E-ISSN: 2664-603X
P-ISSN: 2664-6021
Impact Factor (RJIF): 5.92
IJPSG 2025; 7(10): 152-156
www.journalofpoliticalscience.com
Received: 16-08-2025
Accepted: 19-09-2025

Satyabrata Behera
Lecturer in Political Science
Lokanath Mohavidyalaya,
Kendrapara, Odisha, India

Corresponding Author:
Satyabrata Behera
Lecturer in Political Science
Lokanath Mohavidyalaya,
Kendrapara, Odisha, India

India's role in counter terrorism: Strategic opportunities and challenges

Satyabrata Behera

DOI: https://www.doi.org/10.33545/26646021.2025.v7.i10b.719

Abstract
India's counter-terrorism trajectory has been shaped by its strategic location, complex socio-political environment, and decades of exposure to diverse forms of violence, including cross-border terrorism, insurgencies, and radicalization. High-profile incidents such as the 2001 Parliament attack, the 2008 Mumbai attacks, and the 2019 Pulwama bombing exposed systemic vulnerabilities and compelled reforms in legislation, intelligence coordination, and institutional frameworks. More recently, the 2023 Rajouri and 2025 Pahalgam attacks underscore the evolving nature of terrorist threats. In response, India has developed a multidimensional strategy that integrates hard power through specialized forces, intelligence modernization, and robust legal frameworks with soft approaches such as community engagement, de-radicalization, and socioeconomic inclusion. At the international level, India actively contributes to global counter-terrorism initiatives through the United Nations, FATF, and bilateral partnerships. Despite these advances, persistent challenges remain, including inter-agency coordination gaps, exploitation of digital technologies by terrorist groups, and the volatility of regional geopolitics. This study argues that India's counter-terrorism framework demonstrates resilience and adaptability by blending global best practices with indigenous solutions. The analysis highlights that India's experience offers lessons not only for national security but also for shaping international counter-terrorism cooperation in the 21st century.

Keywords: Counter-terrorism, Insurgency, National Intelligence Grid (NATGRID), South Asia Security, Radicalization, community engagement, technological innovation, cybersecurity

Introduction
Terrorism has, over the years, grown into one of the most pressing challenges confronting India. The country's geography at the heart of South Asia, its diverse society, and its layered political realities have made it vulnerable to multiple forms of violence, including cross-border militancy, regional insurgencies, and left-wing extremism (Kalyanaraman, 2014) [6]. The harsh reality of this threat has been underscored time and again by devastating attacks that left a lasting mark on the nation's collective memory. From the 1993 Mumbai serial bombings, which exposed the scale of organized urban terrorism, to the 2001 assault on the Indian Parliament that struck at the symbolic core of democracy, and the 2008 Mumbai siege which unfolded live on global television, India has witnessed terror in its most brutal forms. More recent incidents such as the 2016 Uri attack, the 2019 Pulwama tragedy, and the Pahalgam attack have reinforced the fact that terrorism in India continues to evolve, adopting new tactics and technologies to challenge the state. These incidents were not isolated episodes of violence but turning points that exposed systemic gaps in security, governance, and intelligence coordination, compelling wide-ranging reforms in legislation and institutional frameworks.

In response to this persistent threat, India has developed a counter-terrorism strategy that is both comprehensive and adaptive. It combines hard power through stringent laws like the Unlawful Activities (Prevention) Act (UAPA), the strengthening of specialized forces such as the National Security Guard (NSG), and the modernization of intelligence capabilities with softer measures that aim to address the underlying causes of extremism. Initiatives in development, education, and community engagement have been employed to reduce the appeal of radical ideologies and build resilience within vulnerable populations.

At the international level, India has taken an increasingly proactive role in shaping global counter-terrorism norms, consistently calling for stronger cooperation at forums such as the United Nations and the Financial Action Task Force (FATF). By pressing for tighter controls on terror financing, deeper intelligence sharing, and a universal definition of terrorism, India has positioned itself as both a victim of terror and a leading advocate for stronger international responses.Yet, despite these efforts, the challenges remain deeply entrenched. Terrorist groups continue to adapt, using encrypted communication, cyber-radicalization, and even drone technology to widen their reach. Cross-border terrorism, often abetted by state sponsorship, persists as a formidable obstacle, while inter-agency gaps within India's security architecture occasionally undermine coordination (Staniland, 2014) [11]. These realities underscore the fact that terrorism in India is not merely a domestic law-and-order concern but one deeply embedded in regional geopolitics. The continuing struggle has made India's counter-terrorism experience significant not only for its own national security but also for the global community, offering lessons in resilience, adaptation, and the urgent need for collective international action.

Historical Context

India's counter-terrorism efforts began taking shape in the late 20th century, when domestic insurgencies and cross-border threats started to converge, creating a complex security environment. The insurgency in Punjab during the 1980s and the escalation of violence in Kashmir toward the end of that decade marked the beginning of a prolonged struggle against militancy. What started as regional unrest soon evolved into a larger challenge, as external support to militant groups in Kashmir made the conflict even more volatile and enduring.

The 1990s were a turning point. The devastating 1993 Mumbai serial bombings shocked the nation and signalled the arrival of organized, cross-border-backed terrorism in India's cities. This period saw the rise of groups like Lashkar-e-Taiba and Jaish-e-Mohammed, whose reach and sophistication demanded stronger intelligence networks and tougher legal measures.

The December 2001 Parliament attack was another watershed moment. By striking at the heart of Indian democracy, it revealed serious gaps in preparedness and forced the government to strengthen its laws and security institutions. Only a year later, in 2002, militants targeted the Akshardham Temple in Gujarat, killing dozens of civilians. The attack underscored the vulnerability of public spaces and the urgent need for rapid-response forces to protect them.

Urban centres remained frequent targets. The 2005 Delhi market blasts during the festive season, the 2006 Mumbai train bombings that claimed over 180 lives, and the Jaipur and Delhi blasts of 2008 all highlighted how easily terror could exploit crowded cities. But nothing had the same impact as the November 2008 Mumbai attacks. For three days, the world watched as armed militants laid siege to India's financial capital. The scale and coordination of the attack exposed deep flaws in coastal and urban security, leading to sweeping reforms including the creation of the National Investigation Agency and the strengthening of intelligence-sharing mechanisms. The following decade continued to test India's resilience. The 2010 Pune German Bakery blast and the 2011 Mumbai serial blasts underscored the rise of homegrown networks like the Indian Mujahideen. In 2013, Hyderabad and Patna witnessed deadly explosions, including one aimed at a political rally revealing how terrorism was being used to target democratic processes. Meanwhile, militancy in Kashmir remained intense, with repeated strikes on army camps and civilians through 2014 and 2015.

By 2016, India's response had shifted. The Pathankot Airbase attack exposed vulnerabilities in protecting critical infrastructure, but the Uri attack later that year triggered "surgical strikes" across the Line of Control a bold move that signaled a more offensive approach. This trend continued in 2019, when the Pulwama suicide bombing killed 40 CRPF personnel. India's retaliation through the Balakot airstrikes not only marked a military escalation but also reshaped diplomatic conversations with Pakistan and the wider international community.

Even in recent years, terrorism has not relented. The 2023 Rajouri attacks and the 2025 Pahalgam incident are stark reminders that the threat remains persistent and adaptive. These newer episodes highlight how militants continue to exploit infiltration routes and evolve their tactics, keeping security forces on constant alert.

Alongside domestic efforts, India has steadily expanded its international cooperation. Over time, it has deepened partnerships with the United States, Israel, and Russia, while also engaging with global platforms like the United Nations, the Financial Action Task Force (FATF), and the Global Counter-Terrorism Forum. These collaborations reflect India's recognition that terrorism is a transnational challenge that no country can tackle alone.

From Punjab in the 1980s to Pahalgam in 2025, India's counter-terrorism journey has been shaped by painful lessons, institutional reforms, and evolving strategies. Each attack left scars but also pushed the nation to adapt, ensuring that its fight against terrorism remains both a national priority and a contribution to the global struggle against violent extremism.

Key Strategies

India's counter-terrorism strategy is multidimensional, combining intelligence gathering, international cooperation, technological innovation, community engagement, and robust legal measures.

- **Intelligence Gathering and Analysis:** India has steadily expanded its intelligence capabilities, integrating both human intelligence (HUMINT) and signals intelligence (SIGINT). HUMINT plays a vital role in uncovering sleeper cells, radical networks, and planned attacks, while SIGINT and cyber-intelligence track digital communications and online activities of terrorist groups (Ghosh, 2017) [3]. To enhance preparedness, India increasingly employs predictive analysis, artificial intelligence, and risk assessment tools. These methods enable security agencies to forecast potential threats and identify high-risk individuals and regions (Bajpai, 2020) [1]. However, effective intelligence requires seamless coordination among agencies such as RAW, IB, and the NIA, a challenge India continues to refine.
- **International Cooperation:** Recognizing the transnational nature of terrorism, India has prioritized international collaboration. It has entered into bilateral

agreements with key partners such as the United States, Russia, and Israel, focusing on intelligence sharing, counter-terrorism training, and technology transfer (Pant, 2016) [15]. At the multilateral level, India actively participates in the United Nations' counter-terrorism bodies, the FATF, and the Global Counter-Terrorism Forum. Regionally, India engages through SAARC and BIMSTEC frameworks to combat cross-border terrorism (Singh, 2018) [10].

- **Use of Technology:** India has increasingly leveraged advanced technologies in counter-terrorism. Surveillance tools such as satellite imagery, drones, and biometric systems strengthen border and urban security, while AI-driven analytics and big data help in detecting patterns of terrorist activity (Sharma, 2019) [9]. Additionally, India has prioritized cybersecurity to safeguard critical infrastructure and conducts offensive cyber operations to disrupt terrorist networks online (Banerjee, 2021) [2].
- **Community Engagement and De-radicalization:** India recognizes that counter-terrorism cannot rely solely on hard power. Community-based strategies focus on trust-building, addressing grievances, and preventing radicalization. Dialogue platforms, community policing, and educational programs promoting critical thinking are used to counter extremist narratives (Chatterjee, 2018) [4]. De-radicalization programs emphasize psychosocial support, vocational training, and reintegration of individuals disengaging from extremist groups. These measures align with best practices in countries like the UK and Canada, underscoring the importance of early intervention and community trust (Neumann, 2013) [7].
- **Legal and Policy Measures:** India's legal architecture against terrorism has been significantly strengthened. Laws such as the UAPA and the establishment of fast-track special courts ensure the swift prosecution of terrorism-related cases (Jayaram, 2020) [5]. Preventive detention provisions and asset-freezing mechanisms allow authorities to neutralize threats and dismantle terror financing networks. At the policy level, India has introduced stricter financial regulations, compliance with FATF norms, and cybersecurity frameworks aimed at monitoring online radicalization and preventing the misuse of non-profit organizations for terrorist funding (Gupta, 2016) [4].

India's Unique Approach to Tackle Terrorism

India's counter-terrorism strategies are not only comprehensive but also tailored to its unique threat environment. Unlike many countries that face isolated threats, India has had to contend simultaneously with cross-border militancy, home-grown radicalization, and insurgencies in diverse regions. This has compelled the country to build a multi-layered approach that combines lessons from its past with global best practices.

- **Intelligence Integration:** A central feature of India's unique approach is the emphasis on integrated intelligence. The creation of platforms such as the National Intelligence Grid (NATGRID) reflects efforts to bridge the gaps exposed by incidents like the 2008 Mumbai attacks. This integration mirrors practices in countries like the United States, yet India's system has been designed to address its vast internal security challenges across multiple states and languages.
- **Specialized Counter-Terrorism Units:** India has developed specialized forces such as the National Security Guard (NSG) and region-specific teams like the CRPF Valley Quick Action Team in Kashmir. Their focus on rapid deployment in both urban and insurgency-prone regions reflects India's dual need to counter large-scale urban assaults, such as those in Mumbai, and persistent militancy in Border States. This model is comparable to Israel's elite counter-terrorism units but is uniquely adapted to India's demographic and geographic scale.
- **Community engagement and Deradicalisation:** Recognizing that hard power alone cannot defeat terrorism, India has emphasized community outreach. Educational initiatives, vocational training, and local dialogue programs are increasingly being used to prevent radicalization, a lesson reinforced by urban attacks in Delhi and Hyderabad. While similar to programs in the UK and Canada, India's approach places stronger emphasis on socio-economic inclusion as a long-term stabilizer in vulnerable regions.
- **Technological Integration:** India has also leveraged technology to strengthen surveillance, border management, and predictive analytics. From the deployment of drones and biometric systems to AI-driven threat analysis, these tools have been integrated into counter-terrorism operations. The focus on securing critical infrastructure after the Pathankot and Uri attacks demonstrates India's resolve to adapt technology to specific vulnerabilities, rather than relying solely on imported models.

Taken together, India's unique approach lies in blending global best practices with indigenous solutions. By learning from its history from the Mumbai 2008 attacks to Pulwama in 2019 and the recent Pahalgam incident India has created a counter-terrorism framework that is both adaptive and context-specific. Its strategies underscore that counter-terrorism in India is not just about force but about resilience, integration, and community partnership.

Challenges

Despite significant progress, India's counter-terrorism framework continues to face persistent and evolving challenges. These span institutional weaknesses, cross-border dynamics, technological vulnerabilities, and broader socio-political pressures.

- **Internal Challenges:** One of the greatest hurdles remains the coordination between multiple agencies. Overlapping mandates between national bodies such as the NIA, IB, and RAW, and state police forces often result in duplication of effort or delays in operational response. This was evident during high-profile incidents such as the 2008 Mumbai attacks and the 2016 Pathankot assault, where gaps in information-sharing slowed immediate responses. Political interference and bureaucratic red tape further complicate long-term policy implementation. Additionally, resource limitations particularly in manpower, modern equipment, and training remain acute in rural and border regions, leaving vulnerabilities that militants frequently exploit.
- **External Challenges:** Cross-border terrorism continues

to be India's most pressing external challenge. Groups based in Pakistan, including Lashkar-e-Taiba and Jaish-e-Mohammed, have demonstrated their ability to orchestrate major attacks such as the 2016 Uri strike and the 2019 Pulwama bombing. Infiltration across the Line of Control remains a persistent threat, as underscored by the recent Rajouri and Pahalgam incidents. At the global level, geopolitical rivalries and the lack of consensus on the definition of terrorism often hinder India's ability to build unified international responses (Pant, 2016) [8].

- **Technological Challenges:** The rapid growth of digital infrastructure has created new vulnerabilities. Terrorist organizations increasingly exploit encrypted communication platforms, social media, and cryptocurrencies to plan operations, recruit followers, and finance networks. Drone-based infiltration and attacks have also emerged as a new frontier, adding another layer of complexity to border security. At the same time, while India expands surveillance and digital monitoring, it faces the delicate task of protecting civil liberties and maintaining democratic accountability.
- **Socio-Political Challenges:** Terrorism in India is not only a matter of security but also of social cohesion. Radicalization often feeds on unresolved grievances, marginalization, and communal tensions. Preventing extremist recruitment requires more than military operations; it requires inclusive governance, grassroots engagement, and community trust-building. Striking the right balance between hard security measures and soft approaches remains a continuing challenge.

Recommendations

Policy Recommendations

India's evolving security environment calls for reforms that go beyond reactive measures. A first priority is strengthening intelligence integration by ensuring that national and state-level agencies share information in real time. Many of the urban attacks such as those in Mumbai, Delhi, and Hyderabad exposed gaps in surveillance and coordination that can be bridged through technology-driven platforms. Legal frameworks must also keep pace with modern threats. Expanding existing laws to cover cyber-terrorism, drone-based infiltration, and financial transactions through cryptocurrencies is essential to stay ahead of adversaries.

Equally important is enhancing the protection of critical infrastructure. Attacks on transport systems and military bases, from the 2006 Mumbai train bombings to Pathankot in 2016, revealed the need for layered defenses, advanced monitoring, and rapid-response mechanisms. At the same time, counter-terrorism cannot rely solely on hard power. Educational, vocational, and psychosocial initiatives aimed at vulnerable populations are vital to prevent recruitment and radicalization. Finally, strengthening border management with smart fencing, drone surveillance, and biometric systems will help address persistent infiltration along the Line of Control.

Implementation Strategies

For any reform to succeed, implementation must be phased and accountable. New programs can be piloted in high-risk areas such as Jammu and Kashmir before being expanded nationwide. Specialized task forces dedicated to cyber defense, drone warfare, and financial intelligence will help meet emerging challenges. Regular training and joint exercises both domestic and international are critical to ensure readiness against large-scale urban attacks. Equally, independent oversight mechanisms should be strengthened to ensure that counter-terrorism measures remain transparent and consistent with democratic freedoms.

Technology must be leveraged responsibly. Artificial intelligence, data analytics, and blockchain-based tools offer enormous potential for detecting threats and tracking illicit financing. However, these must be deployed with safeguards that protect privacy and prevent misuse.

Best Practices and Lessons Learned

India's experience over the last two decades offers several lessons. Urban centers remain vulnerable and require multi-layered security combining surveillance, rapid-response units, and effective emergency communication systems. Post-attack reviews must become institutionalized, with every major incident feeding directly into reforms rather than being treated as isolated crises. International cooperation should also be deepened, not only for intelligence sharing but also for training, technology transfer, and coordinated responses to transnational terrorism.

Finally, community engagement is indispensable. Counter-radicalization efforts are most effective when they involve civil society, local leaders, and grassroots organizations that can build trust and resilience. By combining hard security measures with community-driven approaches, India can create a more balanced and sustainable counter-terrorism framework.

Conclusion

India's role in counter-terrorism has evolved through a long and complex trajectory, shaped by insurgencies of the 1980s, the devastating cross-border attacks of the 1990s, and watershed moments such as the 2001 Parliament attack and the 2002 Akshardham temple attack. The 2006 Mumbai train bombings, the 2008 Jaipur and Delhi blasts, and the 2008 Mumbai attacks highlighted severe gaps in India's security infrastructure and drove major institutional reforms, including the establishment of the National Investigation Agency (NIA).

The following decade underscored the persistence of terrorism, with incidents such as the 2010 Pune blast, 2011 Mumbai serial blasts, 2013 Hyderabad and Patna explosions, and recurring militant strikes in Kashmir. High-profile attacks at Pathankot and Uri in 2016 further signaled the evolving tactics of militant groups and prompted India to adopt a more proactive, offensive counter-terrorism stance. The Pulwama attack in 2019 marked another turning point, leading to pre-emptive military responses and a decisive shift in India's diplomatic posture against cross-border terrorism. More recently, the 2023 Rajouri and 2025 Pahalgam attacks demonstrate that terrorism in India remains a dynamic and persistent challenge requiring constant vigilance.

Today, India's counter-terrorism strategy is multidimensional spanning intelligence integration, international cooperation, technological innovation, community engagement, and robust legal frameworks. Yet, persistent challenges endure, including inter-agency coordination gaps, political and bureaucratic hurdles, the

exploitation of digital technologies by terrorist groups, and the volatility of the regional security environment.

Nevertheless, India's trajectory demonstrates resilience and adaptability. By continuously reforming its security institutions, expanding international partnerships, and investing in both hard and soft approaches, India has strengthened its counter-terrorism architecture. Looking ahead, India's success will depend on institutionalizing reforms, leveraging technology responsibly, and balancing robust security measures with the preservation of democratic freedoms. The historical record from Punjab and Kashmir insurgencies to the Pahalgam attack underscores that counter-terrorism in India is not a one-time achievement but an ongoing process of adaptation to ever-evolving threats.

References

1. Bajpai K. National security and counter-terrorism in India: emerging challenges. New Delhi: Oxford University Press; 2020.
2. Banerjee S. Countering online extremism in India: technology and policy dimensions. J Cyber Policy. 2021;6(2):189-204.
3. Ghosh S. Intelligence and internal security in India. New Delhi: Sage Publications; 2017.
4. Gupta R. Terror financing and regulatory frameworks in India. Indian J Int Aff. 2016;55(4):221-239.
5. Jayaram M. Law and terrorism in India: the evolving legal framework. Cambridge: Cambridge University Press; 2020.
6. Kalyanaraman S. Counter-terrorism strategy. New Delhi: Institute for Defence Studies and Analyses; 2014.
7. Neumann P. The trouble with radicalization. Int Aff. 2013;89(4):873-893.
8. Pant HV. India's evolving foreign policy: counterterrorism and global cooperation. London: Routledge; 2016.
9. Sharma R. Technology and national security: the Indian approach. Def Stud. 2019;19(1):67-84.
10. Singh A. Regional security cooperation in South Asia: SAARC, BIMSTEC, and counter-terrorism. South Asian Surv. 2018;25(2):145-163.
11. Staniland P. India's counter-terrorism policy against jihadist terror. CTC Sentinel. 2014;7(4):7-11.