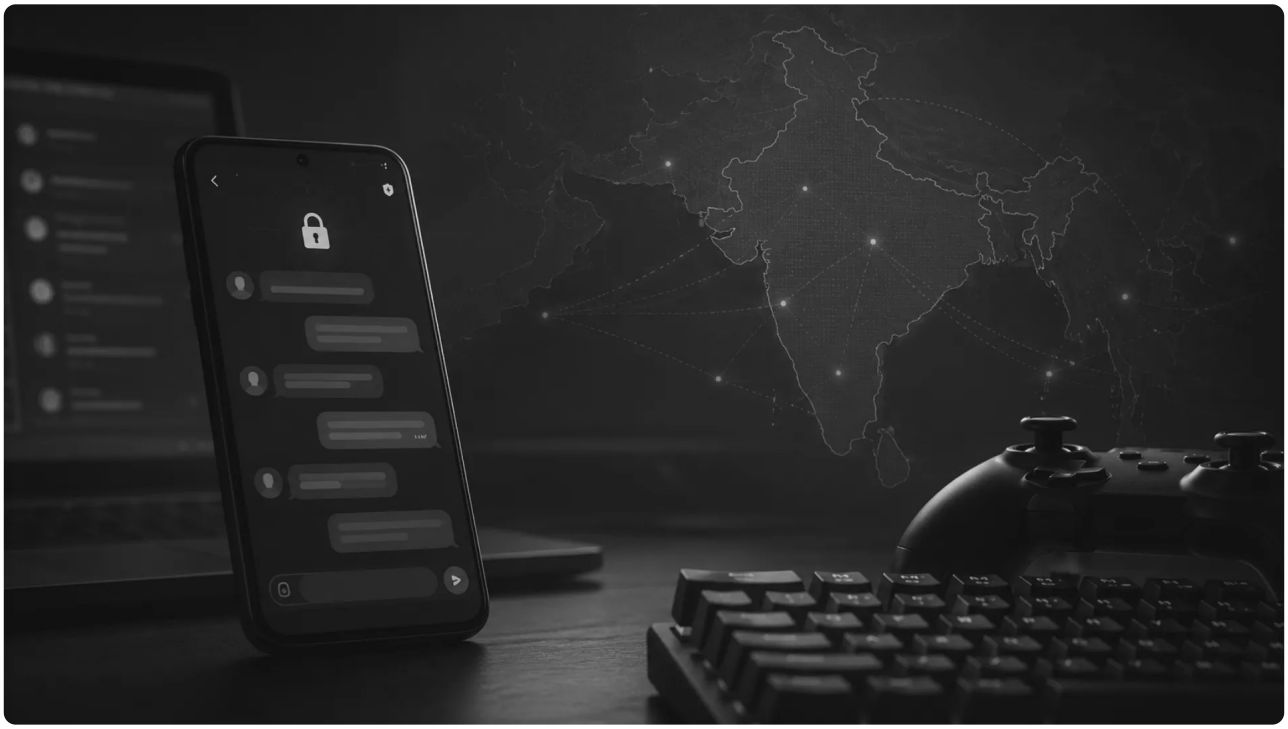
ARTICLES

The Evolving Digital Radicalization Ecosystems in South Asia: From Telegram to Gaming Platforms (2020-2026)

Author: Mahima Katiyar • **Published:** June 26, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Digital radicalisation in South Asia is no longer confined to the visible spaces of Facebook, YouTube, or X. Since 2020, extremist organisations have increasingly shifted toward encrypted messaging applications, private online communities, and gaming ecosystems where anonymity, scale, and weak moderation create new opportunities for propaganda, recruitment, and cognitive manipulation. This evolving threat is especially serious for India, where rapid digitalisation, a large youth population, expanding internet access, and gaps in digital governance have created a complex security challenge. As extremist narratives move from public platforms to hidden networks and immersive virtual spaces, the fight against radicalisation is no longer only about removing content. It is about understanding how digital ecosystems shape identity, belonging, and belief before they translate into real-world security risks.

Internet is a shared domain of humanity where beliefs, ideas and ideologies are continuously being shared and contested. Widespread digitalisation has not only made it possible for information and news to spread across the globe at lightning speed with just a click, it has simultaneously rendered the human mind even more susceptible and vulnerable to manipulation by extremist organizations. For the longer period of time, digital radicalisation was mainly associated with the popular social media platforms. This trend now however has seen a significant change. Since, 2020 many extremist organisations in South Asia has being to jump off towards encrypted messaging platforms like Telegram

and popular gaming platforms catering vast young populations [1]. The reason behind this jump is the capability of these platforms to offer privacy and enhanced security which makes oversight mechanism very difficult. Extremist organizations which are constantly seeking secure hidden communication channels and ways to prevent information leaks, find these new platforms highly effective in fulfilling those needs [2]. Weak digital governance system is making the countries increasingly vulnerable by unintentionally allowing such radicalisation processes to continue. By taking advantage of these new digital platforms and by exploiting the weaknesses in regulation and monitoring, these extremist groups are creating serious challenges for the law enforcement agencies and governments across the world.

Our research delves into this exact phenomenon by asking and examining three important questions across three important domains of why, how and what. First, it explores why extremist organisations are abandoning mainstream social media platforms and are jumping onto newer platforms and tools. Second question investigates into how these new platforms and gaming ecosystems are being used as tools for radicalization and recruitment. In third question we seek to examine the gaps and vulnerabilities within the Indian digital governance framework that may amplify this threat by contributing to the growth of this threat.

The Shifting Digital Landscape: From Mainstream to Encrypted Platforms

Since 2020 onward extremist organisations gradually moved towards the encrypted messaging applications particularly Telegram. What drove this shift are the stricter policies implemented by social media platforms. Companies have adopted a firm approach by significantly strengthening their monitoring and removal policies targeting content and accounts that promote hate speech, violence and extremism. These measures have made it difficult for the extremist organizations to spread their propaganda on widely famous open platforms like Facebook, YouTube and X. And due to this groups in their search for greater privacy, enhanced security and fewer restrictions have stumbled towards these newer platforms, and one of those is Telegram [2]. Telegram has emerged as one of the most attractive alternative because of its capabilities and features ensuring end to end encryption and flexible communication tools. The feature of Telegram allowing for creation of large groups and broadcasting channels makes it possible for extremist organisations to share and disseminate content and messages with a significantly large population simultaneously. And End to end encryption creates a sense of enhanced security for these thousands of users as it allows messages to flow with a significant lower risk of intervention by authorities. People join private groups and broadcasting channels where their minds are repeatedly exposed and bombarded with same ideas, narratives and ideologies. Over time, this constant exposure normalizes the extreme viewpoints by hijacking their cognitive processes. This creates an echo chamber where people encounter same ideas again and again which reinforces their existing beliefs. In such environments, opposing and rational viewpoints are absent and even if there, are dismissed. Since people rarely encounter cognitive competition from different or challenging viewpoints, these narratives gradually strengthen and amplify over time. And as a result, members develop such a strong sense of shared belonging, identity and purpose that they become less receptive and increasingly intolerant toward alternative perspectives [2]. Another important point is that the communication on this app is decentralised. So, instead of relying on single large account which may make them vulnerable, extremist organisations operate through various channels, groups and even private conversations. This strengthens their functioning as even if one account or channel is removed, they can continue functioning with other ones. And this decentralised structure makes it harder for the authorities to monitor activities, identify the perpetrators and disrupt communication networks since encryption veils almost everything unlike the public social media platforms.

In essence, this migration towards encrypted messaging platforms have significantly increased the difficulties on the part of the law enforcement organizations and intelligence agencies. These agencies often face legal and technical barriers and thereby struggle to access the encrypted communications. And even they identify and flag suspicious activities, gathering evidence and tracking networks is difficult of conversations being happening in private spaces within the insulated box of encryption. And this is why, extremist organisations have been using these platforms to distribute

propaganda, recruitment and for coordinating their activities. It’s the very structure if these platforms that enable them to continue operating even after being removed from more heavily monitored social media sites

Gaming Ecosystems: New Frontiers for Cognitive Manipulation

Apart from encrypted messaging applications, gaming platforms have also emerged as new fertile grounds for extremist organisations to flourish. Gaming platforms today are social spaces characterised by vast, diverse young population. Since for many people these gaming platforms often work like social media, extremist organisations have started seeing them as a potential target spaces [4]. This immersive and interactive environment which gaming platforms provide makes them particularly potent to gradual indoctrination through shared experiences and a sense of camaraderie. The young user base is particularly vulnerable and this creates a catalytic environment where extremist ideologies can subtly and gradually be introduced and normalized. Unlike traditional social media, conversations inside games, private servers, voice chats and gaming communities often receive less attention and moderation, this perceived anonymity is the gold which the extremist organizations look for [3].

To achieve their goal, extremist organisations exploit the social features built in the gaming ecosystems and other such adjacent platforms. For instance, platforms like Discord allows people to create voice channels, private servers and community groups which extremist organisations can exploit to build closely knitted communities and foster a sense of belonging among their potential recruits. The need for belonging is a powerful human emotion, is specially more heightened in young population due to their tender age and to those, who feel isolated, frustrated and disconnected in real life. This exploitation manifests through various mechanisms such as in-game propaganda dissemination channels, extremist themed content, private servers and gamification of extremists narratives [4]. Extremists organizations portray real -world conflicts as if they are exciting missions, heroic adventures or a competition between good and evil. Since they frame their ideology in ways that resembles video games, it makes these violent and extremist beliefs appear more attractive to the young audience who are already familiar with gaming culture. Extremist groups have been observed using popular games to create virtual training grounds, disseminate propaganda through custom game modifications and recruit new members through in-game chats and associated voice communication platforms like Discord. In platforms like Roblox, despite their efforts to combat such exploitation, extremist content is disseminated while keeping it hidden within the user-generated content or private servers that are difficult to monitor for moderators [3]. These subtle integration of extremists ideologies within the gaming context may seem like a not so dangerous act but it gradually desensitises the young individual and push them towards radical ideologies because now those ideas feel more normal. And not only this, even the competitive nature of gaming platforms can be exploited to create binaries of us vs. them, which is often a stepping stone towards radicalisation because it encourages division, hostility and a belief that conflicts between groups are inevitable.

While the South Asia specific data on the exploitation of gaming platforms for radicalization purposes is nascent, the global trends as highlighted by the Global Terrorism Index [7] warn us about a potentially dangerous digital hurricane. And what makes South Asia a potential site is its demographic profile, characterized by vast, multi-diverse , youth population and phenomenally expanding internet penetration. The week digital governance frameworks , nascent and sometimes almost absent AI monitoring and rules and regulations may act as a catalyst. These gaming ecosystems pose significant challenges to the traditional social media monitoring and radicalisation countering mechanisms, thereby requiring innovative strategies and methods from both counter-terrorism agencies and the gaming platforms. These may involve better moderation systems, digital literacy programs, stronger cooperation between agencies and service providers and the development of tools specifically designed to detect harmful behaviour in gaming environments without unnecessarily restricting the experiences of ordinary users. But any solution must take into account the unique social and cultural realities of South Asia. The process of radicalization does not occur in similarly designed trajectories everywhere; local history, religion , culture, language, politics, social and mental fault lines play an important role in how

extremist narratives are received [1]. Therefore understanding the local communities and cognitive maps of population is essential for diagnosing the root cause that makes them more vulnerable to extremist agendas for designing the effective counter-narratives and successful interventions.

Vulnerabilities in Indian Digital Governance

While the digitalisation drive has brought significant and rapid transformation along with enhanced benefits in terms of whether its economic growth, public services or technological advancements, it has simultaneously made India more vulnerable by generating more risks and by exposing inherent vulnerabilities within country's digital governance systems [11], [12]. As governments, governance institutions and people are becoming more and more dependent on the digital systems, the area and opportunities for extremist organisations have rather drastically been increased because of sheer scale of digital adoption. Simply put, the larger the population, greater the number of potential focal points available for exploitation.

The scale for cybersecurity threats in India is rather substantial than minimal. In 2025 alone, CERT-In addressed a substantial volume of cyber threats, documenting over 2.94 million cyber incidents, issuing 1530 alerts, 390 vulnerable notes and 65 advisories [9]. This data gives the evidence of the persistent and continuously evolving threat landscape of the digital domain of the country. The 2026 India Cyber Threat Report by Seqrite illustrates this risk further by revealing 265.52 millions detections across 8 million endpoints with average 505 detections per minute. The report highlights the constant barrage of cyberattacks including sophisticated ransomware campaigns and phishing attacks [10]. These threats however are not just technical and economic but can also contribute to radicalisation as extremist organizations can leverage these attacks to steal sensitive data, disseminate misinformation, disinformation and propaganda, disrupt essential services, hijack the cognitive processes of young population and even undermine public trust in institutions.

The key vulnerable points in Indian digital governance include the gaps in data protection and AI governance , plus the weaknesses in supply chain security and cloud infra [5],[6]. The absence of a comprehensive and robust data protection network makes the personal data vulnerable since its adequately protected. And extremist organizations can exploit exactly this leakage point to hijack information target individuals with tailored propaganda and even engage in blackmail and coercion. AI is being increasingly intertwined with our daily lives but advancements in this domain doesn't match the rules and regulations governing this powerful technology. Extremist groups can exploit these nascent governance structures by creating convincing deep fakes, by generating diverse and vast amount of automated propaganda. Such content can spread misinformation, inflame social tensions and makes it increasingly difficult for people to distinguish between authentic and false information. And as the technology advances the risk with only amplify further. Vulnerabilities existing within the cloud infra and supply chain can be exploited by the extremist organizations to infiltrate networks, lunch cyberattacks and establish covert communication channels. While evolving, the regulatory frameworks faces significant challenges in keeping pace with rapidly evolving technology and adaptive nature of cyber threats. For example, while CERT-In compliance rule in 2026 mandates the incident reporting within 6 hours and regular audits for governments entities, the sheer volume and sophistication of these attacks indicate a continuous struggle to maintain robust and continuously evolving digital defences. Cybercriminals and extremist organizations continuously change their tactics making it difficult for governments to anticipate and respond to emerging threats effectively. These governance gaps makes it harder to combat online extremism by hindering intelligence gathering, making monitoring difficult and by reducing the ability to implement proactive mitigation strategies thereby creating an environment conducive to proliferation of extremist ideologies.

Conclusion

The nature of digital radicalisation has underwent a serious transformation since 2020. As mainstream social media platforms have tightened their clutches on the necks of extremist content and accounts, extremist organisations have adopted by moving to encrypted messaging applications and increasingly, to gaming platforms. These new digital heavens offer greater anonymity, broader reach and new innovative ways for recruitment and propaganda dissemination. Simultaneously, the weaknesses within the Indian digital governance ecosystems particularly in cybersecurity, emerging technologies and data protection creates fertile grounds for these groups to flourish. The significant increase in terrorism related fatalities in South Asia, as evidenced by SATP data [8] and further contextualized by global trends in the Global Terrorism Index [7], further underscores the urgency of addressing these evolving digital threats. The need of the hour is a multi-faceted approach, encompassing enhanced international cooperation for addressing cross-border radicalization, collaboration with tech companies to implement more robust content moderation by developing AI driven detection mechanism and fostering greater transparency. Furthermore, significant investment is needed for improving country's digital governance framework. For India, this doesn't mean only bolstering cybersecurity defences through advanced threat intelligence and incident response capabilities but also proactively addressing legislative and regulatory gaps in the data protection and AI governance to prevent their exploitation by extremist groups. Besides these, what country must act on is developing comprehensive public awareness campaigns targeting youths about the risk of online radicalisation within gaming communities and ecosystems. There is a dire need for South Asia specific data so that we can grasp the volume of the threat hanging on our throats. Understanding the socio-economic and psychological factors making individuals prone to radicalization is also vital for any developing targeted and effective prevention program.

References

1. Giustozzi, Antonio, Imtiaz Bashar, Ananya Chakraborthy, and Abdul Basit. "South Asia." Counter Terrorist Trends and Analyses (2026). https://www.jstor.org/stable/48853535.

2. GNET Research. "Group Dynamics in Far-Right Telegram Communities: A Worthy Challenge for Radicalisation Research." February 18, 2026. https://gnet-research.org/2026/02/18/group-dynamics-in-far-right-telegram-communities-a-worthy-challenge-for-radicalisation-research/.

3. GNET Research. "Virtual Worlds, Real Threats: Violent Extremist Exploitation of Roblox and Wider Gaming Ecosystems." September 22, 2025. https://gnet-research.org/2025/09/22/virtual-worlds-real-threats-violent-extremist-exploitation-of-roblox-and-wider-gaming-ecosystems/.

4. Schlegel, Linda, and Rachel Kowert. Gaming and Extremism: The Radicalization of Digital Playgrounds. Cham: Palgrave Macmillan, 2024.

5. Centre for Social and Economic Progress (CSEP). Governing Digital India: A Report on Institutions and Instruments. New Delhi: CSEP, October 2025. https://csep.org/wp-content/uploads/2025/10/GOVERNING-DIGITAL-INDIA.pdf.

6. CyberPeace Foundation. "Cybersecurity Threats to India's Digital Ecosystem in 2026." January 8, 2026. https://www.cyberpeace.org/resources/blogs/cybersecurity-threats-to-indias-digital-ecosystem-in-2026.

7. Institute for Economics and Peace. Global Terrorism Index 2026. Sydney: Vision of Humanity, March 21, 2026. https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf.

8. South Asia Terrorism Portal. "South Asia Fatalities Data." 2026. https://www.satp.org/datasheet-terroristattack/fatalities/southasia.

9. Press Information Bureau, Government of India. “CERT-In: India’s Frontline Defender against Cyber Threats.” January 23, 2026. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537.

10. Seqrite. India Cyber Threat Report 2026. Pune: Seqrite, 2026. https://www.seqrite.com/india-cyber-threat-report-2026/.

11. Mordor Intelligence. India Digital Transformation Market – Growth, Trends, Forecasts (2026–2031). January 27, 2026. https://www.mordorintelligence.com/industry-reports/india-digital-transformation-market.

12. Observer Research Foundation. “A Decade of Digital India Mission: Achievements, Gaps, and the Way Forward.” August 14, 2025. https://www.orfonline.org/research/a-decade-of-digital-india-mission-achievements-gaps-and-the-way-forward.

The views expressed are those of the authors and do not represent the views of CNAWS.

?Image Source: ChatGPT