# Weaponising Influence: Navigating the Impact of Social Media on Indian Armed Forces

**Colonel Satish Kumar Sinha**[@]

**Abstract**

*The advent of Web 2.0 has revolutionised communication paradigms, with social media emerging as a pervasive force influencing every facet of modern life—including national security and the armed forces. While traditionally shielded by institutional seclusion, military personnel today are intensely enmeshed in a digital ecosystem that fosters connectivity as well as vulnerability. This article critically examines the multidimensional impact of social media on the Indian Armed Forces, primarily focusing on behavioural, operational, and organisational aspects. It evaluates threats such as psychological manipulation, information or narrative warfare, ideological polarisation, and data leaks, and proposes a roadmap that balances operational security with strategic narrative dominance. The article recommends an institutional recalibration of internal communication, artificial intelligence-enabled monitoring tools, and a proactive narrative strategy to safeguard morale and operational effectiveness of the armed forces.*

## Introduction

The advent of social media has been one of the most significant technological phenomena of the 21st Century, reshaping not just personal communication but also institutional interactions, public discourse, and the strategic information environment. In

[@]**Colonel Satish Kumar Sinha** is an infantry officer currently posted at the Indian Military Academy, Dehradun. He has extensive experience across diverse terrains and has served at Army Headquarters, attended a foreign course, and been deployed abroad on a United Nations mission. His academic interests include national security and the impact of technology on warfare. He is presently pursuing a PhD in Defence and Strategic Studies.

*Journal of the United Service Institution of India*, Vol. CLV, No. 641, July-September 2025.

India, the rise of platforms such as Orkut, Facebook, WhatsApp, Twitter (now X), and Instagram has led to a profound transformation in information dissemination and citizens' engagement. Social media platforms have redefined the boundaries of individual expression, information dissemination, and collective behaviour. Originally conceptualised for civilian networking, platforms like Facebook, Instagram, and X have evolved into instruments of influence, propaganda, and even psychological warfare.[1] While these tools offer unparalleled connectivity, they also represent a double-edged sword—especially for national security institutions like the Indian Armed Forces.

In the yesteryears, the Indian Armed Forces were largely insulated from these changes due to their hierarchical and security-centric structure which ensured controlled flow of information, but the landscape has undergone a sea change. Resultant to the exponential surge in digital penetration owing to affordable smartphones and widespread data access, the military is no longer insulated from the societal transformations driven by these technologies. The ubiquitous digital technologies and increasing number of tech-savvy personnel have necessitated a reassessment of the armed forces' approach towards social media. This article examines the complex intersection between social media and the armed forces', analysing its psychological, behavioural, and institutional implications. It further explores how social media is weaponised by state and non-state actors and offers salient recommendations to counter its adverse effects while harnessing its potential for institutional gain.

## The Rise of Social Media in India and the Armed Forces

India's social media journey began in the mid-2000s with platforms like Orkut, followed by the explosive popularity of Facebook and WhatsApp in the early 2010s. The affordability of smartphones, reduced data costs post-2016 (Reliance Jio's entry and its impact), and a youth-dominated demographic profile created a fertile ground for digital engagement.

As of Mar 2024, India reported 954.59 million internet subscribers[2] and 491 million active social media identities[3]. As on date, India has emerged as the largest market by the number of users for Facebook, WhatsApp and Instagram.[4]

These social media platforms have not only facilitated communication but also fostered digital activism, the mobilisation of public opinion, and contributed towards the democratisation of information while giving voice to the voiceless. However, they have also become breeding grounds for misinformation, hate speech, surveillance, and data exploitation—issues particularly sensitive in the context of national security. The armed forces', being one of the primary stakeholders in national security, have come a long way from viewing social media with scepticism to gearing up to embrace and fully leverage it.

## Initial Caution: Armed Forces and Digital Scepticism

The armed forces have traditionally maintained a conservative approach towards public communication and media engagement, rooted in the need for operational secrecy, hierarchical command structures, and the utmost importance of political neutrality. During the early phase of social media evolution, there was a widespread perception that social media posed risks related to information leakage, breach of discipline, and reputational harm to the organisation.

However, as armed forces personnel began using these platforms in personal capacities to stay in touch with families or for entertainment, the line between institutional control and individual freedom started to blur. The first serious concerns emerged with cases of operational details being shared inadvertently on public platforms or soldiers falling victim to phishing scams and hostile intelligence agencies. Instances of honey-trapping via fake social media profiles led to court-martials and administrative action against armed forces personnel, including officers.[5] Such incidents prompted the services to issue formal advisories and guidelines on permissible digital behaviour. In a nutshell, armed forces personnel were discouraged from using social media platforms.

## Institutional Engagement and Emergent Policy

By the mid-2010s, the Indian Armed Forces began adopting a more structured approach toward social media. The Indian Army, for instance, launched official Twitter handles and began using YouTube and Instagram to broadcast ceremonial events, motivational videos, and recruitment campaigns. The navy and air

force followed suit, using these platforms to project professionalism, valour, and technological prowess.

Simultaneously, policy frameworks began to evolve. In 2013, the Indian Army issued comprehensive guidelines on social media use, later updated to ban the use of specific apps deemed high-risk due to security vulnerabilities. In 2020, an order on the subject required personnel to delete 89 apps, including Facebook, TikTok, and Instagram, citing data security concerns and potential links to foreign intelligence agencies.[6] Violations were classified as offences under the Army Act and Air Force Act, indicating the seriousness of digital compliance.

To address the growing influence of social media on perception management, the Ministry of Defence initiated collaborations with public relations experts and digital media consultants to modernise its outreach. However, these efforts remained cautious, often constrained by bureaucratic clearance procedures and deep-rooted risk aversion on reputational aspects.

## Digital Soldiers

The digital revolution within the armed forces accelerated with the entry of Generation Z (individuals born between 1996 and 2012). Having grown up in an era of smartphones, gaming, and instant communication, Gen Z exhibits behavioural patterns marked by multi-tasking, visual learning, and social validation through likes and shares.

This shift presents both opportunities and challenges. On one hand, the digital fluency of new recruits can be harnessed for Information Warfare (IW), cyber operations, and strategic communications. On the other hand, unchecked use of social media may affect mental health, discipline, and information security. A 2022 study by the Defence Institute of Psychological Research found that 47 per cent of cadets checked their phones more than ten times a day during training breaks, and 21 per cent reported feelings of restlessness when cut off from the internet.[7]

## Impact of Social Media on Armed Forces Personnel

**Psychological Conditioning and Addiction**. Social media platforms exploit reward-based neurological mechanisms, primarily through dopamine release associated with likes, comments, and

views.[8] This leads to addictive patterns of use, particularly among Gen Z recruits, whose digital immersion predates their induction into the military. For military personnel, whose duties demand emotional discipline, alertness, and mental clarity, this addiction has corrosive consequences, including impaired sleep, reduced attention spans, and diminished capacity for introspection and creativity.

**Behavioural Changes and Reduced Information Discipline**. The instant, audiovisual gratification offered by social media reduces tolerance for text-heavy, structured communication formats such as official publications or briefings. Platforms prioritise emotive content, making individuals more reactive and susceptible to misinformation. The algorithmic structures of social media foster impulsive behaviour by promoting emotionally charged content over fact-based discourse, undermining reflective thinking essential to the military ethos.[9]

**Ideological Polarisation and Echo Chamber Effect**.

- Platforms such as Instagram, Facebook, and X are designed to serve users content reinforcing their preferences, creating an 'Echo Chamber' effect that reduces exposure to diverse viewpoints and entrenches ideological polarisation.[10] This dynamic not only reduces exposure to diverse viewpoints but also entrenches ideological extremities, creating a fertile ground for polarisation. Though the Indian Armed Forces are traditionally insulated from overt politicisation due to their institutional ethos and strict codes of conduct, the pervasiveness of social media has begun to breach this historical firewall. Internal army communications have reported growing instances of political discussions, policy-related frustrations, and the circulation of divisive content within unit-level WhatsApp and Telegram groups. While these developments may appear trivial in isolation, their cumulative impact can erode unit cohesion, foster distrust in military leadership, and undermine the collective identity vital to combat effectiveness. The phenomenon is not merely theoretical; historical precedents such as the desertion of Sikh soldiers in the aftermath of Operation Blue Star illustrate how fragmented ideological perceptions can trigger organisational instability, particularly when amplified by communication technologies.[11]

- Though the armed forces are apolitical and cohesive, the seepage of ideological content via social media has created subtle ideological polarisation. The echo chamber effect, where individuals are exposed primarily to views that reinforce their own, diminishes critical thinking and fosters confirmation bias.[12] Although institutional mechanisms like community living and regimental discipline buffer against ideological polarisation, the risk remains potent.

## Social Media in Counterinsurgency and Internal Security Operations

The consequences of social media use extend into the operational realm, especially in conflict theatres. In contemporary Counter-Insurgency (CI) and Counter-Terrorism (CT) environments such as Jammu and Kashmir or the northeastern insurgency zones, militants and their supporters have weaponised social media to amplify propaganda, intimidate civilian populations, and demoralise security forces.[13] Terrorists often release real-time audio-visual content depicting armed encounters, casualty figures, or public mourning ceremonies to establish dominance over the narrative landscape.[14] These materials, unencumbered by fact-checking or institutional scrutiny, spread virally before any official response can be issued.

Military press releases, though factually accurate and responsible, often suffer from bureaucratic delays and sanitised language, limiting effectiveness in the high-velocity digital ecosystem. This temporal and tonal asymmetry contributes to psychological stress among Counterinsurgency/Counterterrorism (CI/CT) operators, who often find themselves reacting to a hostile narrative that has already taken root among the public. In majority of CI/CT incidents in the Kashmir Valley, the initial media narrative was shaped by hostile or unverified sources rather than official military accounts. Soldiers deployed in conflict zones may face moral dilemmas and psychological distress due to this asymmetry in IW.[15]

## Organisational Communication Gaps

Due to the hierarchical and security-conscious nature of the armed forces, information is typically disseminated on a 'Need-To-Know' basis through multiple chains of command. While this preserves

operational secrecy, it creates significant information gaps at the unit level, increasingly filled by external sources such as news portals, influencers, or leaked documents that often present distorted versions of reality.[16] A prominent case was the rollout of the *Agnipath* (Path of Fire) scheme, where delays in internal communication allowed misinformation to circulate widely before the official narrative could be asserted.[17] Incidents of perceived high-handed treatment of army officers by police in Odisha (Sep 2024) and Punjab (Mar 2025) were similarly distorted by rapid, sensationalised third-party narratives, creating confusion and mistrust.[18] This erodes trust in internal communication structures and challenges efficacy in the digital age.

## Espionage and Cybercrime

Espionage and cybercrime facilitated by social media remain pressing concerns. Cases have emerged wherein adversarial agencies lured Indian service members via honey-traps on social media to extract operational data or gain system access.[19] In response, the armed forces periodically issued updated lists of banned apps, with the 2020 order requiring soldiers to de-platform from Facebook, Instagram, and 87 other apps marking a major step.[20] However, manual phone inspections remain labour-intensive and prone to oversight, necessitating systemic and technology-driven countermeasures.[21]

## Recommendations

The armed forces must move from a reactive posture to a proactive digital doctrine, recognising the centrality of IW and human cognition as both vulnerability and asset. Given the multifaceted nature of social media threats to cohesion, discipline, and security, comprehensive countermeasures are essential.

- **Legal and Regulatory Framework**. India's Information Technology Rules (2021) and Digital Personal Data Protection Act (2023) offer a foundation but require stricter enforcement and refinement.[22] Lessons may be drawn from the General Data Protection Regulation and Australia's Online Safety Act for enhanced protections and platform cooperation with defence institutions.[23]

- **Artificial Intelligence(AI)-Based Monitoring**. AI tools should monitor public platforms for hostile narratives and device-level apps should flag or disable banned apps, while encrypted, locally stored data should preserve privacy alongside institutional control.[24]

- **Tri-Service Social Media Command**. Establish under Integrated Defence Staff for monitoring, training, and coordinated digital operations.

- **Civil-Military Coordination**. Work with Press Information Bureau Fact Check, Indian Computer Emergency Response Team, and Ministry of Information and Broadcasting for coherent responses to disinformation.

- **Narrative Engagement**. Expand permissible commentary, delegate approvals, and incentivise positive digital engagement while establishing a Social Media Impact Assessment Framework.

- **Unified Digital Conduct Policy**. Covering all ranks, with clear penalties, incentives, and case studies for reinforcement.

- **Social Media Literacy Training**. Integrated into all training levels for fake news identification, emotional management, and responsible engagement.

- **Narrative Response Protocols**. Establish for operations, ensuring verified, visual, and timely communications.

- **Internal Communication Transformation**. Publish non-sensitive updates on secure intranets and issue regular digital bulletins to reduce misinformation demand.

- **Psychological Resilience**. Integrate counter-propaganda modules into CI/CT training, using real-world social media scenarios to build resilience against digital manipulation.

## Conclusion

Social media is not merely a technological tool but a theatre of influence where ideas, identities, and ideologies collide. As modern warfare increasingly expands into the cognitive and informational domains, the battlefield is no longer confined to borders but it exists in hashtags, viral videos, and emotional resonance. Social

media poses a complex set of challenges to military personnel, ranging from psychological fatigue and ideological polarisation to operational compromise and cyber espionage. For the Indian Armed Forces, navigating this space requires a fine balance between operational security and cognitive freedom.

With its capacity to influence morale, discipline, and even mission success, social media must be managed with a strategy that is simultaneously restrictive, proactive, and adaptive. Addressing these challenges requires a multi-pronged strategy that incorporates legal regulation, AI deployment, communication reform, narrative engagement, and psychological resilience training. The armed forces must now evolve from a posture of cautious restraint to a position of proactive, secure, and strategic engagement with social media.

By integrating AI tools, refining communication protocols, and embracing narrative competitiveness, the armed forces can reclaim the digital space as a domain of strength rather than vulnerability. With a well-thought-out plan and embracing the change, the armed forces can transform social media from a liability into an instrument of national strength and military credibility.

## Endnotes

[1] PW Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media, 31 Jan 2024*, accessed 14 Jun 2025, https://www.youtube.com/watch?v=cNiGRhoWIqI

[2] Press Information Bureau, "Under the Digital India Initiative … As of Mar 2024, out of a total Internet Subscribers of 954.40 million in India…" Ministry of Information and Broadcasting, *Government of India, press release*, August 2, 2024, accessed 14 Jun 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2040566#:~:text=Thus%2C%2095.15%20%25%20villages%20are%20having,(CAGR)%20of%2014.26%25

[3] Sue Howe, "Social Media Statistics for India [Updated 2025]", *Meltwater Blog*, March 14, 2025 (based on *Global Digital Report 2025*), accessed 14 Jun 2025, https://www.meltwater.com/en/blog/social-media-statistics-india

[4] "Facebook Global Users Statistics 2025 | FB Demographics", *TheGlobalStatistics.com, 2025* (India leads with around 384 million Facebook users), accessed 15 Jun 2025, https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/;

"WhatsApp: The Best Meta Purchase Ever?" *Investopedia* (India is WhatsApp's largest market with ~531 million users), accessed 15 Jun 2025, https://www.statista.com/forecasts/1146773/whatsapp-users-in-india?srsltid=AfmBOoq610hm5oSw8m1woflbVXcF8lZw9mxU_hQxpn2035udSJQk4b5m; and "India Social Media Statistics 2025", *TheGlobalStatistics.com (Instagram in India has ~517 million users)*

[5] Press Information Bureau, "Honey-Trapping in Armed Forces", *Government of India*, 04 Feb 4, 2019, accessed 15 Jun Sep 2025, https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=188019

[6] Ministry of Defence, Government of India, "Full List of 89 Mobile Apps Banned for Army Soldiers", 2020; Business Today News Bureau", *Business Today*, Juny 9, 2020, accessed 15 Jun 2025, https://www.businesstoday.in/latest/trends/story/full-list-of-89-mobile-app-banned-for-army-soldiers-263551-2020-07-09

[7] Defence Institute of Psychological Research, "Study on Social Media Usage among Cadets" (New Delhi: DRDO, 2022).

[8] Christian Montag, Bernd Lachmann, Marc Herrlich, and Katharina Zweig, "Addictive Features of Social Media/Messenger Platforms and Freemium Games against the Background of Psychological and Economic Theories", *International Journal of Environmental Research and Public Health* 16, no. 14 (2019): 2612, accessed 16 Jun 2025, https://doi.org/10.3390/ijerph16142612; also available at https://www.mdpi.com/1660-4601/16/14/2612

[9] Ethan Hilman, "This Is Your Brain on Social Media: How Social Media Use Is Changing Our Attention Spans," *ResearchGate*, October 14, 2024, https://doi.org/10.58445/rars.1860

[10] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton: Princeton University Press, 2017). Book review by Ruth Abbey, accessed 17 Jun 2025, https://www.researchgate.net/publication/324548791_Cass_R_Sunstein_Republic_Divided_Democracy_in_the_Age_of_Social_Media_Princeton_NJ_Princeton_University_Press_2017_Pp_xi310_2995

[11] Pradeep P. Baruah, "Ethnic Conflict in the Military of Developing Nations: A Comparative Analysis of India and Nigeria", *Armed Forces & Society* 19, no. 1 (Fall 1992): 123–37, accessed September 26, 2025, https://doi.org/10.1177/0095327x9201900106

[12] Cass R. Sunstein, *Going to Extremes: How Like Minds Unite and Divide* (New York: Oxford University Press, 2009), accessed 17 Jun 2025, https://doi.org/10.1093/oso/9780195378016.001.0001

[13] Soumya Awasthi, "Extremist Propaganda on Social Media: Impact, Challenges, and Countermeasures," *ORF Issue Brief*, 28 Mar 2025, accessed 17 Jun 2025, https://www.orfonline.org/research/extremist-propaganda-on-social-media-impact-challenges-and-countermeasures

[14] Ibid.

[15] Col Gaurav Gupta and Thejus Gireesh, "Interpreting the War of Attention: Impact of Social Media on the Armed Forces", *CLAWS Issue Brief no. 309* Nov 2021, accessed 17 Jun 2025, https://claws.co.in/wp-content/uploads/2025/01/IB-309_Interpreting-the-War-of-Attention-Impact-of-Social-Media-on-the-Armed-Forces-1.pdf

[16] Gurmeet Kanwal, "The Imperative of Modernising Military Communications Systems", *IDSA Comment*, 16 Feb 2010, accessed 18 Jun 2025, https://www.idsa.in/publisher/comments/the-imperative-of-modernising-military-communications-systems

[17] Mayank Singh, "Agnipath Scheme: Amidst Protests, Government Issues Clarification to Bust the Myths", *The New Indian Express*, 17 Jun 2022, accessed 18 Jun 2025, https://www.newindianexpress.com/nation/2022/Jun/16/agnipath-scheme-amidst-protests-government-issues-clarification-to-bust-the-myths-2466427.html

[18] "Colonel Assault Case: Punjab and Haryana HC Transfers Probe to CBI", *The Hindu*, 16 Jun 2025, accessed 18 Jun 2025, https://www.thehindu.com/news/national/punjab/colonel-assault-case-punjab-and-haryana-hc-transfers-probe-to-cbi/article69818665.ece; "Orissa Crime Branch to Probe Custody Abuse of Army Captain, Fiancée 'Molestation", *The Times of India*, 17 Sep 2024, accessed 18 Jun 2025, https://timesofindia.indiatimes.com/city/bhubaneswar/odisha-crime-branch-to-probe-custody-abuse-of-army-captain-fiance-molestation/articleshow/113435763.cms

[19] Press Information Bureau, "Honey-Trapping in Armed Forces", *Government of India*, 04 Feb 2019, accessed 18 Jun 2025, https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=188019

[20] "Army Personnel Told to Delete Facebook, Instagram and 87 Other Apps by 15 Jun", *The Hindu*, 10 Jun 2020, accessed 18 Jun 2025, https://www.thehindu.com/news/national/army-bans-89-apps-including-facebook/article32029792.ece

[21] Nitin Desai et al., "India's Cybersecurity Challenges", *IDSA Task Force Report*, Mar 2012, accessed 19 Jun 2025, https://idsa.in/system/files/book/book_indiacybersecurity.pdf

[22] Ministry of Law and Justice, Government of India, "Digital Personal Data Protection Act", 2023. Also available at chrome-extension://

efaidnbmnnnibpcajpcglclefindmkaj/https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[23] European Union, "General Data Protection Regulation (GDPR)", 2016, accessed 19 Jun 2025, https://gdpr-info.eu/; Government of Australia, "Online Safety Act", 2021, accessed 19 Jun 2025, https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation#:~:text=The%20Online%20Safety%20Act %202021%20allows%20eSafety%20to%20investigate%20complaints,material%20removed%20from%20the%20internet

[24] Vaishali U. Gongane, Mousami V. Munot, and Alwin D. Anuse, "Detection and Moderation of Detrimental Content on Social Media Platforms: Current Status and Future Directions," *Social Network Analysis and Mining* 12, no. 1 (2022): 129, accessed 19 Jun 2025, https://doi.org/10.1007/s13278-022-00951-3