International Journal of Humanities Social Science and Management (IJHSSM)
Volume 6, Issue 2, Mar.-Apr., 2026, pp: 410-417 ISSN: 3048-6874
www.ijhssm.org

India Strategic Approach to Cross border Terrorism in South Asia

Aditya Siingh Chauhan

Date of Submission: 01-04-2026 Date of Acceptance: 10-04-2026

Abstract
South Asia is one of the most geopolitically volatile regions globally. This is due to the prolonged rivalry among nations in the region, insurgencies in some of the nations, the prevalence of religious extremism in the area, and the unsettled border disputes. In the past few years, conventional forms of cross-border terrorism have changed in terms of scale, modus operandi, and technology. During the same period, new security risks have emerged in the area. These risks include water insecurity and the weaponization of resources. This study aims to explore the interrelationship that exists among cross-border terrorism, digital radicalization, and water security risks in South Asia. This is done using contemporary analyses of the situation by scholars. The study aims to evaluate the changes that have taken place in the form of terrorism in the area. In the past, the terrorism in the area was conventional militant terrorism. However, the situation is changing as hybrid forms of warfare are being adopted. Additionally, the study aims to evaluate the risks of the use of the water resources of the area, particularly the river systems, being weaponized in the rivalry between India and Pakistan using the strategic competition approach. This study found that the security environment in South Asia is characterized by a security dilemma. This is due to the conventional rivalry among the nations in the area and the unconventional security risks that have emerged in the area.

I. Introduction

South Asia's security landscape has historically been shaped by colonial legacies, partition trauma, territorial disputes, and ideological polarization. Since the mid-twentieth century, the rivalry between India and Pakistan has significantly influenced patterns of militarization, proxy warfare, and regional alignments. Cross-border terrorism has emerged as one of the most persistent destabilizing forces in this environment. In the post-Cold War period, terrorism in South Asia evolved from localized insurgencies to transnationally connected networks. Militant groups operating across borders have exploited porous boundaries, ideological grievances, and state rivalries to sustain violent campaigns. The digital revolution has further transformed the operational dynamics of these groups, allowing recruitment, propaganda dissemination, and financial coordination to transcend geographical limitations. More recently, analysts have warned about the intersection of terrorism with environmental and resource-related vulnerabilities, especially water security. South Asia's dependence on shared river systems—such as those governed under the Indus Waters Treaty—creates a delicate hydropolitical equilibrium. The weaponization of water discourse, infrastructure sabotage, or misinformation campaigns could amplify tensions in an already volatile region.This study situates cross-border terrorism within a broader framework of regional security complexity, incorporating digital transformation

and resource-based vulnerabilities. It seeks to understand how evolving threat landscapes interact with traditional geopolitical rivalries.The South Asian region is part of one of the least stable regional security complexes within the contemporary international system. Since the partition of British India in 1947, this region has witnessed interstate rivalries, territorial disputes, ideological differences, and internal insurgencies. One of the prominent and persistent causes of regional instability is cross-border terrorism. Cross-border terrorism can be described as an act of violence perpetrated by non-state actors who cross state boundaries, often with the support of state actors, to attain particular political, ideological, and strategic objectives. The India-Pakistan rivalry has persistently emerged as a major factor that influences the contours of cross-border terrorism. The Kashmir conflict has played an important role in sustaining interstate rivalry and has acted as an ideological divide. For decades, terrorist groups have used this conflict to fuel cross-border terrorism by utilizing political differences, porous borders, and shifting geopolitical alignments. Cross-border terrorism is traditionally regarded as an extension of proxy war. However, recent events suggest that this phenomenon has witnessed a structural shift. The digital revolution has impacted cross-border

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 6, Issue 2, Mar.-Apr., 2026, pp: 410-417 ISSN: 3048-6874
www.ijhssm.org

terrorism on both operational and ideological grounds. The emergence of online platforms has led to an environment where terrorist groups can engage in recruitment, indoctrination, fundraising, and operational planning. The spread of extremist narratives has become more prevalent than ever. The emergence of encrypted communication tools and cryptocurrencies has further confused state-centric counter-terrorism strategies.In this context that the current security situation in South Asia can be best understood not in terms of individual lenses such as terrorism, digital radicalization, and water politics, but rather in a holistic manner that recognizes their interlinked nature. The current research argues that the intersection of issues such as cross-border terrorism, digitalization, and hydropolitics creates a complex security dilemma that conventional deterrence theories fail to address.

Research Objectives

- To examine the evolution of cross-border terrorism in South Asia.
- To examine the influence of digital technologies on the mobilization of extremists.
- To examine the water security dimension of regional instability.
- To examine the current counterterrorism cooperation mechanisms.
- To develop policy recommendations for regional stability.

II. Review of the Literature on South Asian Cross-Border Terrorism

The significance of state-sponsored or state-tolerated militant networks has been a recurring theme in scholarly research on cross-border terrorism in South Asia. Analysts contend that unresolved political conflicts, especially those involving Kashmir, are closely linked to terrorism in the area. According to research, militant organizations frequently function in a debatable yet politically significant strategic gray area.

The rivalry between Pakistan and India is a key factor in understanding cross-border militancy, according to studies looking at regional security dynamics. Within the framework of traditional military asymmetry, some academics contend that asymmetric warfare has proven to be a financially advantageous tactic. Others draw attention to the blowback effect, which is the process by which militant networks that were first developed for strategic reasons eventually cause instability at home.

In addition, studies on regional security complexes indicate that the security environment in South Asia is closely interconnected. Perceptions of threat in one state invariably impact decisions about policy in other states, perpetuating cycles of militarized and trust. South Asia appears to be a closely linked security environment, according to research on regional security complexes. Policy actions in other states are invariably influenced by threat perceptions in one state, which feeds militarization and mistrust cycles.

Current academic work focuses on how extremist groups are going digital.

Researchers have noticed that social media, encrypted chats, and online payment methods now support more spread-out group structures. Online propaganda is important for creating group identities, making complaints seem bigger, and getting new members.

Like other scholars, some emphasize state sponsorship variations as indicating that (some) militant groups have historically served as foreign-policy tools. But some other scholars dispute this state-centered interpretation and claim that militant groups frequently acquire independent agendas, at variance with those of their original sponsors.

1. Digital Radicalization and Hybrid Threats

Digital tools have transformed the way terrorism operates all over. In South Asia, the internet assists disseminate radical. Concepts, discover fresh participants, get funds, and organize assaults. Once, instead of large organizations with leaders, today's fanatical teams. Are frequently miniature, spread-out teams that communicate covertly on the internet.

Hybrid warfare has emerged as one concept trying to describe these changes. Characterised by the use of conventional techniques blended with cyber attacks, information operations and other measures such as psychological warfare, grievances are exaggerated through online propaganda campaigns which seek to drive the public narrative and sow discord. Online algorithms frequently boost radical voices to greater visibility.

Research on online extremism is still emerging. Regional studies, particularly those focused on South Asia, are limited with several analysing countries in the MiddlleEast.

2. Evolution of Cross Border terrorism

In South Asia, cross-border terrorism has not been a phenomenology that just stayed the same. It has been changing in the last few decades due to the changes in the political sphere, technological advances, and developments among the global extremists. Although the geographical lines of South

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 6, Issue 2, Mar.-Apr., 2026, pp: 410-417 ISSN: 3048-6874
www.ijhssm.org

Asia have not changed, modalities, instruments and strategic reasoning of terrorist activity have been reflexive to more general changes in the technology and governance.

This part will trace the path of technological evolution of the post-colonial insurgencies in the early years to digitally facilitated hybrid threats and finally explain that South Asian terrorism has kept up with the evolution of communication technologies, weaponry, and global connectivity**.**

i. **Post-Colonial Insurgency (1947 – 1980s)**

Right after the decolonization, the emergence of transnational terrorism in South Asia was literally a by-product of the fact that the past colonial borders remained on the map but no one could guess where they exactly ended. The British India partition was simply a haphazard piece of land and bang, new boundaries, displaced persons, emotional tensions on a large scale. Much of the preliminary mayhem was regarding armed infiltration particularly in Jammu and Kashmir where that was simply the order of the day. The terrorist groups were largely concerned with the acquisition of territory, and most of them were predominantly locally focused. They traversed the mountains, received the assistance of locals, and possessed the most basic communication equipment.

It was as primitive technologically as it could be. The small arms and homemade explosives that the militants also used and even analog radios were used. Couriers were made or they would meet face-to-face and therefore, all was slow and local. No advanced surveillance equipment was available to enhance border crossings, therefore, they had to rely on a bare minimum, yet it served. Succinctly, it is a time of savage physical assaults, near absence of technology and very few international networks.

ii. Proxy Warfare and Military Modernisation (1980- 2001)

The Soviet-Afghan War made the Southern Asian game different. It transformed the region into an ideological networking field, introduced more advanced guns and trained an enormous amount of irregular warriors. The situation changed to frequent insurgencies, systematic proxy wars, and it was all incident to the India-Pakistan rivalry.

It is at this point that the terrorist groups began to acquire modern assault rifles, RPGs, superior explosives, and superior training. They also started transferring money out of the country through hawala system hence they were not starving only on local resources. The communications were also enhanced by the use of radios and satellite phones, and this enabled the coordination of the operations. Operating IEDs became complicated and caused increased deaths and psychological effects.

Tech was beginning to transform the way they were operating but it was not yet completely digital. Communication became better; operations have become more disorganized; logistics chains become larger. They ceased to be the peripheral rebels and more or less cyber-like warriors in a wider geopolitical battle. Militancy was also a political weapon and a terror strategy among the bigger rivalry among states.

iii. From 2001-2010, Jihad globalization and early digital integration have struck.

The 9/11 attacks propelled the cross-boundary terror in South Asia to an international level. Organizations started identifying themselves with the wider jihad discourses. Local issues were put in the context of religion or civilizational issues, which helped in recruiting and legitimizing ideology.

The show was also technology driven, e-mails, internet forums, and the emerging social media were all clogging the usual channels. Coded messaging applications and satellite phones became common. These technological acquisitions enable them to organize faster and propagate propaganda across borders.

Money flows also went global. The money travelled across the boundaries through donors, diaspora organizations and the informal digital channel. These crowds were not confined to the local hideouts to themselves, they also centered on the entire internet. In spite of the fact that infiltration was enormous, digital communication was beginning to transform the way that they organized themselves as well as the way that they propagated their ideas.

iv. Digital radicalization and networked terrorism (2010 -present).

Social media became the primary platform of cross-border terrorism. The process of recruiting, brain-washing and propaganda became almost completely digital. Such sources as Facebook, YouTube, Twitter, WhatsApp, and Telegram allow extremist messages to cross borders without making a physical move. Radicalization does not represent a

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 6, Issue 2, Mar.-Apr., 2026, pp: 410-417 ISSN: 3048-6874
www.ijhssm.org

face-to-face work anymore, but rather it is pushed through the algorithms.

Encrypted messaging helped in boosting operational security. End-to-end encryption enables fighters to coordinate their activities with low chances of getting apprehended. Online anonymity eliminates the exposure and facilitates decentralization. Hierarchies are falling and loose cells take care of themselves whilst sharing beliefs in core.

Another tech leap was drones. UAVs are utilized in the scout, throwing weapons across the borders, and surveillance. Drones reduce the physical intrusion yet they still have a tactical punch.

FinTech also redefined terror. Digital wallets and cryptocurrencies allow you to conceal cash and go without the banking system. Online crowdfunding and encrypted transfer make counter-terror surveillance more complicated.

Along with the kinetic and financial advantages, the digital age introduced info-war as the main part of transnational terrorism. Disinformation, communal incitement, and psychological operations separate society; disinformation causes large-scale reactions of the state. The current terrorism in South Asia is hybrid combining physical assaults with cyber-control and narrative warfare.

v. Security Threats

Cross-border terrorism in the current world is essentially a blend of the old methods and new technologies. There are still guys who break the door with a gun, but now it is a complete cyber squad, Internet propaganda, and backdoor brain-weaving. The boundary that previously separated terrorism and the cyberwarfare has become blurred. The fighters take advantage of the existing social breaks, fabricate fake tales, and distort what the audience can view in the news to exaggerate even the mildest physical assaults.

This combined approach adds more complexity to strategy. Although there is no major bombing, digital propaganda may confuse whole communities, trigger riotous relations, and cause people to lose trust in institutions. Cross-border terrorism now operates on the triple front simultaneously on the ground, on the net and in the heads of people.

vi. Technological Modernisation and Its Strategy.

Technological advancements have transformed cross-border terrorism over the years into a three-legged creature:

To start with, communication has ceased to be slow and localized to instant and secret connections around the world. It implies that threats can bypass the detection procedure with ease and they can organize more quickly.

Second, the recruitment process has been transformed so that it is not attracting individuals through local rallies but through aggressive online campaigning that can lure involved youths across borders.

Third, the movement of money has changed to smuggling of money in form of cash, to smuggling in form of digital coins and crypto that conceal the tracks.

All this technology implies that the jihadists are able to operate to a greater extent, quicker and more stylishly.

vii. Implications of Technological Evolution in the region.

The concerns of India are about digital radicalisation in such locations as Jammu-and in-Kashmir and major cities as well as attempts at drone intrusion. Pakistan receives the blow of its own militant groups and has to maintain a lid on the cyber space occupied by the extremists. Online radicalisation in Bangladesh is giving rise to local cells that are influenced by global discourses. It has been evident in the case of Sri Lanka where global ideologies can creep in through the digital realm. Nepal and Bhutan might appear peaceful but they remain a victim of the online spill-over and propaganda.

The thing is that digital borders are permeable; they extend outside of the physical scopes.

viii. Prevention of Cross-border Terrorism: Regional Level.

To discontinue this stuff is to keep in pace with tech growth. It is not simply a matter of constructing fences and deploying the forces. Countries must combine aspects of physical defence, cyber-intel, money-watching, and counter-narratives.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 6, Issue 2, Mar.-Apr., 2026, pp: 410-417 ISSN: 3048-6874
www.ijhssm.org

It must be a co-operation on the side of the region. The risk can be reduced by sharing intelligence, harmonizing cyber legislation, securing a joint system, and enhancing money controls. In its absence, technological disparities may cause militants to exploit intercountry loopholes.

The Indian View on Prevention of the Cross-border Terrorism.

The combination of hard security and tech in India is brought together in a couple of ways. Increasing border inspections by using sensors, drones, and real-time surveillance makes the physical game more restrictive. The cyber squads that pursue extremist content on the internet have also been enhanced in the same country.

The legislation such as anti-terror bills into IT regulations puts the law-enforcement on a leash in shutting down digital assistants. The tighter concentration between central and state authorities enhances the level of coordination and virtually enables AI and data science to identify threats before they become a reality.

This is also propagated by India that radicalisation can only stop when you invest in the society; get young people involved, provide them with opportunities, and establish relationships within the neighbourhoods. The campaigns are run in a variety of languages in order to break down digital propaganda ecosystems.

The Indian perspective dictates that this needs a pile of layers consisting of:

• Physical border protection
• Cyber watch-AI surveillance.
• Money-intel regulation
To discuss trade-talk with neighbours.
• Local de-radicalisation programs.

India wants to talk more in bilateral streets and multilateral rooms, and maintains a sound army.

Regional Cooperation in South Asia to Prevent Cross-Border Terrorism: Structures, Challenges, and Strategic Pathways

The South Asian cross border terrorism has evolved beyond broken local revolutions to mad-tech hybrid warfare. With every step a new layer of tech and a new set of tactics has been introduced. The technological update, particularly higher-speed communications, coded messages, drone hacks, and cryptocurrency have altered the scope, as well as the nature, of the threat.
Addressing this hustle would be going beyond the old deterrence pushing. It will only be possible to secure this on a long-term basis by a combination of excellent governance, technological preparedness, regional collaboration, and local advocacy.

The cooperation between the region in South Asia in terms of cross-border terrorism is vital and complicated. Its porous borders, common ethnicities, transnational religious connections, maritime routes and the convergence of multiple digital spaces form an interdependence network that the terrorist networks use to carry individuals, funds and propaganda across. This fact proves that the action of individual states is not sufficient. In its place, there is a need to have integrated regional structures, which intertwine intelligence communications, lawfulness, monetary controls, cyber controls, and diplomatic good faith.

The geography of South Asia explains the importance of such collaborative endeavors. India shares borders with Pakistan, Nepal, Bhutan, Bangladesh and Myanmar and maritime connections with Sri Lanka and Maldives. The porous border that exists between Nepal and India, the thick border that exists between Bangladesh and India as well as the historic maritime routes that exist between Sri Lanka and India all offer avenues through which terrorist actors can escape notice, seek safe havens or access to logistics. Thus, this collaboration is not just a rhetorical device, but it is structural security requirement.

The South Asian Association of Regional Cooperation (SAARC) was one of the first attempts to solve the issue of regional security. SAARC embraced the anti-terrorism conventions and established procedures of mutual legal assistance and extradition. Yet official agreements have not been translated into good action. The India-Pakistan rift and any other political suspicion that could cause this rift, has time and again stunted the effectiveness of SAARC. The counter-terrorist co-operation within the framework of SAARC is mostly declarative but not operational with ineffective intelligence sharing systems and minimal joint drills. As a result, SAARC has not yet turned into a well-functioning security organization that can swiftly react to cross-border menaces.

In order to identify these weaknesses, sub-regional organizations such as BIMSTEC (Bay of

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 6, Issue 2, Mar.-Apr., 2026, pp: 410-417 ISSN: 3048-6874
www.ijhssm.org

Bengal Initiative of Multi-Sectoral Technical and Economic Cooperation) have been increasing in momentum. BIMSTEC unites India, Bangladesh, Nepal, Bhutan, Sri Lanka, Myanmar, and Thailand, but not Pakistan, which is the source of the Indo-Pak conflict that paralyses co-operation. The organisation puts more emphasis on counter-terrorism, intelligence coordination and joint drills. India encourages the concept of BIMSTEC as a platform of safety especially in maritime security and cyber governance. However, BIMSTEC is still institutionally constrained and requires more integration of its operations.

The most feasible kind of regional counter -terrorism interaction is bilateral relations. The intelligence sharing agreements with Bangladesh has helped India to significantly curb the insurgent safe-houses along the northeast frontier. Collaboration with Bhutan had been used in the past to conduct joint operations, eliminating militant camps. India and Sri Lanka are also aligning their maritime security-related activities, particularly following the 2019 Easter attacks that indicated a lack of intelligence sharing between the countries. India and Nepal coordinate their borders using border coordination committees, and the open-border system presents a problem with monitoring. Such bilateral deals exemplify that cooperative gains in the form of tangible security are achievable through the bilateral cooperation, even where the larger regional platforms fail.

The maritime cooperation has gained a greater focus in the context of the regional security. The Indian Ocean has been transformed into a strategic rivalry theatre and transnational risks. Weapons, money or even terrorists can be smuggled to sea by terrorist groups. India has developed coast radars, which connect with SriLanka, Maldives and Mauritius to enhance the awareness of the maritime domain. Information-sharing agreements can be used to track suspicious ships in real time and common naval drills enhance interoperability. There has been relative success in maritime security cooperation due to the fact that it is not as politically contrived as land boundary issues.

The cyber cooperation is a very important border of regional security. Digital radicalisation transcends physical boundaries, and the spread of social media propaganda in a particular country spreads fast to others. The use of encrypted platforms makes it harder to monitor them, and cross-regional cyber coordination is still weak since states have taken different regulatory approaches. Terrorists can take advantage of regulatory loopholes without co-ordinated cyber laws and co-operative monitoring. The cooperation in the future must focus on cyber intelligence sharing, undertaken counter-narrative campaigns, and training in digital forensic analysis.

Monetary cooperation is also an essential aspect. Funding of terrorists is achieved informally in the banking sector, remittance networks, digital wallets, and more often cryptocurrencies. Local standards should be meeting international standards as established by the Financial Action Task Force (FATF). South-Asian state actors ought to organize reporting suspicious transactions, exchange financial information, and control digital transactions between countries. Uneven enforcement can be used by militants without coordinated attention. Despite development, there are structural problems.

The largest obstacle to successful cooperation is the historical mistrust. Security cooperation in South 1 Asians tends to be perceived as a zero-sum game. States fear that sharing intelligence would hurt their sovereignty or reveal their weakness to their strategic position. Foreign policy is also influenced by domestic politics so that flexibility is curtailed. Also, there is the asymmetry between India and its neighbours, this creates fear of being overpowered by the smaller states, but India fears external forces taking control over its neighbourhood.

The increasing influence of China in South Asians contributes to the further complexity. Port developments, economic projects, and infrastructure projects have a strategic implication. Although economic involvement is not necessarily a source of security mismatches, geopolitical competition may undermine the confidence in the region. When the great-power rivalry is engrossed in the cooperation, the joint counterterrorism can be undermined. India has to thus work towards systems that bring out common security interests as opposed to containment.

The regional cooperation requires institutional innovation. Mistrust can be minimized by confidence-building measures. Familiarity of operations is achieved through regular intelligence meetings, joint training courses, and common databases on counter-terrorism. Inter-agency crisis-communication hotlines can avoid the escalation following incidents. Track-two diplomacy, which takes part in academicians and think tanks, can

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 6, Issue 2, Mar.-Apr., 2026, pp: 410-417 ISSN: 3048-6874
www.ijhssm.org

produce a policy idea that is immune to political instability.

Another way of counter-terrorism is through socio-economic cooperation. Radicalisation breeds on poverty, unemployment and marginalisation. The resilience to extremist narratives can be enhanced by regional development projects, infrastructure connectivity, and educational exchanges. There is less incentive to destabilise due to economic interdependence. Therefore, trade and development interaction is the complement to the hard security measures.

In the case of India, the regional cooperation is in line with its overall strategic objective of becoming a net security provider in South Asia. India is big in size and capabilities but the key to good leadership is the assurance and not coercion. Efforts to strengthen collective resilience can be achieved by providing capacity-building support to border management of neighbouring states, cyber security and financial monitoring.

Regional cooperation fundamentally must in future develop into an integrated security architecture. That is to connect the maritime surveillance systems, align cyber surveillance systems, coordinate anti-terror legislations, and institutionalization of intelligence sharing. Although we will not be able to become a NATO-style alliance even in South Asia because of political rivalry, we can cooperate in certain areas.

After all, it is all about similar vulnerabilities in cross-border terrorism in South Asia. These terror groups are not concerned with borders and thus the state retaliation can not remain entrenched within them. It is important even though the cooperation at the region level, though not perfect and politically constrained, still matters. In the absence of mechanisms of collaboration, technology will continue to accelerate at a rate beyond our ability to follow it. Sustainable security in south Asia requires transforming mistrust between the regions in South Asia, into actual, structured coordination relying on mutual interest and practical involvement.

India's Perspective on Preventing Cross-Border Terrorism

The manner in which India views the prevention of cross-border terrorism is influenced by a collection of factors such as geography, historical battles, the nuclear alteration of the game, and regional antagonism and novel technology threats. To India it is not merely an abstract debate on security; it is an actual day-to-day strategy issue. The nation has had to contend with foreigners who support militants, insurgent groups finding their way in, and transnational terror networks that cut across porous borders of land and sea since gaining independence. That way, it is no more a defense-only policy of reactivity of India, but a comprehensive, proactive deterrence policy that combines military, diplomacy, spying, economics, technology and regional cooperation.

India primarily regards cross-border terrorism as an activity or condoned by other states, in particular, with regards to the militants of pakistan origin that are involved in attacks on Jammu and Kashmir and big city centers. However, the future does not end with Pakistan. India sees that chaos in Nepal, unsteady politics in Sri Lanka and radical networks in Bangladesh along with great power competition in the Indian Ocean can also precondition the terrorist activities indirectly. That is why counter-CBT strategy of the country is not only grounded and focused on one enemy.

Deteterrence that is well calculated is a large portion of the Indian mindset. The country had been influenced by the 2008 attacks and subsequent bombings in Uri and Pulwama, and felt like it was time to abandon decades of so-called strategic restraint and incline more towards an explicit doctrinal break. Surgical raids and air attacks demonstrated that India is willing to cross-border strike should it be necessary, as it seeks to bring the terrorists down and hopefully avoid the nuclear shadow blow up any such escalation. This is aimed at increasing the risk to the attackers and the puppet masters in which they consider an attack prior to striking again.

Simultaneously, India acknowledges that shooting bad guys down with guns will never succeed in overcoming cross-border terrorism. This is the reason why it is highlighting border management. The government has gone a notch higher with the fences, floodlights, thermal and motion sensors, drones, satellites and fully integrated border systems across the sensitive frontiers. It is an attempt to reduce the leaks with this combination of high tech and on-ground fixes to reduce the possibility of bad actors getting in.

Conclusion

I have also observed that terrorism as a foreign based threat to South Asia is becoming one of the most incessant and disruptive security predicaments we have been discussing in our

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 6, Issue 2, Mar.-Apr., 2026, pp: 410-417 ISSN: 3048-6874
www.ijhssm.org

international relations classes. It is not just a single instance of violence, but a mirror image of structural reality, historic conflict, unresolved border issues, permeable borders, ideological radicalism, technological dispersion, and geopolitical conflict. Gradually, it has been moving beyond the ancient paradigm of infiltration and proxy warfare and toward an undercover blend of cyber-radicalization, encrypted messaging, drone-deliveries of weapons, online money laundering, and transnational propaganda bugging. What I understand is that in this light terrorism is dynamic, is technology-driven and is strategically aligned with the large scale politics within the area.

The strategic centralization of India in the center of the continent has made it the center of such cross border threats, where external powers tend to sponsor the attacks. The evolution of the strategy of the country has changed to a purely restrained approach into more balanced approach of incorporating both proactive deterrence and structural prevention. That is, the contemporaryization of border infrastructure, integration of intelligence, enhanced cyber surveillance, interruption of funding streams, changing laws, and selective responsiveness across borders where necessary. I believe that it is obvious that a military reaction can not be a sustainable solution in the long term. Diplomatic negotiations, regional cooperation, technological advancement, and domestic resilience is the future of security.

The local context is crucial. South Asia is also very interconnected and all the socio cultural vulnerabilities are common to all states and no individual state can address these issues individually. Countering terrorists will entail the sharing of information, following money trails, broadening the area of maritime awareness, and harmonizing laws. But there is still political mistrust, particularly between India and Pakistan that suffocates collective security endeavors. It appears that pragmatic, trust-based cooperation occasionally ensures a better result: small multilateral discussions have proved to be not very effective in comparison to the sub-regional forums and bilateral agreements.

Technology is transforming cross-border terrorism. Online messaging, cryptography and drones reduced the operational cost of the terror groups and made them difficult to trace. The strategies used in the future must aim at adjusting to new technologies, enhancing cyber governance, applying AI to filter through intelligence, and unifying the border systems. The fact that the modernization direction of India is already modernized proves that these alterations are indeed in progress and that the funding and collaboration of the agencies will be pivotal.

In the future, geopolitical changes, such as an increase in competition in the Indo-Pacific and an increase in external interventions in South Asia, create complications. The more regional organizations become tight and neighbors become unsteady, the more the likelihood of proxy wars or transnational militancy increases. The long-term strategy of India should not be deterrence or dialogue, technological innovation or institutional change, dominance or partnership assurance in the region.

References -

[1]. https://www.ipcs.org/ipcs_books_selreviews.php?recNo=185
[2]. https://ijlmh.com/paper/echoes-of-conflict-navigating-cross-border-terrorism-in-south-asia-in-the-digital-era/
[3]. https://dkiapcss.edu/security-nexus-perspective-explores-water-terrorism-and-escalating-risk-in-south-asia/
[4]. https://strafasia.com/cross-border-terrorism-cbt-and-its-impact-on-regional-security-and-stability-of-south-asia/