 2021), pp. 91–94

⁵⁰Lok Sabha Secretariat, "*Report of the Standing Committee on Home Affairs on the UAPA (2023)*," p. 22

⁵¹The Wire and Amnesty International, *Pegasus Project: India Report*, August 2021

⁵²Ministry of Electronics and IT, "*Draft Digital India Act 2023*," Government of India

⁵³Seema Sirohi, "*De-Radicalizing India's Youth*," *India Foundation Journal*, Vol. 9, No. 1 (2023), pp. 29–33

Internationally, India must step up as a normative leader against terrorism. Pushing for the CCIT with renewed diplomatic vigor, expanding intelligence-sharing arrangements with QUAD and BIMSTEC partners, and seeking fast-track extradition protocols with allies like the UAE, France, and Israel must remain top priorities⁵⁴. Maritime and cyber cooperation with Australia and the U.S. under the QUAD framework can also pre-empt new forms of asymmetric warfare⁵⁵.

Above all, the idea of Bharat must remain central. National security in a democracy cannot be secured by compromising the very freedoms it seeks to protect. Terrorism challenges not just our territorial sovereignty but the spirit of our constitutional republic. Our response must be rooted in courage, but also in compassion; in strength, but also in justice.

Conclusion

India's journey in combating terrorism is long, painful, and ongoing. From the bloodshed of 26/11 to the ambushes in Pahalgam, from the encryption cells of Kerala to drone attacks in Jammu, the nation has endured repeated wounds and yet remained resilient. But resilience must now give way to reform. This paper has argued that India's current legal and strategic framework is fragmented and reactive. A forward-looking, democratic, and constitutionally robust national security model is urgently needed—one that leverages technology, upholds human dignity, and ensures operational accountability.

The time has come for India to rise not just as a powerful nation, but as a just one. Terrorism will test our strength; let our response be a testimony of our values. Let our Constitution—not coercion—be the shield that guards the soul of Bharat.

⁵⁴United Nations, "CCIT Negotiations and India's Role," UNGA Documents, 2023

⁵⁵ Ministry of External Affairs, "QUAD Joint Statement on Counter-Terrorism Cooperation," May 2024