WEAPONISING INFLUENCE: NAVIGATING THE IMPACT OF SOCIAL MEDIA ON OUR ARMED FORCES

SATISH KUMAR SINHA

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 the institutional interactions, public discourse, and strategic information environment. In our country, 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 (formerly Twitter) have evolved into instruments of influence, propaganda, and even psychological warfare.[1] While these

Colonel **Satish Kumar Sinha** is an Infantry Officer presently posted at the Indian Military Academy, Dehradun.

1. P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt, 2018), p. 8.

tools offer unparalleled connectivity, they also represent a double-edged sword—especially for national security institutions like the Indian armed forces.

In 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. With 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. The paper examines the complex intersection between social media and our armed forces, analysing its psychological, behavioural, and institutional implications. The study critically examines the multi-dimensional impact of social media on the Indian armed forces, primarily focussing 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. It further explores how social media has been 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. According to the Internet and Mobile Association of India (IAMAI, 2023), India had over 759 million active internet users by 2022, with more than 60 per cent of them using at

least one social media platform on a regular basis.[2] The proliferation of regional language content and customised mobile applications for almost everything further accelerated this growth. Consequently, as on date, India has become the largest market for WhatsApp and one of the top five for Facebook and Instagram.

These social media platforms have not only facilitated communication but have also fostered digital activism, mobilisation of public opinion, contributed towards the democratisation of information, and given a voice to the voiceless. However, they have also become breeding grounds for misinformation, hate speech, surveillance, and data exploitation—issues that are particularly sensitive in the context of our 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

Our armed forces have traditionally maintained a conservative approach towards public communication and media engagement. This is deeply rooted in the need for operational secrecy as well as hierarchical command structures and the utmost importance of maintaining 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 the armed forces personnel began using these platforms in personal capacities, often to stay in touch with families or for entertainment purposes, 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 falling prey to calls of hostile intelligence agencies, primarily from our western adversary. Instances of honey-trapping via fake social

2. Internet and Mobile Association of India (IAMAI) and Kantar, *Internet in India Report 2023* (Mumbai: IAMAI, 2024), p. 16.

media profiles led to court martials and administrative action against armed forces personnel, including officers.[3] Such incidents prompted the Services to issue formal advisories and guidelines on permissible digital behaviour. In a nutshell, the armed forces personnel were discouraged to use 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, which were 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 ensure deletion of 89 apps, including Facebook, TikTok, and Instagram, citing data security concerns and potential links to foreign intelligence agencies.[4] 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 also 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 a deep-rooted risk aversion on reputational aspects.

3. Ministry of Defence, "Honey-Trapping in Armed Forces," Press Information Bureau, February 4, 2019. https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1562583. Accessed on September 1, 2025.
4. Ministry of Defence, Government of India, "Order on Prohibited Mobile Applications for Armed Forces, 2020;" *Business Today News Bureau*, "Full List of 89 Mobile Apps Banned for Army Soldiers—Including Facebook, PUBG, Zoom," *Business Today*, July 9, 2020. https://www.businesstoday.in/latest/trends/story/full-list-of-89-mobile-app-banned-for-army-soldiers-263551-2020-07-09. Accessed on September 1, 2025.

DIGITAL SOLDIERS

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

This shift presents both opportunities and challenges. On the one hand, the digital fluency of new recruits can be harnessed for information warfare, cyber operations, and strategic communications. On the other, unchecked use of social media may affect mental health, discipline, and information security. A 2022 study by the Defence Institute of Psychological Research (DIPR) 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. Apropos, it is important to understand the impact of social media on the armed forces personnel.

IMPACT OF SOCIAL MEDIA ON ARMED FORCES PERSONNEL

Psychological Conditioning and Addiction

Social media platforms exploit reward-based neurological mechanisms, primarily through the release of dopamine associated with likes, comments, and views.[5] This leads to addictive patterns of use, particularly among Gen Z recruits, whose digital immersion predates their induction into the military. The most immediate psychological impact stems from the addictive architecture of social media platforms, which leverage dopamine-triggering mechanisms such as "likes," "shares," and emotionally resonant content to keep users engaged. As numerous neuroscientific studies confirm, each digital affirmation or act of passive consumption results in a transient release of dopamine, the so-called "happiness hormone",

5. 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, p. 2612.

producing a behavioural feedback loop that is strikingly similar to substance addiction.[6] For military personnel, whose duties demand a high degree of emotional discipline, alertness, and mental clarity, this addiction has corrosive consequences, including impaired sleep patterns, reduced attention spans, and a diminished capacity for introspection and creativity.

Behavioural Changes and Reduced Information Discipline

The instant, audio-visual gratification offered by social media reduces tolerance for text-heavy, structured communication formats such as official publications, correspondence or briefings. As platforms are designed to prioritise emotive content, individuals become more reactive, impatient, and susceptible to misinformation. The algorithmic structure of social media further fosters impulsive behaviour by promoting emotionally charged content over fact-based discourse. The cycle reinforces impulsiveness and undermines the reflective thinking essential to military ethos.

Ideological Polarisation and Echo Chamber Effect

Platforms such as Instagram, Facebook, and X (formerly Twitter) are designed to serve users content that reinforces their existing preferences or biases, a phenomenon commonly referred to as the "echo chamber" effect.[7] 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 have been 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 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 the military leadership, and undermine the collective identity so vital to combat

6. Ibid., p. 2612.
7. Cass R. Sunstein, *Echo Chambers: Bush v. Gore, Impeachments, and Beyond* (Princeton, NJ: Princeton University Press, 2001), p. 12.

effectiveness. The phenomenon is not merely theoretical; historical precedents such as the desertion of a few Sikh soldiers in the aftermath of Operation Blue Star illustrate how fragmented ideological perceptions can trigger organisational instability, particularly when amplified by communication technologies.

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. Although institutional mechanisms, such as community living and regimental discipline, buffer against ideological polarisation, the risk remains potent.

SOCIAL MEDIA IN COUNTER-INSURGENCY AND INTERNAL SECURITY OPERATIONS

The consequences of social media use extend into the operational realm, too, especially in conflict theatres. In contemporary Counter-Insurgency (CI) and Counter-Terrorism (CT) environments, such as Jammu and Kashmir (J&K) or the northeastern insurgency zones, militants and their supporters have weaponised social media to amplify propaganda, intimidate civilian populations, and demoralise the security forces. Terrorists often release real-time audio-visual content depicting armed encounters, casualty figures, or public mourning ceremonies to establish dominance over the narrative landscape.[8] These media materials are typically unencumbered by fact-checking or institutional scrutiny, allowing them to spread virally before any official response is issued.

On the other hand, military press releases, though factually accurate and responsible, suffer from bureaucratic delays and overly sanitised language, limiting their effectiveness in the high-velocity digital ecosystem. This temporal and tonal asymmetry contributes to psychological stress among CI/CT operators, who often find themselves reacting to a hostile narrative that has already taken root among the public. A 2022 study conducted by the Centre for

8. Arindam Banerjee, "Social Media and Insurgency in Kashmir," *ORF Occasional Paper*, no. 310, 2021.

Land Warfare Studies (CLAWS) confirmed that in over 60 per cent 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, especially those deployed in conflict zones, may face moral dilemmas and psychological distress due to this asymmetry in information warfare.[9]

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 approach preserves operational secrecy, it creates significant information gaps at the unit level. These gaps are increasingly being filled by external sources such as news portals, social media influencers, or even leaked documents, which often present distorted or incomplete versions of the reality. A prominent case in point is the rollout of the Agnipath scheme, wherein delays in internal communication allowed misinformation to circulate widely before the official narrative could be asserted. Incidents of recent high-handed treatment meted out to army officers by the police in Odisha (September 2024, Bharatpur Police Station) and Punjab (March 2025, Patiala) have similarly been distorted by the rapid and often sensationalised dissemination of third-party narratives, creating confusion and mistrust among the rank-and-file. This systemic delay in information flow erodes the credibility of internal communication structures and raises questions about the efficacy of internal communication arrangements within the armed forces in the digital age.

ESPIONAGE AND CYBER CRIME

The threat of espionage and cyber crime facilitated by social media remains a pressing concern. Numerous cases have emerged in recent years wherein adversarial intelligence agencies lured Indian Service members through honey-trap techniques on social media platforms, eventually extracting sensitive operational data or access to secure

9. Asm Sharfuddin, "Psychological Warfare and Its Impact", 2025, https://doi.org/10.13140/RG.2.2.20285.58088. Accessed on September 1, 2025.

systems.[10] The Indian armed forces have responded by periodically issuing updated lists of banned applications and instituting punishable clauses for non-compliance. The Indian Army's 2020 order requiring soldiers to de-platform from Facebook, Instagram, and 87 other apps marked a significant step in this direction. However, manual monitoring methods, such as physical inspection of phones, remain labour-intensive and vulnerable to oversight. Thus, while the risks now have been acknowledged, and partially addressed, the scale and sophistication of the threat continue to evolve, demanding more systemic and technologically driven counter-measures.

ANALYSING POTENTIAL OPTIONS

The time has come for the Indian armed forces to move from a reactive posture to a proactive digital doctrine which acknowledges the centrality of information warfare in modern conflict and the importance of human cognition as both a vulnerability and a strategic asset. Given the multi-faceted nature of social media threats to military cohesion, discipline, and security, it is imperative to develop and implement comprehensive counter-measures at the strategic, institutional, and individual levels. The following are recommended:

- The first area demanding immediate attention is the legal and regulatory framework governing social media usage in national security contexts. India's current regulatory structure, including the Information Technology Rules (2021) and the recently passed Digital Personal Data Protection Act (2023), offers a foundational basis for content moderation and data governance.[11] However, stricter enforcement and continuous refinement are needed to address the evolving tactics of digital subversion. The Indian government could draw lessons from the European Union's General Data Protection Regulation (GDPR) and Australia's

10. Kriti Singh, "Exploitation of Social Media by Enemy: Honeytrap Operations," *CAPS In Focus*, Centre for Air Power Studies, January 28, 2016, https://capsindia.org/wp-content/uploads/2021/10/CAPS_Infocus_KS_09.pdf. Accessed on September 1, 2025.
11. Ministry of Electronics and Information Technology, Government of India, New Delhi 2023, Digital Personal Data Protection Act, 2023, https://www.meity.gov.in/. Accessed on September 1, 2025.

Online Safety Act (2021), both of which institute rigorous penalties for non-compliance by platforms and offer enhanced protections for high-risk user groups, including children and security personnel. Specific amendments must also mandate that major platforms cooperate with defence institutions in real-time removal of harmful content and provide Artificial Intelligence (AI)-driven tools for internal security scanning.

- AI holds transformative potential in content moderation, surveillance, and operational security within the military context. Globally, billions of social media messages are exchanged daily, making manual review infeasible. AI-based monitoring tools, trained on local languages and dialects, can identify, classify, and flag malicious content in real time. For the Indian armed forces, two parallel AI modules should be developed. First, an institutional-level AI platform that continuously monitors public social media for mentions of sensitive keywords, personnel data leaks, or hostile narrative building. This system could also track geo-tagged misinformation in border areas or CI/CT zones. Second, a device-level application could be installed on the personal phones of Service members, automatically flagging or disabling banned apps and alerting users to the presence of potentially classified content. While this approach may raise privacy concerns, these can be mitigated by ensuring that all data is stored locally, encrypted, and accessible only to the user unless manual consent is provided. Such a model preserves individual agency while enhancing institutional control. Given the volume of digital traffic, manual monitoring is neither scalable nor effective. AI-based solutions can automate detection of fake content, track the spread of propaganda, and identify sensitive leaks. Custom software should be developed for the armed forces—one module for organisational monitoring and another for personal device management to flag banned apps or content. Privacy concerns can be mitigated through transparent data ownership policies.
- Establish a Tri-Service Social Media Command under the Integrated Defence Staff (IDS) to coordinate content, monitor hostile campaigns, and train personnel in digital operations.

- Coordinate with civilian agencies like Press Information Bureau (PIB) Fact Check, Computer Emergency Response Team (CERT-IN), and Ministry of Information & Broadcasting to ensure a coherent government-wide response to disinformation.
- Narrative control and proactive public engagement remain central. Historically, the Indian armed forces have adopted a cautious, often reticent posture in dealing with the media. This approach, though rooted in operational prudence, has allowed adversarial narratives to fill the vacuum. It is recommended that a comprehensive review of the social media policy be undertaken with the structural reforms wherein the list of topics permissible for public commentary by personnel is expanded, approval authority for social media releases is delegated to lower echelons (e.g., one-star rank officers), institutional tolerance for minor public backlash in exchange for narrative speed becomes acceptable, and incentive structures, such as awards or commendations for units and individuals that engage positively with the public in digital spaces are institutionalised. Further, the establishment of a Social Media Impact Assessment Framework to periodically evaluate the efficacy of information campaigns would ensure strategic alignment of our efforts in this domain.
- Develop a Unified Digital Conduct Policy covering all ranks, including officers, Junior Commissioned Officers (JCOs) and Other Ranks (ORs). This must include penalties, incentives, and real-life case studies for reinforcement. Defeating a hostile narrative requires a stronger counter-narrative. The armed forces must shed their media reticence and adopt a proactive stance. Policy changes should include:
- Reducing over-classification of information.
- Delegating content approval authority to lower ranks.
- Instituting 6–12 hour timelines for digital responses.
- Incentivising content creation that aligns with institutional values.
- A metrics-based evaluation system should be implemented to assess the effectiveness of digital information campaigns and reward positive engagement.

- Integration of social media literacy into military training at all levels. This should include modules on identifying fake news, managing emotional responses to online content, and engaging responsibly.
- Institutionalisation of narrative response protocols for operations such as surgical strikes, internal unrest, or CI/CT actions. Verified, visual, and timely communication must become the norm.
- Internal organisational communication must also undergo digital transformation. The current system, often dominated by slow, hierarchical message flows, is ill-suited to the fast-paced, information-rich environments that soldiers now inhabit. It is recommended that generic, non-sensitive information related to welfare schemes, promotion policies, or organisational updates be published regularly on secure intranet portals accessible to all ranks. Headquarters at the command and corps levels should issue weekly or bi-weekly digital bulletins, summarising key developments and dispelling circulating rumours. Such proactive disclosure not only builds institutional trust but also reduces the demand for external information sources, thereby curbing misinformation.
- Finally, psychological preparation of military personnel against digital propaganda must be integrated into formal training modules, particularly for personnel deployed in CI/CT environments. The *modus operandi* of terrorists and their support groups' psychological operations via social media aimed at demoralising own troops while glorifying their cause/acts must be disseminated to our soldiers threadbare and exercises can be designed to prepare military personnel to face such propaganda. Ultimately, all propaganda must be countered not with denial but with transparent, well-timed, and emotionally resonant official narratives.

CONCLUSION

Social media has emerged as a powerful and ubiquitous tool. It has assumed multiple roles wherein ideas, identities and influence converge. The complex nuances of social media lend itself for positive as well as harmful usage including affecting behavioural

changes. The armed forces personnel are confronted with the complex challenge of social media ranging from psychological fatigue and ideological polarisation to operational compromise and cyber espionage.

It is imperative that our armed forces adopt a nuanced strategy which balances the organisational requirements and yet leverages social media to the hilt without ceding space to inimical elements. Such a strategy will compulsorily be multi-pronged, incorporating changes at the strategic, operational and individual levels. Towards this end, certain recommendations have been made in the article which include reforming legal regulations, AI deployment at national and organisational levels, creating competitiveness in the narrative by the armed forces through time-bound releases and audit of effectiveness, transforming internal communication within the organisation, and psychological preparation of soldiers. By implementing changes in a proactive manner, our armed forces can turn social media from a liability to a force multiplier.