MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Digitally Enabled Radicalisation and Violent Extremism in India

Saman Ayesha Kidwai

July 15, 2026

Summary

The digital ecosystem is increasingly playing an enabling role in disseminating propaganda, incitement and mobilisation in the pursuit of violent extremist acts. India's rapidly evolving security landscape is increasingly shaped by the online ecosystem, driven by the convergence of emerging technologies, decentralised peer-to-peer networks, and online communities.

Introduction

The digital ecosystem is increasingly playing an enabling role in disseminating propaganda, incitement and mobilisation in the pursuit of violent extremist acts. While not every act of radicalisation has manifested into incidents that could be categorised as violent extremist in nature, rigorous online indoctrination carries the potential to, through sustained radicalisation, eventually transform into acts of violent extremism targeted at state infrastructure, places of worship, government agencies, elected representatives, or unarmed civilians.

This is particularly important as traditional avenues and timelines for radicalisation and subsequent acts of violent extremism (including terrorism) have become far less dependent on physical or in-person interactions over prolonged periods. As per the Global Terrorism Index Report 2026, the time taken for an individual to become radicalised and subsequently commit acts of extremist violence has shrunk to a matter of weeks by 2026, down from more than a year in 2005, from first exposure to radical material to the carrying out of an attack.[1]

Broader Domestic Context

Over the last decade, India has taken decisive steps to neutralise emerging security threats, including the institutionalisation of PRAHAAR in February 2026, India's first publicly available national counter-terrorism strategy.[2] The document acknowledges the growing concerns attached to the exploitation of social media and encrypted chat forums by violent extremists. It signals that developments within the broader digital ecosystem need to be factored into national security policy.

This is particularly crucial given the recent acts of extremist violence, including the car blast near the Red Fort in New Delhi (November 2025) and the lone wolf stabbing incident in Mumbai (April 2026), which indicate that the perpetrators have increasingly been indoctrinated online to carry out acts aimed at undermining national security (see subsequent sections for details).

At the same time, there have been crackdowns on micro-cells and online networks of extremists inspired by the virulent ideology espoused by Al-Qaeda (AQ) and ISIS on the one hand, and criminal networks linked to Pakistan's Inter-Services

[1] **"Global Terrorism Index Report 2026"**, Report, Institute for Economics & Peace, March 2026, p. 66.

[2] **"National Counter-Terrorism Policy & Strategy"**, Ministry of Home Affairs, Government of India, 23 February 2026.

Intelligence (ISI) on the other. The latter, in particular, operates at the intersection of organised crime and terrorism.

Therefore, as conventional threats such as organised crime and terrorism converge with an increasingly penetrable digital environment, regulating content shared on social media or encrypted chat forums becomes crucial.

The Threat of Online Radicalisation

India has, over the decades, faced physical acts of terror and narcotics trafficking (via drones) linked to Khalistanis and Pakistan-backed groups such as Jaish-e-Mohammed (JeM) and Lashkar-e-Taiba (LeT). While these threats have persisted, the transformations taking place in the technological realm have resulted in important developments. This has been particularly evident in the ways non-state actors evade surveillance, conduct logistical and operational planning aimed at carrying out acts of violence to undermine state security, and raise funds through encrypted blockchain technology available on cryptocurrency platforms, where regulatory enforcement measures remain limited.[3]

Furthermore, the structural transformations underway as a consequence of technological evolution, aided by the expansion of internet access and advancements in emerging technologies that enable encrypted communication for operational planning and the dissemination of extremist content, have raised the stakes for states, including India, seeking to revamp their security apparatus in tandem with existing realities and emerging trends.

PRAHAAR is an important and much-needed step in that direction. The Union government acknowledges in its national counter-terrorism policy and strategy document that:

> For propaganda, communication, funding and other guiding terror attacks, these terror groups (ISIS, Al-Qaeda, and Pak-backed terror outfits) use social media platforms as well as 'instant messaging applications.' Technological advancements like encryption, dark web, crypto wallets, etc. have allowed these groups to operate anonymously.[4]

[3] Soumya Awasthi, **"Exploring the Nexus: Cryptocurrency, Zakat, and Terror Funding"**, Expert Speak, Observer Research Foundation, 8 May 2024.

[4] **"National Counter-Terrorism Policy & Strategy"**, no. 2, p. 3.

Recent investigations and case studies further reveal that online radicalisation in India is anchored in four fundamental pillars: encrypted communication, online propaganda, social media, and private messaging platforms or applications. The recurring trends reflect a concerning reality: the dual challenges of radicalisation and violent extremism no longer require prolonged physical or in-person communication, trust-building exercises, the cultivation of offline social networks, face-to-face recruitment, or repeated indoctrination lasting several months. Rather, the entire process can take place online within a few short weeks. Taken together, these investigations indicate that online radicalisation within the domestic context has been shaped by three facets operating simultaneously, and at times overlapping: imported propaganda consumed online, digitally networked infrastructure, and foreign handlers, particularly those based in Pakistan.

Key Trends and Patterns

May 2026 proved to be a critical month in uncovering the cross-border machinations behind the online or digital grooming of impressionable Indian youth, engineered by organised criminal elements such as Shahzad Bhatti (with ties to a new violent extremist outfit, Tehreek-e-Taliban Hindustan or TTH) and Pakistan's ISI. Reports noted that Bhatti is at the helm of operational planning for TTH activities and the dissemination of propaganda.[5] Hizbullah Ali Khan alias Tushar Chauhan (Meerut) and Sameer Khan (Delhi) were apprehended by Uttar Pradesh's (UP) Anti-Terrorism Squad (ATS) while undergoing systematic grooming following the establishment of trust between them and Bhatti.[6]

As is often the case in systemic radicalisation, friendship, trust and loyalty are established before potential recruits are introduced to extremist and virulent content to advance the cause of violent extremist actors. By following this pattern, the extremists presumably seek to ensure that the bonds of loyalty, trust and solidarity cultivated in the initial phases of interaction with potential recruits will drive the hardening of ideological commitment to an extremist cause.

While investigative reports reveal that the above-mentioned individuals had not yet developed a hardliner's worldview, Bhatti's allure of comfort and luxury was being

[5] **"Pakistan-based Shahzad Bhatti Identified as Mastermind Behind TTH"**, Details of Terrorism Update, South Asia Terrorism Portal, 25 May 2026.

[6] Ananya Pattnaik, **"UP on High Alert: ATS Uncovers Pakistan-Linked Digital Radicalisation and Sleeper Cell Network"**, *Pragativadi*, 18 May 2026.

weaponised by the TTH leader to covertly recruit Hizbullah and Sameer into the outfit's rank and file. Their arrest formed part of a larger multi-state raid aimed at disrupting a broader network across North India established by Bhatti through Instagram, YouTube, and encrypted communication channels.

In addition, within less than a month, another extremist network, radicalised and mobilised entirely through WhatsApp, social media and communication via phone numbers originating in Dubai, was dismantled in June 2026. This denoted an upward trend in the scope of radicalisation, as the detained individual had already become deeply involved in recruiting peers and formulating plans to carry out acts of political violence at the behest of foreign handlers.

The crackdown took place when UP's ATS arrested Mohammad Sheikh (Azamgarh) on charges of inciting young men to carry out subversive acts and join Bhatti's cross-border network. Reportedly, Sheikh had also been assigned responsibilities by Bhatti and other criminal entities, including Ajmal Gurjar and Raza, based in Pakistan.[7] The raids conducted by UP's ATS form part of a broader domino effect, reflecting a recurring trend of online grooming and radicalisation among India's youth.

In April 2026, two significant events occurred simultaneously. On the one hand, the Delhi Police Special Cell foiled attempts by four members of a terror module based in Odisha, Bihar and Maharashtra to establish a Caliphate, create a Khorasan-based Lashkar (an army operating in the historic Khorasan region), and prepare for participation in Ghazwa-e-Hind (a disputed eschatological Islamic prophecy propounded by Al-Qaeda concerning a battle in the Indian subcontinent signalling the end of the times).[8]

The members of the extremist cell were not only radicalised entirely online, but also exploited the digital ecosystem to establish a broader extremist network within India. They relied on encrypted communication platforms to deliberate on matters concerning crowdfunding, propaganda dissemination, and preparations for an improvised explosive device (IED) attack, most likely targeting India Gate or the Red Fort in Delhi. During the same month, Maharashtra's ATS discovered that a lone wolf attack had taken place in the state, where an ISIS sympathiser, self-radicalised

[7] **"UP Anti-Terrorism Squad Arrests Suspect For Alleged Links With Shahzad Bhatti Network"**, *News On Air*, 2 June 2026.

[8] Aaqull Jameel, **"4 Arrests, 3 States, Online Radicalisation: Delhi Cops Bust Terror Module"**, *NDTV*, 18 April 2026.

after consuming extremist content online, stabbed two guards who failed to recite the Kalma (Islamic declaration of faith).[9]

One of the most unnerving extremist incidents affecting India's threat landscape was the blast near the Red Fort in November 2025. In the above-mentioned case, the networked perpetrators (with one of them linked to AQ in the Indian subcontinent) relied on ChatGPT and YouTube to construct IEDs and bombs, while using encrypted communication platforms, particularly Telegram.[10] This was done to communicate as well as disseminate extremist propaganda targeted at those with no prior criminal record.

Key Considerations

The impact of online radicalisation has therefore become geographically diffuse within Indian society. Moreover, they signal that the emerging security landscape is increasingly shaped by AI platforms and online networking, both of which have contributed to shaping the current phase of radicalisation and violent extremism in India. They also underline that decentralised radicalisation and violent extremism executed by lone wolves or micro-cells have become more prominent than activities pursued by centralised and rigid organisations. Finally, the digital ecosystem has exacerbated the scope of the security threats confronting the country.

The proliferation of online-driven networks indicates that the security threats arising from them cannot be relegated. Rather, they signal a likely shift in the nature of the security threats that India will face moving forward. Policies and reforms therefore need to keep pace with emerging security threats, which are often exacerbated by the leapfrogging potential of technological developments and the democratisation and decentralisation of internet access.

To address the dual-faceted challenges of radicalisation and extremism, it is necessary to formulate a holistic policy framework and strategy grounded in existing realities and emerging trends, while being supported by appropriate legislative guidelines. Law enforcement agencies at both the centre and state levels

[9] Paras Harendra Dama, **"Lone Wolf, Wanted to Join ISIS: Cops on Mumbai Man Who Stabbed Guards"**, *NDTV*, 28 April 2026.

[10] Imran Ahmed Siddiqui, **"Red Fort Blast Rocket: IED Tips from AI: NIA Probe Reveals ChatGPT Role in Attack"**, *The Telegraph*, 25 May 2026.

must be equipped with specific tools, such as databases, to statistically analyse the distinctive characteristics and overlaps among the modes, pathways, and types of radicalisation, extremism, criminal activity, and the criminal-terror nexus.

Social media and encrypted messaging companies need to be held accountable through enforceable regulatory measures and to work in tandem with state authorities. At the same time, counter-radicalisation and counter-violent extremism measures need to be effectively implemented. The government could partner with the private sector to work towards creating an AI-enabled platform that would have the capability to examine real-time trends within the extremist and radicalisation ecosystems. A pre-emptive approach could then be followed to stay ahead of evolving trends and prevent online discourse from escalating into physical threats.

Moreover, as part of its long-term vision, India must work towards establishing legislative frameworks and institutional mechanisms that are operating at the nexus of digital literacy, psychosocial support, behavioural threat assessment, and grassroots interventions supported by family and community leaders. It must do so while incorporating lessons from global best practices that can be contextualised within the local ecosystem. Ultimately, as technology continues to shape the global security landscape relentlessly, India's security-driven responses need to evolve at the same pace.

About the Author

Ms. Saman Ayesha Kidwai is Associate Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses