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

MP-IDSA
Commentary

'Anti-Social Media': The Changing Tech of Terror

Adil Rasheed

February 11, 2026

Summary

Both the 'anti-social media' of the Dark Web and the mainstream social media promote hate, violence and indecency for profit and political ends.

The limited span of attention of today's dopamine-fed and adrenaline-rushed social media junkies, be they on TikTok, X, YouTube Shorts or Instagram posts, often bypasses the cortex of cerebral consciousness and directly targets the pre-cognitive instinctual and visceral seat of the collective unconscious.

Thus, a serious debate is currently raging over whether anti-social elements or violent extremists exploit social media platforms for their insidious purposes, or whether most social media outlets and their apps intentionally design provocative hashtags to spur prolonged, polarising debates and profit from them.

By providing content creators with anonymity and by stripping censorship regulations, the steady livestreaming of visceral online responses has become difficult to regulate, given the speed at which messages are communicated and exchanged.

Medium is the Message

In fact, the business models of many social media platforms are based on engagement algorithms, hashtags and rabbit holes that spur further online debate and thereby increase advertising revenue. In the words of Carlos Diaz Ruiz, "Incendiary, shocking content – whether it is true or not – is an easy way to get our attention, which means advertisers can end up funding fake news and hate speech." [1]

Thus, Marshall McLuhan's famous phrase "The Medium is the Message"[2] renders highly interactive social media platforms a real-time hazard to public safety and security, particularly in relation to sensitive societal issues.

In an August 2019 internal memo (leaked in 2021), a Facebook staffer admitted that "the mechanics of our platforms are not neutral"[3] and concluded that, to maximise profits, optimisation for engagement is necessary. To increase engagement, hate and misinformation become profitable. Thus, the memo states: "The more incendiary the material, the more it keeps users engaged (and) the more it is boosted by the algorithm."[4] Although Facebook has taken commendable steps to prevent incendiary

[1] Carlos Dias Ruiz, **"Disinformation is Part and Parcel of Social Media's Business Model, New Research Shows"**, *The Conversation*, 23 November 2023.

[2] Marshall McLuhan, ***The Medium Is the Massage: An Inventory of Effects***, Bantam Books, New York, 1967.

[3] Clare Duffy, Aditi Sangal, Melissa Mahtani and Meg Wagner, **"Internal Facebook Documents Revealed"**, *CNN*, 26 October 2021.

[4] Ibid.

material from appearing on its platforms, the complexities of regulating problematic content appear to be increasing.

According to a 2018 MIT Sloan study, "false rumours spread faster and wider than true information, which supports the adage that 'A lie can travel halfway around the world while truth is still putting on its shoes'". Thus, the study states that falsehoods are 70 per cent more likely to be retweeted than the truth, and reach their first 1,500 people six times faster. This effect is more pronounced for political news and for content targeting particular races, nationalities, or religions.

Thus, before examining the damage caused by encrypted social media platforms in online radicalisation, one must not overlook mainstream social media apps, which arguably serve as the first layer for the dissemination of extremist content.

The Anti-Social Media

In the wake of the white noise generated by mainstream social media channels and apps, a new trend of 'anti-social media' has emerged in recent years, which seeks to abandon mainstream platforms, reduce screen time, and seek private, intimate, or even 'analogue' communication to avoid algorithm-driven polarisation, surveillance and loneliness.[5]

However, some of these so-called anti-social media platforms have also become off-the-wall mediums for disseminating extremist propaganda. Young users strategically construct online identities and cultivate large numbers of online 'friends' based on shared interests. They even use specialised, encrypted apps in the deep web and dark web to ensure anonymity and security, and often inadvertently enter rabbit holes and echo chambers of radical forces, thus risking being radicalised and recruited by terror groups.[6]

ISIS is known to have utilised social media platforms between 2013 and 2017 to marshal their terrorist forces, agents and operatives during their terror ops. They broadcast wartime events in near-real time, transforming the Syrian conflict into one of the most socially mediated conflicts in history.

In fact, terrorists use social media for eight main purposes:

1. For propaganda
2. For scouting radical recruits

[5] Sara Wilson, **"The Era of Anti-Social Media"**, *Harvard Business Review*, 5 February 2020.

[6] Benjamin Kevaladze, **"Yes, Online Communities Pose Risks for Young People, But They Are Also Important Sources of Support"**, *The Conversation*, 21 April 2021.

3. For indoctrination and radicalisation of recruits
4. For generating finances through apps for terrorist activities
5. For conducting cyberattacks (hacking, doxxing, flaming)
6. For combat training and explosives/weapons manufacturing
7. For making terror plans and for coordinating terror attacks
8. For marshalling terrorists/agents/forces during terror ops

Despite best efforts to curb misuse, we often find that even popular social media platforms such as Facebook and Twitter struggle to prevent radicals from disseminating their messages, spreading propaganda and indoctrination, and building large networks. It is often too late for these social media platforms to detect such activities and remove them from public view.

In addition, end-to-end encrypted (E2EE) apps, such as WhatsApp, Telegram, Signal, Viber, Discord and Olvid, are widely used by extremist and radical actors to create so-called 'secure echo chambers' for radicalisation, recruitment and attack planning.[7]

Algorithmic AI

The For You Page (FYP) on TikTok demonstrates how algorithms can push users towards far-right, hateful, or violent content through a continuous stream of recommendations.[8] Similar pathways exist even on YouTube, where users exploring mainstream political topics can be guided towards extremist channels and conspiracy theories such as QAnon. In fact, YouTube has stated it plans to purge conspiracy theory content used to justify real-world violence.[9]

Algorithms pose dual risks in terrorism: extremists use them for sophisticated recruitment, propaganda (deepfakes, targeted messaging), cyberattacks and planning. The rise of deepfake AI technologies has increased the risk of data theft, socio-cognitive community hacking, fake-identity fraud and forgeries, online trolling,

[7] **"Secure Messaging Apps like Signal, Telegram Major Challenge to Counter Online Radicalisation: Government"**, *The Economic Times*, 11 December 2024.

[8] Morgan Keith, **"How TikTok's Algorithm Enables Far-right Self-radicalization"**, *Business Insider*, 6 November 2021.

[9] Kari Paul, **"Youtube Announces Plans to Ban Content Related to QAnon"**, *The Guardian*, 15 October 2020.

flaming and doxxing, as well as the proliferation of incriminating memes and hate content.

Governments and intelligence agencies around the world have also begun utilising AI to analyse vast datasets (e.g., communications and financial records) to identify patterns and potential threats. It helps process diverse data from CCTV, emails and internet logs to build intelligence. It can also help detect and respond to AI-augmented cyber threats against infrastructure.[10]

Social media platforms have also become a highly critical channel for terrorist financing (TF), with reports by institutions like the Financial Action Task Force (FATF) indicating that the highest percentage of internet-based terror activities relate to terror funding.[11] In fact, after initiating contact on public platforms, organisers often move to encrypted messaging apps to provide bank transfer, hawala, or cryptocurrency details.

Many terrorist groups use social media platforms to promote cryptocurrency addresses, thereby masking the movement of their funds and evading sanctions. Terrorists also abuse legitimate crowdfunding platforms by setting up campaigns disguised as humanitarian aid, charity, or supporting families of terror inmates.

Social Media Exploitation: India's Strategy

India's strategy against social media exploitation employs a 'whole-of-government' approach, combining legal frameworks, advanced technology and international cooperation to combat online radicalisation, propaganda and terrorist financing.

The Information Technology (IT) Rules 2021 empower law enforcement to mandate the removal of unlawful content within 24 hours. Section 69A of the IT Act is used to block websites, URLs and social media accounts related to extremist groups. Under the same legal provisions, Indian authorities have enhanced their capacity to track suspicious accounts, with a particular focus on encrypted platforms.[12]

Artificial Intelligence (AI), big data analytics and facial recognition tools are being used to detect terrorist networks, monitor radical discourse and map influence. The

[10] **"AI and National Security: Promise and Peril"**, Cognyte, 17 October 2025.

[11] **"Comprehensive Update on Terrorist Financing Risks"**, FATF Report, July 2025.

[12] **"From Social Media to OTT Platforms: Government Enforces Strict Accountability to Curb Obscenity, Misinformation and Cyber Offences Online"**, Press Information Bureau, Ministry of Information & Broadcasting, Government of India, 17 December 2025.

Defence Research and Development Organisation (DRDO) has developed NETRA (Network Traffic Analysis) to monitor encrypted communication.[13] In 2024, the Ministry of Electronics and Information Technology (MeitY) blocked thousands of terror-tainted accounts.[14]

Conclusion

In addition to the present efforts at reforming digital platforms to counter disinformation, where efforts seem to be focused on blocking, content moderation and fact-checking, attention may also be paid to reforming the online advertising market, which should be barred from financially backing extremist content. Credible punitive action should also be taken against popular 'influencers' who are found to be undermining democratic values and institutions or to be engaged in disseminating hate speech and anti-social propaganda. In the end, there needs to be a concerted campaign at the global, regional and national levels in creating standards and legislative frameworks along with mechanisms for information sharing and joint actions to counter the abuse of social media for extremist and terrorism purposes.

[13] **"NETRA: A Vigilant Eye on the Internet"**, *Research Matters*, 8 March 2017.

[14] **"MEITY Blocked Over 9,000 Accounts and Websites in 2020"**, *SabrangIndia*, 12 March 2021.

About the Author

Dr. Adil Rasheed is Research 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