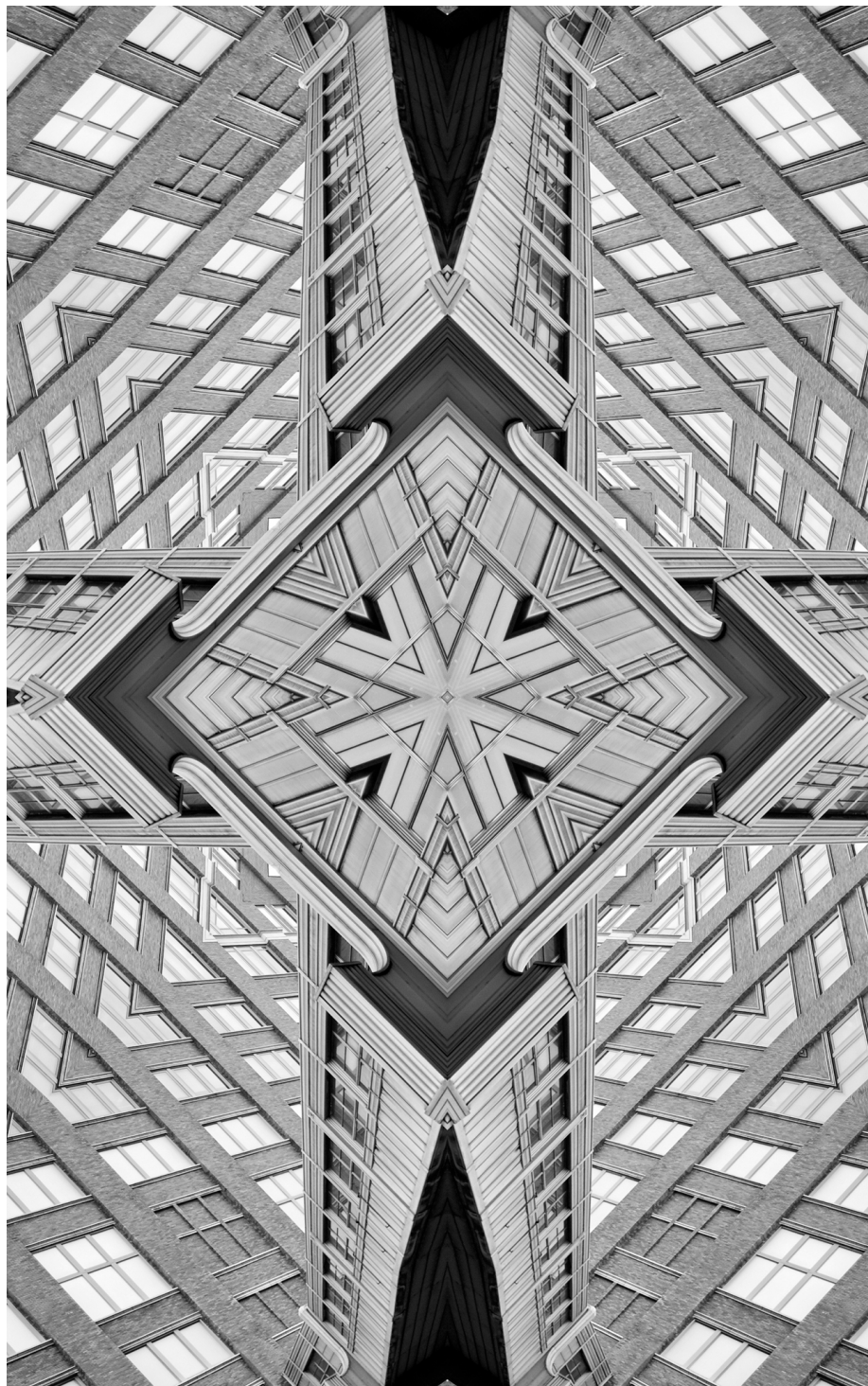


# Issue Brief

ISSUE NO. 790  
MARCH 2025



© 2025 Observer Research Foundation. All rights reserved. No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from ORF.



# Extremist Propaganda on Social Media: Impact, Challenges, and Countermeasures

## Soumya Awasthi

### Abstract

Social media is becoming an increasingly useful tool for radicalisation and the recruitment and mobilisation of individuals for extremist activities. India, with its unique socio-political landscape, is particularly susceptible to the misuse of social media. This brief explores the challenges posed by social media extremism in India and globally. It examines the psychological and societal impacts of platforms like X, the interplay between local and international propaganda, and the limitations of existing regulatory measures. The brief makes a case for a multi-pronged strategy for addressing these gaps to allow India to effectively counter the evolving threats of social media extremism while balancing security needs with the right to freedom of expression.

Propaganda is a powerful tool for influencing public opinion and normalising violence. For extremists, a primary propaganda strategy is the exploitation of individuals' vulnerabilities—such as emotional instability, social isolation, dissatisfaction with government policies, and the desire for belonging or respect—to create an “us vs. them” mentality, often using psychological warfare to dehumanise perceived adversaries and justify violence.<sup>1</sup>

In recent years, extremist actors have increasingly used social media platforms—low-cost, fast, decentralised, and globally connected—to spread their ideologies, recruit followers, and foster support for their activities. Terrorist groups are turning to the internet for activities such as recruitment and the dissemination of violent content through tools such as hashtags, videos, images, and open letters. Though social media is an enabler rather than a primary driver of violent radicalisation, its role in reinforcing extremist ideologies, identifying potential recruits, and fostering engagement cannot be underestimated.

Each platform offers unique advantages to extremist groups. Facebook, for example, acts as a decentralised hub for sharing information; X allows for rapid communication and engagement with global audiences; and YouTube is the preferred platform for video propaganda that is often tailored to resonate with specific cultural and linguistic audiences.

As of 2024, there were around 5.35 billion internet users worldwide, each generating approximately 15.87 Terabytes (TB) of data, including 500 million tweets on X, daily.<sup>2</sup> Facebook had the highest number of visitors globally in 2023, producing around 4,000 TB of data daily that year. The same study found that WhatsApp users share the most number of images, with 6.9 billion photos shared between users daily, followed by Snapchat, with 3.8 billion photos shared.<sup>3</sup>

Terror groups can easily reach out to registered users on social media without having to build their audiences. Extremist groups exploit social media's global reach, anonymity, and interactive capabilities by creating emotionally charged content. For radicalisation and recruitment, terror groups disseminate violent content targeting vulnerable youth, such as propaganda videos that show military training and other battlefield activities. Extremists also use video games to embed their narratives, modifying popular titles to reflect jihadist themes.

They use visual and audiovisual mediums, such as videos of attacks or symbolic imagery, to trigger powerful psychological responses and incite violent behaviour. Vulnerable individuals, particularly the youth, are drawn to these narratives, which aim to provide a sense of purpose and identity.



Understanding the methods and strategies that extremist groups use on social media is essential to countering their influence. By examining the psychological and social dynamics at play, policymakers and stakeholders can develop effective counter-narratives and interventions to address the root causes of radicalisation and prevent its spread. This will ensure that the digital space enables positive engagement rather than divisiveness, conflict, and violence.

This brief uses interviews and analyses of research material to identify propaganda strategies used by terror groups to rationalise their acts of terror and to recruit and radicalise members. Approximately 100 such images, slogans, hashtags, and social media posts in English, Hindi, and Urdu were assessed. According to the analysis, extremist groups target three kinds of audiences: the general public, for gaining sympathy and justifying their actions; the enemy group, usually the government and its various agencies; and existing members of the group to keep them motivated.

Table 1 shows the results of interviewing practitioners from the paramilitary and the strategic communications and cybersecurity sectors.

**Table 1: Propaganda Strategies Used by Extremist/Terror Groups**

	Audience	Strategy
1.	Members of the Group	<ul style="list-style-type: none"> <li>• Identity Fusion</li> <li>• Martyrdom Narrative</li> <li>• Glorification</li> <li>• Victory Narrative</li> <li>• Victimisation</li> </ul>
2.	Enemy Audience	<ul style="list-style-type: none"> <li>• Slurring</li> <li>• Demonising</li> <li>• Defamation</li> <li>• Disinformation</li> <li>• Conspiracy Against them</li> <li>• Instilling Threat</li> <li>• Challenging their Strength</li> </ul>
3.	Universal Audience	<ul style="list-style-type: none"> <li>• Us vs. Them</li> <li>• Victimhood</li> <li>• Social Welfare</li> </ul>

*Source: Author's own, based on field work<sup>a</sup>*

<sup>a</sup> The author interviewed a group of Indian security officials in November 2024.



India's diverse cultural and political fabric makes it vulnerable to exploitation by these groups. Platforms like Facebook, WhatsApp, Telegram, and X are extensively used for spreading propaganda, mobilising individuals, and fuelling communal tensions.

For instance, extremist groups capitalised on the COVID-19 pandemic, framing it as divine retribution against non-believers<sup>4</sup> and leveraging the increased screen time as a result of the lockdowns to recruit and radicalise individuals.

Indian security agencies have attempted to counter these threats by monitoring social media and collaborating with tech companies to flag harmful content. However, the decentralised and rapidly evolving nature of digital platforms requires more robust policies and proactive measures. Understanding how these platforms are exploited is crucial to addressing the broader threats. Extremist groups rely on the susceptibility of audiences to unverified information, using repeated exposure to propaganda to shape opinions and deepen ideological divides.

Pakistan-backed groups such as the Kashmir Tigers (KT),<sup>b</sup> the Resistance Front (TRF), and the People's Anti-Fascist Front (PAFF), as well as global groups like the Popular Front of India and the Islamic State (IS) have used social media for propaganda.

TRF, a proxy of Lashkar-e-Taiba, also emerged in 2019 and projects itself as an "indigenous resistance movement", using victory narratives to rally sympathisers and instil fear among adversaries. The group's attacks, such as the Anantnag (2023) and Ganderbal (2024) incidents,<sup>c</sup> are celebrated in propaganda posts that glorify martyrs and emphasise the group's strength.<sup>5</sup> They also utilise the tactic of slurring as part of 'psychological operations' to undermine the morale of the Indian security forces and foster a sense of shared identity among the members of the terror groups.

---

<sup>b</sup> KT, which is linked to Jaish-e-Mohammed, emerged after the abrogation of Article 370 in India in 2019. They have carried out multiple attacks, including the Kathua attack in 2024, and use slurring and conspiracy narratives to mobilise followers and gain media attention. See: <https://www.firstpost.com/explainers/doda-encounter-kashmir-tigers-terror-group-jaish-e-mohammed-security-personnel-attacks-jammu-kashmir-13793546.html>. In the case of the Kathua attack, they created a perception of power and dominance, claiming moral superiority by emphasising that their targets are only security forces, not civilians.

<sup>c</sup> These were attacks carried out by The Resistance Forces and Kashmir Tigers in 2024.

# India's Challenge

Similarly, the PAFF, which emerged in 2020, operates as a proxy for Jaish-e-Mohammed (JeM). PAFF publicises its attacks and spreads misinformation to generate public sympathy and degrade the state and its forces. For example, during the Poonch attack, PAFF circulated messages and images designed to provoke a response from security forces and amplify their propaganda.

These groups demonstrate a calculated and adaptive use of social media to advance their objectives. By understanding their strategies and countering their influence, India can better address the challenges posed by extremist propaganda in the digital age.



The use of social media and digital platforms by extremist and terrorist groups reflects a sophisticated adaptation to technology, enabling recruitment, propaganda dissemination, and global coordination. Hamas<sup>d</sup> utilised platforms like Telegram, X, and Instagram during the October 2023 Israel-Gaza conflict to distribute graphic content and sensationalist posts.<sup>6</sup> By January 2024, Hamas had escalated its digital presence, such as through TikTok, collaborating with Hezbollah to amplify anti-Israel narratives and glorify its own militancy through coordinated messaging strategies that involved humour, memes, and emotionally charged content.<sup>7</sup>

ISIS also leverages encrypted platforms like Telegram and WhatsApp. Throughout 2023, the group expanded its recruitment campaigns into Southeast Asia by exploiting local political and economic grievances. In 2024, ISIS activities extended into South Asia and Africa,<sup>8</sup> targeting vulnerable populations in regions like India, Bangladesh, Nigeria, and Somalia through emotionally charged narratives spread through secure communication channels.

White supremacist and far-right groups<sup>9</sup> in the West, like the Identitarian Movement (Europe), The Proud Boys (US and Canada), and the Patriot Front (US) mirrored these tactics, using platforms such as Telegram and Gab for recruitment and coordination. These groups exploited Middle Eastern conflicts to propagate narratives about a “clash of civilisations”, fuelling anti-immigrant and anti-Muslim sentiments. The Taliban also adapted their digital strategy by publishing online magazines like *Voice of Khurasan* or *Voice of Hind*, after regaining power in Afghanistan, using platforms like X and WhatsApp to build legitimacy, disseminate governance content, and suppress dissenting narratives. Crowdfunding became another key strategy, with Hamas and Hezbollah exploiting online platforms to circulate financial appeals through cryptocurrency.<sup>10</sup>

Psychological warfare has also become a prominent tactic. During the Gaza conflict in 2023-24, Hamas spread social media posts that included manipulated footage aimed at instilling fear and confusion among Israeli civilians.<sup>11</sup> Similarly, Iran-backed militia have disseminated anti-Western sentiments on social media during the ongoing Russia-Ukraine conflict.<sup>12</sup> Encrypted platforms like Telegram also serve as hubs for extremist activity, hosting virtual “classes” on operational security and propaganda dissemination.

The widespread exploitation of digital platforms has made them indispensable tools for extremist agendas, underscoring the critical need for robust countermeasures.

<sup>d</sup> The United Nations has not designated Hamas as a terrorist organisation. A number of countries have, including the US, UK, Japan, Australia, and the EU.

# Psychological Impact

Social media extremism operates on a foundation of emotional and psychological manipulation. At the heart of this manipulation is the exploitation of human emotions, which often lead to the escalation of violent tendencies. Extremist narratives tap into deep-seated grievances, cultivating anger and resentment among targeted individuals or communities. These narratives usually frame certain groups or institutions as oppressors, creating a perceived justification for hostility and aggression. Over time, exposure to such content desensitises individuals to violence, normalising it as a legitimate response to perceived injustices. The desensitisation is coupled with a sense of empowerment derived from aggression, as individuals feel validated through the approval and encouragement of like-minded online communities.

Alienation and anti-state sentiments are exacerbated by extremist propaganda, which fosters a sense of victimhood in vulnerable individuals. By portraying communities as systematically oppressed or marginalised, these narratives reinforce an “us vs. them” mentality that pits groups against one another and the state. This polarisation feeds into the formation of radical identities, which is marked by loyalty to extremist ideologies.

This psychological manipulation extends beyond individuals to target state institutions, particularly security agencies. Extremist groups deploy strategies of humiliation and psychological warfare against law enforcement, undermining their authority and credibility. Public shaming and online abuse of security officials are commonplace, often accompanied by victory narratives that glorify attacks on state agencies. Conspiracy theories further erode trust, painting security forces as corrupt, ineffective, or oppressive. This barrage of disinformation weakens public confidence in the institutions responsible for maintaining law and order.<sup>13</sup>

Among security officials, operational stress and paranoia become more widespread in an environment rife with misinformation and hostility. The vilification and scrutiny strain their capacity to act effectively while also impacting their mental health. Propaganda-induced mistrust also creates barriers between law enforcement and the public. Extremist narratives also often target the families and social standing of security officials.



# Psychological Impact

The cumulative effect is a spiralling of violence and distrust. Online extremism frequently translates into street-level violence,<sup>14</sup> which weakens the capacity of security forces to respond and further polarises society. Communities become divided, with mutual distrust and hostility replacing dialogue and cooperation. The resulting fractures threaten the social fabric, undermining efforts to build cohesive, peaceful societies.

Counter-extremism strategies must prioritise individuals' emotional and cognitive well-being, promoting inclusion, resilience, and critical thinking. Strengthening community ties and fostering trust between the public and security agencies are equally vital. Only by tackling the psychological roots of extremism can society hope to break the cycle of manipulation, violence, and division perpetuated by extremist groups online.

The Government of India has implemented a comprehensive approach to address the misuse of social media platforms by extremist groups for radicalisation, propaganda, and recruitment. Recognising the influence and potential of these platforms to disseminate harmful content rapidly, Indian authorities have introduced a combination of legislative frameworks, technological solutions, and collaborations with social media companies to mitigate the threat. In 2024, the Ministry of Electronics and Information Technology (MeitY) used its mandate under Section 69A of the Information Technology Act to block websites, URLs, WhatsApp accounts, Instagram, Facebook, and YouTube channels related to, linked to or owned by extremists and terrorist groups, including KT, Kashmir Fights, Resistance Media, TRF, and Jhelum Media.<sup>15</sup>

**Table 2: Number of Sites/URLs and Accounts Blocked by MeitY Since 2022**

Year	Social Media Platforms	Number of Accounts/URLs
2022	WhatsApp	6,775
	X	3,417
	Facebook	1,743
2023	WhatsApp	12,483
	X	3,772
	Facebook	6,074
2024	WhatsApp	8,821
	X	2,950
	Facebook	3,159
	Khalistan-Linked URLs	10,500
	Popular Front of India URLs	2,100
	YouTube (extremist Content)	2,211
	Instagram Accounts	2,198
	Telegram Accounts	225
	WhatsApp (Extremist Content)	138

*Source: Authors' own*



## Legal Instruments

India has enacted legal frameworks to regulate social media content. The Information Technology (IT) Rules 2021 empower law-enforcement agencies to take swift action against unlawful content. These rules require flagged material that violates laws relating to public order, security, or morality to be removed within 24 hours of notification by authorities. This provision is critical in combating extremist propaganda that could incite violence or spread misinformation.<sup>16</sup> Section 69A of the IT Act also grants the government authority to block access to content or entire platforms if they threaten national security, public order, or the country's sovereignty. This has proven to be effective in curbing the spread of harmful material with around 28,000 URLs blocked in 2022.<sup>17</sup>

## Monitoring and Intelligence Gathering

India has enhanced its monitoring and intelligence capabilities to address the use of encrypted platforms by extremist groups. The Cybercrime Coordination Centre works with state-level cybercrime cells to track suspicious accounts and identify patterns of harmful online activity.<sup>18</sup> Mechanisms have been developed to provide specialised training, monthly workshops, information-sharing to detect extremist content and trace networks operating on encrypted platforms such as Telegram, WhatsApp, and Signal.<sup>19</sup> Although end-to-end encryption presents challenges in accessing communications, intelligence agencies employ advanced analytical tools to track digital footprints, uncover group activities, and pre-empt potential threats. This coordinated effort between central and state authorities ensures a comprehensive response to the misuse of digital platforms.

## Mutual Legal Assistance Treaties

The Indian government has entered Mutual Legal Assistance Treaties (MLATs) with various countries<sup>e</sup> to facilitate cross-border investigations. These treaties provide a structured framework for cooperation between nations to address crimes involving digital platforms, many of which are headquartered outside India. Through MLATs, Indian authorities can request access to user data, trace the origins of extremist content hosted on foreign servers, and access encrypted communications when necessary. Such international collaboration is essential for overcoming jurisdictional challenges posed by the global operations of social media platforms, ensuring that offenders cannot take advantage of the constraints of geographical boundaries to evade accountability.

---

<sup>e</sup> As of 2019, the Government of India has signed MLATs with 42 countries.

# India's Countermeasures

These measures have helped India's efforts at regulating social media and addressing its misuse for extremist purposes. However, the rapidly evolving tactics of extremist groups and technological innovations employed by social media platforms demand ongoing innovation and adaptability. Balancing the need for security with preserving democratic principles and individual privacy is an enduring challenge in the effort to combat online radicalisation.

Despite India's legal framework aimed at regulating social media and curbing online extremism, the system has shortcomings in effectively preventing the misuse of these platforms.

### **Ineffectiveness of Internet Shutdowns in Jammu & Kashmir**

Following the abrogation of Article 370 in August 2019, the Indian government imposed a prolonged internet shutdown in Jammu & Kashmir intended to curb the spread of extremist content and maintain public order. However, this measure failed, with extremist groups utilising alternative communication methods like publishing and circulating pamphlets and newsletters. Indeed, the shutdowns only served to alienate the local population instead.<sup>20</sup>

### **Legal Challenges to Content Regulation**

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2023, were introduced to enhance social media content regulation.<sup>21</sup> These rules empower the government to direct social media platforms to remove content deemed “fake, false, or misleading” by a government-established fact-checking unit.<sup>22</sup> This approach has raised concerns about potential overreach and censorship, leading to legal challenges.<sup>f</sup>

### **Proliferation of Hate Speech and Misinformation**

Despite existing laws, social media platforms continue to be conduits for hate speech and misinformation. Unchecked online content exacerbates communal tensions.<sup>23</sup>

### **Misuse of Social Media During Elections**

Social media has been used during electoral periods to spread disinformation and manipulate public opinion. For instance, during the 2024 Indian general elections, deepfake videos featuring political figures were circulated to mislead voters. AI was used, for example, to create a fake video of PM Modi dancing, or misleading videos of Bollywood celebrities using Hindu supremacist language.<sup>24</sup> Despite legal frameworks, the rapid dissemination of such content has posed challenges to regulatory authorities.<sup>25</sup>

---

<sup>f</sup> Comedian Kunal Kamra filed a petition in the Bombay High Court, arguing that these provisions could suppress free speech. See: <https://internetfreedom.in/in-kunal-kamras-petition-in-the-bombay-high-court-the-government-undertakes-not-to-notify-its-fact-check-unit/>



### **Inadequate Response to Online Extremism**

The limitations of the legal framework are evident in the persistence of online extremism. Despite laws to curb hate speech and actions promoting enmity between groups, online platforms continue to host extremist content, indicating enforcement gaps.<sup>26</sup>

These cases illustrate that, while India has established legal measures to counter the misuse of social media, enforcement challenges and the dynamic nature of digital platforms often undermine their effectiveness. Addressing these issues requires robust legislation, adaptive enforcement strategies, and collaboration with social media companies to mitigate the spread of extremist content.

A multi-pronged approach is essential to address the multifaceted challenges posed by the misuse of social media platforms for radicalisation, propaganda, and extremist activities. This involves strengthening existing regulatory frameworks, enhancing technological capabilities, and fostering awareness among the population. Below are policy recommendations that aim to counter these issues effectively.

### **Regulatory Reforms**

One key issue is the lack of jurisdiction over platforms like WhatsApp, which do not host their servers in India and operate under United States laws. The Indian government should introduce regulations under Section 87 of the IT Act, 2008 to ensure that intermediaries adhere to Indian legal requirements. Strengthening existing provisions like Section 79 and Section 85 of the IT Act is necessary to hold platforms accountable for extremist content. Additionally, organisations and individuals must enact a specific law targeting the spread of misinformation. Precise definitions of cyber offences, penalties for non-compliance, and a system for regularly evaluating these policies should be included to ensure effective enforcement.

### **National Cyber Doctrine**

India must develop a comprehensive National Cyber Doctrine that includes a clear definition of cybercrimes, categories of cybercriminals, and legal repercussions for offenders. Such a doctrine should also outline a strategic framework for planning, training, and executing cybersecurity initiatives. By integrating various stakeholders, including law enforcement, intelligence agencies, and private organisations, the doctrine can enable a cohesive approach to countering cyber threats.

### **Tri-Service Military Cyber Intelligence Team**

Establishing a joint cyber-intelligence cell across all military commands is crucial for bolstering cyber defences against state-sponsored propaganda and cyber warfare. The team should focus on timely and precise actions against hostile activities, including monitoring and countering adversaries' misuse of social media.

## Digital Literacy Initiatives

With increasing social media usage among young people, early education on identifying and resisting disinformation is vital. A nationwide digital literacy drive should be launched, integrating modules on cyber safety into school curricula. Teaching students how to disengage from harmful online interactions and adopt a “no-comment” policy for contentious content can be a first step toward sanitising digital platforms.

## Content Analyses and Building Counter-Narratives

State-sponsored research into flagged content on platforms like YouTube and Facebook can help identify the rhetoric used by extremist groups. Such analyses should guide the development of effective counter-narratives to neutralise harmful ideologies. YouTube’s technology that redirects users vulnerable to extremist messaging towards curated videos that counter these narratives is an example of effective intervention.<sup>27</sup> India can adopt similar models to combat online extremism.

## Digital Fingerprints and Cross-Platform Blocking

Another plausible solution is using digital “fingerprints”, or hashes, to identify and remove harmful content. This technology ensures that, once content such as terrorist imagery or recruitment videos is removed from one platform, it cannot resurface on others within the same cooperative network. Indian authorities should collaborate with international organisations and platforms to adopt this technology.

## Evaluation and Improvement of Regulatory Policies


Regularly evaluating existing regulatory measures is necessary to adapt to evolving threats and challenges. Building a feedback loop between stakeholders—governments, tech companies, and civil society—can improve the effectiveness of policies over time.

# Conclusion

Countering the misuse of social media platforms for extremist propaganda and radicalisation requires an evolving approach. While India has progressed through measures such as the IT Rules 2021 and Section 69A of the IT Act, gaps persist in adapting to emerging technologies, ensuring swift content removal, and navigating the complexities of encrypted communications.

Strengthening the IT Act to include provisions for AI-driven propaganda and deepfakes, introducing penalties for non-compliance, and enhancing cyber law enforcement capacities are crucial. A National Cyber Doctrine can serve as a guiding framework for involving various stakeholders and addressing threats comprehensively. Establishing joint military cyber cells and state-sponsored research into extremist content can enhance India's ability to counter threats at both domestic and international levels.

Promoting digital literacy, particularly among young people, will empower individuals to resist harmful narratives and become responsible digital citizens. Incorporating advanced technologies like digital fingerprints for cross-platform blocking and creating tailored counter-narratives will strengthen the defence against online extremism.

By balancing security needs with the preservation of democratic freedoms, India can build a resilient digital ecosystem that safeguards citizens from the threats posed by online extremism while fostering a safe and inclusive digital space for all. 

**Soumya Awasthi** is Fellow, Centre for Strategy, Security and Technology, Observer Research Foundation.



- 1 A. Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review," International Centre for Counter-Terrorism, <https://icct.nl/publication/radicalisation-de-radicalisation-counter-radicalisation-conceptual-discussion-and>.
- 2 Edge Delta, "Breaking Down the Numbers: How much Data Does the World Create Daily in 2024?," Edge Delta, March 11, 2024, <https://edgedelta.com/company/blog/how-much-data-is-created-per-day>
- 3 Delta, "Breaking Down the Numbers: How much Data Does the World Create Daily in 2024?"
- 4 Soumya Awasthi, "Fragile State of Africa, Non-State Actors Annual Assessment," *Journal of Family Medicine and Health Care* 7, no. 1, March 2021, <https://www.sciencepublishinggroup.com/article/10.11648/j.jfmhc.20210701.11>
- 5 Sudeep Lavania, "Why Pakistan-Backed The Resistance Front Has Become Biggest Headache of Security Forces in Kashmir," *India Today*, September 14, 2023, <https://www.indiatoday.in/india/story/the-resistance-front-trf-let-lashkar-e-taiba-front-most-active-anantnag-encounter-2435627-2023-09-14>.
- 6 Kevin Collier, " Hamas Videos Spread Across Some Social Media Apps," *NBC News*, October 14, 2023, <https://www.nbcnews.com/tech/internet/hamas-videos-spread-social-media-apps-rcna120128>
- 7 Edmond Fitton Brown, "The Global Jihadi Terror Threat in September 2024," *Combating Terrorism Center Sentinel* 17, no. 8, September 2024, <https://ctc.westpoint.edu/commentary-the-global-jihadi-terror-threat-in-september-2024/>.
- 8 Brown, "The Global Jihadi Terror Threat in September 2024"
- 9 Edma Ajanovic et al., "Spaces of Right Wing Populism and Anti-Muslim Racism in Austria. Identitarian Movement, Civil Initiatives and the Fight against 'Islamisation'," *Czech Journal of Political Science*, no. 2, 2016, <https://czechpolsci.eu/article/view/34915/29805>
- 10 S. Farber and S.A. Yehezkel, "Financial Extremism: The Dark Side of Crowdfunding and Terrorism," *Terrorism and Political Violence*: 1–20, doi: 10.1080/09546553.2024.2362665.
- 11 "Misinformation About the Israel-Hamas War is Flooding Social Media," *AP News*, October 30, 2023, <https://apnews.com/article/israel-hamas-gaza-misinformation-fact-check-e58f9ab8696309305c3ea2bfb269258e>
- 12 Benjamin Jensen and Divya Ramjee, "Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs," Center for Strategic and International Studies, December 20, 2023, <https://www.csis.org/analysis/beyond-bullets-and-bombs-rising-tide-information-war-international-affairs>

- 13 Johannes Baldauf et al., “Hate Speech and Radicalisation Online,” Institute for Strategic Dialogue, 2019, <https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf>
- 14 R. Scrivens et al., “The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research,” in *Handbook of International Cybercrime and Cyberdeviance*, ed. T. Holt and A. Bossler (Palgrave Macmillan, 2020), [https://doi.org/10.1007/978-3-319-78440-3\\_61](https://doi.org/10.1007/978-3-319-78440-3_61)
- 15 “India Blocks 10,500 Social Media URLs Promoting Khalistan Referendum in Three Years,” *Greater Kashmir*, 2024, <https://www.greaterkashmir.com/latest-news/india-blocks-10500-social-media-urls-promoting-khalistan-referendum-in-three-years/>.
- 16 Ministry of Electronics and IT, Government of India, <https://pib.gov.in/PressReleaseDetailm.aspx?PRID=1700749&reg=3&lang=1>
- 17 Rimjhim Singh, “Govt Blocks Record 28,000 URLs in 2024; Facebook, X Face Maximum Takedowns,” *Business Standard*, December 28, 2024, [https://www.business-standard.com/technology/tech-news/govt-blocks-record-28-000-urls-in-2024-facebook-x-face-maximum-takedowns-124120300714\\_1.html](https://www.business-standard.com/technology/tech-news/govt-blocks-record-28-000-urls-in-2024-facebook-x-face-maximum-takedowns-124120300714_1.html)
- 18 Indian Cybercrime Coordination Centre (I4C), Government of India, “About I4C,” <https://i4c.mha.gov.in/about.aspx>
- 19 Indian Cybercrime Coordination Centre (I4C), Government of India, “Major Initiatives,” <https://i4c.mha.gov.in/initiative.aspx>
- 20 Khalid Shah, “How the World’s Longest Internet Shutdown Has Failed to Counter Extremism in Kashmir,” Observer Research Foundation, August 22, 2020, <https://www.orfonline.org/expert-speak/how-the-worlds-longest-internet-shutdown-has-failed-to-counter-extremism-in-kashmir>
- 21 “Draconian Rules: On the Impact of the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2023,” *The Hindu*, April 10, 2023, <https://www.thehindu.com/opinion/editorial/draconian-rules-the-hindu-editorial-on-the-impact-of-the-it-intermediary-guidelines-and-digital-media-ethics-code-amendment-rules-2023/article66717811.ece>
- 22 “Draconian Rules: On the Impact of the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2023”
- 23 Niam Yaraghi, “How Should Social Media Platforms Combat Misinformation and Hate Speech?,” Commentary – Brookings, April 9, 2019, <https://www.brookings.edu/articles/how-should-social-media-platforms-combat-misinformation-and-hate-speech/>
- 24 Anadi, “Deep Fakes, Deeper Impacts: AI’s Role in the 2024 Indian General Elections and Beyond,” Global Network on Extremism and Technology, September 11, 2024, <https://gnet-research.org/2024/09/11/deep-fakes-deeper-impacts-ais-role-in-the-2024-indian-general-election-and-beyond/>

# Endnotes

- 25 Tom Wheeler, “The Three Challenges of AI Regulation,” *Brookings*, June 15, 2023, <https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/>
- 26 Archit Lohani, “Countering Disinformation and Hate Speech Online: Regulation and User Behavioural Change,” Observer Research Foundation, January 25, 2021, <https://www.orfonline.org/research/countering-disinformation-and-hate-speech-online>
- 27 Todd C et al., “Assessing Outcomes of Online Campaigns Countering Violent Extremis: A Case Study of the Redirect Method,” RAND Corporation, 2018, [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR2800/RR2813/RAND\\_RR2813.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2813/RAND_RR2813.pdf)





Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,  
New Delhi - 110 002, INDIA

Ph. : +91-11-35332000. Fax : +91-11-35332005

E-mail: [contactus@orfonline.org](mailto:contactus@orfonline.org)

Website: [www.orfonline.org](http://www.orfonline.org)