Social Media as a Force Multiplier for Terrorism and India’s Evolving Internal Security Challenges

Published On: 21-08-2026

Recent Developments:

- Security agencies recently dismantled the **Shahzad Bhatti Network**, an alleged Pakistan-based, **ISI-backed terror network**, in a coordinated operation spanning **14 States**.
- The operation resulted in **more than 250 detentions/arrests** and over **80 FIRs**, according to reports, demonstrating the scale of the network and the importance of coordinated counter-terrorism intelligence.
- The case highlights how **social media can connect foreign handlers with potential recruits inside India**, while also facilitating propaganda, radicalisation, reconnaissance, recruitment and financial mobilisation.
- The security challenge is expanding beyond conventional physical networks because digital platforms enable **low-cost, high-reach and cross-border operations** without requiring immediate physical contact.
- India’s regulatory environment is also evolving. The **Information Technology Rules, 2021** were updated in 2026, including provisions concerning **synthetically generated information**, while further amendments concerning intermediary compliance and digital-media oversight have also been proposed.

Social Media and Terrorism:

Why Social Media Has Become a Force Multiplier:

- Social media has transformed terrorism by reducing the **cost of propaganda, recruitment and communication** while increasing the speed and geographical reach of extremist networks.
- Terrorist organisations can use mainstream platforms to identify susceptible individuals and subsequently shift selected contacts to **private or encrypted communication channels**.
- Digital platforms can therefore function as an initial recruitment environment, communication layer and propaganda ecosystem within the same broader network.

Online Radicalisation and Echo Chambers:

- Extremist organisations use **emotionally charged propaganda, grievance narratives and identity-based messaging** to influence vulnerable audiences.
- Recommendation algorithms designed to maximise engagement can repeatedly expose users to similar content, potentially creating **ideological echo chambers**.
- Such environments can reduce exposure to alternative viewpoints and gradually normalise extremist narratives.
- The security challenge becomes greater when propaganda is customised according to **regional language, local grievances and demographic characteristics**.

Digital Recruitment Funnel:

- Terrorist recruiters can follow a **funnel model** in which potential recruits are identified through engagement with extremist material, contacted privately and progressively exposed to more radical content.

- The recruitment process can subsequently move from public platforms to **closed groups, private messaging services or encrypted channels**.
- This decentralised model reduces the need for conventional physical recruitment infrastructure and makes early detection more difficult.

Digital Tradecraft and Terrorist Communication:

Encryption and Anonymity:

- **End-to-end encryption** can protect legitimate user privacy but can also make terrorist communication more difficult for investigators to intercept.
- Pseudonymous accounts, virtual identities and cross-border digital services can make attribution more difficult.
- Investigators therefore increasingly require **metadata analysis, device forensics, behavioural indicators and network analysis** rather than relying solely on conventional interception.

Emerging Digital Techniques:

- Terrorist networks may exploit **anonymous communication methods, virtual private networks and hidden online services** to conceal identities, locations and communication patterns.
- Digital investigators must therefore analyse multiple layers of evidence, including account relationships, device artefacts, financial transactions and publicly available information.
- However, specific operational techniques used by terrorist groups should be understood primarily as **law-enforcement indicators**, rather than treated as inherently unlawful technologies because many such technologies also have legitimate uses.

Digital Terror Financing:

Shift Towards Online Financial Channels:

- Terrorist financing is increasingly affected by the growth of **digital payments, virtual assets and online crowdfunding mechanisms**.
- Terrorist actors may attempt to disguise fundraising activities as legitimate charitable or social campaigns.
- Virtual assets can complicate tracing because transactions may involve multiple jurisdictions, intermediaries and pseudonymous addresses.
- The **Financial Action Task Force** requires jurisdictions to apply anti-money-laundering and counter-terrorist-financing measures to virtual assets and virtual-asset service providers.

FATF Travel Rule:

- The **FATF Travel Rule** requires relevant virtual-asset service providers and financial institutions to obtain, retain and securely transmit information concerning the **originator and beneficiary** of virtual-asset transfers.
- Effective implementation can assist law-enforcement agencies and financial-intelligence units in identifying suspicious transactions and tracing illicit financial flows.
- India therefore needs stronger monitoring of virtual-asset transactions, cross-border transfers and suspicious financial patterns without undermining legitimate digital-finance innovation.

Implications for India's Internal Security:

Psychological Operations and Propaganda:

- Extremist organisations can use social media for **psychological operations** designed to influence public perceptions, generate fear and deepen social divisions.

- Targeted propaganda can be directed towards potential recruits, existing members, wider populations or adversaries according to the strategic objective.
- Foreign actors can also exploit social media to amplify domestic grievances and create perceptions of institutional failure.

Misinformation and Public Order:

- Rapid dissemination of **false or manipulated information** can trigger panic, communal tension and localised violence.
- The scale and speed of social-media communication can allow rumours to spread faster than conventional verification mechanisms.
- The Government has therefore had to develop mechanisms for content intervention and public-order management while facing concerns regarding excessive restrictions and internet shutdowns.

Election and Democratic Security:

- **Deepfakes, synthetic media, coordinated inauthentic behaviour and automated accounts** can manipulate electoral narratives and influence voter perceptions.
- The problem is particularly serious when synthetic content is distributed immediately before elections, leaving insufficient time for verification and correction.
- India's 2026 amendments to the **Information Technology Rules** specifically address **synthetically generated information**, reflecting the growing regulatory importance of AI-generated content.

Polarisation and Social Cohesion:

- Engagement-driven recommendation systems can disproportionately amplify highly emotional or polarising material.
- Persistent exposure to such content can reinforce ideological segregation and increase susceptibility to extremist narratives.
- Social-media security policy must therefore address not only individual terrorist accounts but also the **broader information ecosystem** that enables radicalisation.

Structural Features of the Threat:

Digital Feature

Internal Security Implication

Anonymity and pseudonymity

Foreign or domestic handlers can conceal their identity and location.

Algorithmic amplification

Extremist narratives can reach large and targeted audiences rapidly.

Low cost and high reach

A small network can engage with large numbers of potential recruits.

End-to-end encryption

Investigators may face difficulties in accessing communications.

Cross-border infrastructure

Foreign platforms and servers complicate jurisdiction and evidence collection.

Digital financial channels

Small-value and cross-border transactions can complicate financial tracing.

Challenges for Law Enforcement:

Jurisdictional and Evidence Challenges:

- Major technology platforms and digital infrastructure may operate across multiple jurisdictions, making access to evidence dependent on **international cooperation and legal procedures**.
- Delays in obtaining volatile digital evidence can reduce its intelligence value.
- India therefore requires faster and more predictable mechanisms for cross-border digital evidence sharing.

Scale and Decentralisation:

- The enormous volume of online content makes comprehensive manual monitoring impossible.
- Terrorist networks can rapidly migrate between platforms when accounts are removed or moderation improves.
- Decentralised and smaller platforms can therefore create new monitoring challenges.

Language and Context Gaps:

- Automated systems may struggle with **Indian languages, dialects, coded terminology, cultural references and rapidly evolving slang**.
- Excessive reliance on automated moderation can produce both false negatives, where harmful content is missed, and false positives, where legitimate content is wrongly flagged.

Security, Privacy and Free Speech:

- Counter-terrorism surveillance must be reconciled with the **Right to Privacy under Article 21** and the constitutional protection of freedom of speech under **Article 19(1)(a)**.
- The Supreme Court's **K.S. Puttaswamy judgment** recognised privacy as a fundamental right, making proportionality and procedural safeguards important considerations in surveillance.
- Security measures should therefore satisfy requirements of **legality, necessity, proportionality and procedural safeguards** rather than relying on indiscriminate surveillance.

State-Level Capacity:

- Central institutions can provide specialised intelligence and technical capabilities, but **State police remain crucial first responders** in most internal-security situations.
- Differences in cyber-forensic infrastructure, personnel and technical expertise among States can create weaknesses in the national counter-terrorism architecture.
- The Government should therefore strengthen specialised **cyber-forensics and Open-Source Intelligence capabilities** across State police forces.

India's Existing Institutional and Legal Framework:

Information Technology Framework:

- **Section 69A of the Information Technology Act, 2000** provides a legal mechanism for blocking public access to specified online information on grounds including sovereignty, integrity, defence and security of India.
- The **Information Technology Rules, 2021** prescribe due-diligence obligations for intermediaries and additional obligations for significant social-media intermediaries.
- Under specified circumstances, messaging-oriented significant social-media intermediaries can be required to identify the **first originator** of information through a legally authorised process, subject to safeguards.

Indian Cybercrime Coordination Centre:

- The **Indian Cybercrime Coordination Centre** serves as a nodal institutional mechanism for combating cybercrime and developing technological and forensic capabilities.
- It became an attached office of the **Ministry of Home Affairs** on **1 July 2024** and also works on research and development of technologies and forensic tools for law-enforcement agencies.

Intelligence Coordination:

- Mechanisms such as the **Multi-Agency Centre, National Intelligence Grid and Crime and Criminal Tracking Network and Systems** facilitate information sharing and intelligence coordination.
- Greater integration among central intelligence agencies, State police and specialised cyber institutions is essential because digital terror networks frequently cross administrative boundaries.

Unlawful Activities Prevention Act:

- The **Unlawful Activities (Prevention) Act, 1967** provides the principal statutory framework for dealing with unlawful and terrorist activities.
- Its provisions can address different components of terrorist activity, including **terrorist financing, conspiracy, recruitment and facilitation**, depending on the facts and applicable provisions.

Measures Needed:

Technology-Driven Intelligence:

- India should expand the use of **Artificial Intelligence, Natural Language Processing, network analysis and digital forensics** for identifying emerging extremist narratives and coordinated activity.
- AI systems should support trained investigators rather than replace human assessment, particularly where context, satire or political expression is difficult to classify automatically.

Faster International Cooperation:

- India should strengthen **direct and expedited mechanisms for cross-border access to electronic evidence**, while ensuring due process and legal safeguards.
- Cooperation with foreign governments and technology companies should focus on rapid preservation and lawful disclosure of evidence in terrorism investigations.

Stronger Financial Intelligence:

- Financial intelligence should integrate **banking data, virtual-asset transactions and suspicious online fundraising patterns** to identify terrorist financing.
- India should continue implementing FATF standards, including effective application of the **Travel Rule** to relevant virtual-asset service providers.

State-Level Cyber-OSINT Capacity:

- Every State should develop specialised **Cyber and OSINT cells** equipped with trained personnel, forensic capabilities and multilingual analytical tools.
- Capacity building should extend beyond major metropolitan police forces to districts facing significant cross-border or radicalisation risks.

Platform Accountability:

- Technology companies should maintain transparent systems for reporting and removing **terrorist propaganda and recruitment material**.
- Recommendation systems should undergo appropriate independent risk assessments where there is evidence that their design systematically amplifies harmful extremist content.
- Platforms should also strengthen mechanisms for preserving evidence required for lawful criminal investigations.

Digital De-radicalisation:

- Counter-radicalisation should combine **early identification, counselling, community engagement, credible counter-narratives and rehabilitation**.
- Individuals displaying vulnerability to extremist propaganda should not automatically be treated as hardened terrorists because early intervention can sometimes prevent progression towards violent extremism.
- Counter-narratives should address the underlying misinformation and grievances exploited by extremist recruiters rather than merely repeating official messaging.

Digital and Media Literacy:

- **Digital literacy and media literacy** should become important components of preventive internal-security policy.
- Young users should be trained to identify manipulated media, misinformation, impersonation, extremist recruitment attempts and coordinated influence operations.
- Schools, universities, civil society organisations and technology platforms can contribute to building societal resilience against online radicalisation.

Way Forward:

A Rights-Based Security Architecture:

- India needs a **technology-enabled but rights-based counter-terrorism architecture** that combines intelligence capability with constitutional safeguards.
- Surveillance should be targeted, legally authorised and proportionate to the security threat.
- Content moderation should distinguish between **legitimate political expression and material that directly facilitates terrorism or violence**.

Whole-of-Government and Whole-of-Society Approach:

- Countering digital terrorism requires coordination among **intelligence agencies, State police, cyber institutions, financial-intelligence agencies, technology companies and international partners**.
- The objective should shift from merely removing individual accounts towards disrupting the complete **propaganda-recruitment-financing-operational ecosystem**.
- India should simultaneously strengthen technological capacity, institutional coordination, international cooperation and public resilience.

Conclusion:

- Social media has transformed terrorism from a predominantly physical organisational threat into a **hybrid physical-digital security challenge**.
- The Shahzad Bhatti Network operation illustrates the importance of intelligence-led disruption of networks that can operate across States and potentially exploit digital platforms for recruitment and coordination.
- India's response must therefore combine **AI-enabled intelligence, cyber-forensics, financial surveillance, platform accountability, international cooperation and community-level de-radicalisation**.
- At the same time, counter-terrorism measures must remain consistent with **privacy, freedom of speech, proportionality and rule of law**.
- The long-term objective should be to make India's digital ecosystem **secure, resilient and resistant to extremist exploitation without converting national security into indiscriminate digital surveillance**.

Value Addition for UPSC:

Key Concepts:

- **Force Multiplier:** A factor that significantly increases the effectiveness or reach of an existing capability without requiring a proportional increase in resources.
- **Online Radicalisation:** The process through which individuals increasingly adopt extremist beliefs through digital exposure and interaction.
- **Echo Chamber:** An information environment in which users are predominantly exposed to views similar to their existing beliefs.
- **Psychological Operations:** Activities intended to influence perceptions, emotions and behaviour for strategic purposes.
- **OSINT:** Intelligence derived from publicly accessible information.
- **Cyber-Forensics:** Scientific examination of digital devices, networks and electronic evidence for investigation and prosecution.
- **Digital Terror Financing:** Use of digital payment systems, virtual assets or online mechanisms to raise, transfer or conceal funds for terrorist purposes.
- **Synthetic Media:** Digitally generated or manipulated audio, images or video, including AI-generated deepfakes