

SOCIAL MEDIA IN MILITARY CONFLICTS: EMERGING TRENDS AND LESSONS

SATISH KUMAR SINHA AND SUBODH SHAHI

*Smartphones are potential weapons. They blur the boundaries between war and daily life. Apps and platforms don't just tell the story of conflict; they can directly shape military operations.*¹

– Matthew Ford, Senior Lecturer in War Studies,
Swedish Defence University

INTRODUCTION

Social media emerged in the early 2000s and, owing to its distinctive attributes, rapid proliferation, instantaneous dissemination of information, interactive content, and the plausible anonymity of users, it has evolved into a powerful and pervasive force across multiple domains of contemporary life. With a

Colonel **Satish Kumar Sinha** is an infantry officer presently posted in a field formation in the northeastern region. The officer has rich experience of serving in different terrain, a tenure at Army Headquarters, a foreign course and deployment abroad in the United Nations Mission. His academic interests include national security and the impact of technology on warfare. Currently, he is pursuing his PhD in Defence and Strategic Studies.

Colonel (Dr) **Subodh Shahi** is an expert in Defence and Strategic Studies. He is presently serving as Associate Professor and Director at the Amity Institute of Defence and Strategic Studies.

1. Matthew Ford, "How Smartphones are Changing the Reality of War," Swedish Defence University, August 26, 2025. <https://www.fhs.se/en/swedish-defence-university/stories/2025-08-26-how-smartphones-are-changing-the-reality-of-war.html>

Social media has assumed diverse and often decisive roles, including facilitating story-telling, real-time documentation, organising search-and-rescue efforts, disseminating propaganda, mobilising domestic and transnational supporters, enabling fund-raising, conducting intelligence collection, keeping surveillance over adversary forces, and even directly contributing to the targeting processes.

rapid evolution, it has grown much beyond its original function of being a benign platform for interpersonal communication. Instead, social media has transformed into a consequential instrument capable of shaping perceptions, behaviour, and outcomes across political, social and military spheres.²

In the armed conflict zone, where large scale human suffering, destruction of infrastructure, disruption of essential services and catastrophic humanitarian crises occur, and the truth gets fiercely

contested, social media has assumed diverse and often decisive roles, including facilitating story-telling, real-time documentation, organising search-and-rescue efforts, disseminating propaganda, mobilising domestic and transnational supporters, enabling fund-raising, conducting intelligence collection, keeping surveillance over adversary forces, and even directly contributing to the targeting processes. While journalistic and academic analyses of these phenomena are essential, it is equally imperative to examine social media through the lens of the armed forces. Such an understanding is critical in order to enable militaries to harness its potential while simultaneously countering adversarial exploitation.

Three armed conflicts over the past five years have witnessed a much-enlarged role of social media: the India–Pakistan non-contact conflict of May 2025 (Operation Sindoor by India and Operation Bunyan-um-Marsoos by Pakistan), the recent Israel–Hamas War commencing (October 2023 to January 2024), and the ongoing Russia–Ukraine War since February 2022.

2. David Patrikarakos, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century* (New York: Basic Books, 2017), pp. 2–5.

These conflicts differ markedly in scale, duration, and character.

A comparative examination of these conflicts reveals that social media's influence extends well beyond narrative construction and morale enhancement. Instead, the role of social media has become critical in the domains of information warfare, the digital kill chain, and the audit and arbitration of contested claims. Within the information warfare domain, social media demonstrates a pronounced capacity to amplify the strategic impact of tactical events, compress political

and military decision-making cycles, shape the nature and proportionality of state responses, influence international public opinion, and affect battles for legitimacy and diplomatic manoeuvre. Even more interestingly, social media has emerged as a consequential enabler within the modern digital kill chain wherein military functions such as collection of granular intelligence on the movement and disposition of forces, facilitation of targeting processes, and execution of post-strike battle damage assessment are aided by social media.³ Open-source imagery, geolocated content, and user-generated data increasingly contribute to operational awareness, blurring traditional distinctions between civilian digital activity and military intelligence processes.

Further, in the process of auditing claims and arbitrating victory, social media has assumed an unprecedented role by putting evidence-based narratives for public consumption and as a corollary to either corroborate or de-legitimise official accounts. Verified visual material, crowd-sourced analysis, and independent open-source investigations have grown manifold

In the process of auditing claims and arbitrating victory, social media has assumed an unprecedented role by putting evidence-based narratives for public consumption and as a corollary to either corroborate or de-legitimise official accounts.

3. NATO Strategic Communications Centre of Excellence (StratCom COE), *Social Media as a Tool of Hybrid Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016), pp. 23–27, <https://stratcomcoe.org/publications/social-media-as-a-tool-of-hybrid-warfare/>. Accessed on January 24, 2026.

and these form the backbone in forming perceptions of success, failure, and proportionality, often constraining state narratives and influencing international responses.

Taken together, these developments underscore a fundamental shift: social media can no longer be regarded as an ancillary to an armed conflict. It has emerged as a frontline instrument capable of generating tactical, operational, and strategic effects. This study analyses the three aforementioned conflicts to identify emerging trends and distil lessons relevant to the armed forces, with particular emphasis on preparedness, adaptation, and doctrinal integration.

OPERATION SINDOOR AND OPERATION BUNYAN-UM-MARSOOS (MAY 2025)

In retaliation for a Pakistan-origin terrorist attack on tourists in Pahalgam (District Anantnag, Jammu & Kashmir) on April 22, 2025, India conducted a series of non-contact precision strikes against terrorist infrastructure located in Pakistan during the night of May 6–7, 2025. Pakistan responded with counter-strikes on May 8, 2025, following which the Indian armed forces expanded the spatial scope of operations, targeting eleven military installations across Pakistan. India employed a range of advanced precision-strike capabilities, including fighter aircraft such as the Rafale and Su-30MKI, missiles, including the BrahMos, and Harop loitering munitions. Pakistan deployed the J-10, JF-17, and F-16 fighter aircraft, Babur ground-launched cruise missiles, Ra'ad II air-launched cruise missiles, HQ-9 air defence systems, and unmanned aerial systems, including the Turkish-origin ANKA drones.⁴

With a ceasefire coming into effect on May 10, 2025, which was also announced first on a social media platform, Truth Social, by US President Trump, the non-contact kinetic phase of the conflict concluded, limiting the duration of the conflict to 72–96 hours. The outcome of the conflict remained

4. "Dummy Aircraft to BrahMos and Rafale Jets, How India Tactically Planned Counter-Offensive Against Pakistan", *Indian Defence News*, May 16, 2025, <https://www.indiandefensenews.in/2025/05/dummy-aircraft-to-brahmos-and-rafale.html>

contested and a parallel war unfolded in the digital and cognitive domains through social media platforms such as X (formerly Twitter), Telegram, Instagram, YouTube, and WhatsApp. The question of decisiveness, thus, extended beyond the physical battlespace to the digital cognitive arena, where social media played a central and, arguably, determinative role too.

Social Media as a Tool in the Cognitive Domain

Approximately 54 per cent of Indians turn to social media for factual information and news.⁵ Widespread reliance on social media for news during a conflict is axiomatic. The digital space, comprising social as well as traditional media, soon got filled with conflicting narratives, misinformation, disinformation, and propaganda.⁶ Sensing the huge impact of inimical elements in the social media space, on May 8, 2025, the Government of India directed social media companies, primarily X, to block approximately 8,000 accounts in order to curb misinformation, disinformation, and circulation of provocative content.⁷ About a week earlier, India had banned 16 Pakistan-based YouTube channels and restricted access to other Pakistani social media outlets deemed to be disseminating misleading or inflammatory material.⁸ These measures reflected an explicit recognition of the strategic importance of the information environment during the conflict.

Within hours of the initial kinetic actions, both sides moved rapidly to establish what may be termed “first-mover-truth,” releasing their respective narratives. Pakistan initiated a fast-cycle information campaign through Inter-Services Public Relations (ISPR) affiliated accounts and proxy handles

-
5. “54 Per cent People in India Turn to Social Media for Factual Info: Oxford University Press Study,” *The Tribune* (India), <https://www.tribuneindia.com/news/nation/54-per-cent-people-in-india-turn-to-social-media-for-factual-info-oxford-university-press-study-407736/>
 6. *Four Days in May: The India-Pakistan Crisis of 2025*, (Stimson Centre, May 28, 2025), <https://www.stimson.org/2025/four-days-in-may-the-india-pakistan-crisis-of-2025/>
 7. “X to Block Over 8,000 Accounts in India After Government Order,” *NDTV*, May 8, 2025, <https://www.ndtv.com/india-news/x-to-block-over-8-000-accounts-in-india-after-government-order-8366168>
 8. “Provocative, Communal Content: Centre Bans Pakistan YouTube Channels, Flags ‘Misinformation,’” *The Times of India*, April 28, 2025, <https://timesofindia.indiatimes.com/india/provocative-communal-content-centre-bans-pakistan-youtube-channels-flags-misinformation/articleshow/120685473.cms>

to contest India's claims and create ambiguity, an approach followed by Pakistan after the Indian air strikes at Balakot on February 26, 2019. However, unlike earlier episodes, the information environment obtaining in 2025 was markedly more mature. India's narrative, increasingly buttressed by sophisticated Open-Source Intelligence (OSINT) evidence, began to dominate the digital discourse.

Further, claims made by the state were subjected to rigorous scrutiny by independent OSINT analysts, eroding any single actor's ability to monopolise the truth. The veracity of official statements issued by government spokespersons was measured against evidence circulating on social media platforms that could be independently verified. Pakistan's defence minister attracted criticism for citing social media as evidence to support his claim of the downing of an Indian fighter jet during an interview with CNN on May 8, 2024.⁹ Over time, India gained a perceptible advantage in the digital narrative contest, tilting the balance of legitimacy in its favour. This advantage was amplified by India's large, digitally active diaspora and by a sustained effort to ensure alignment between official claims and verifiable evidence. Pakistan's information campaign, by contrast, remained largely domestically focussed and was unable to generate independently corroborated proof. Ultimately, a broad consensus emerged that India had inflicted significant damage, while the impact of the Pakistani strikes remained comparatively limited.

Social media-driven narratives also influenced global opinion, amplified by professional military commentators and leading think-tanks such as the RAND Corporation, International Institute for Strategic Studies (IISS), Brookings Institution, and Chatham House. These institutions frequently referenced OSINT material circulating on platforms such as X, thereby lending additional credibility and reach to evidence-based assessments.

9. "Pakistan Defence Minister's Live TV Blunder: Khawaja Asif Cites Social Media to Claim Indian Jets were Shot Down, Gets Fact-Checked," *The Economic Times*, May 8, 2025, <https://economictimes.indiatimes.com/news/new-updates/pakistan-defence-ministers-live-tv-blunder-khawaja-asif-cites-social-media-to-claim-indian-jets-were-shot-down-gets-fact-checked/articleshow/120983764.cms>

Social Media as a Cog in the Digital Kill Chain

Beyond narrative construction, social media performed three specific military functions during the conflict: post-strike damage assessment, vectoring and target refinement, and morale sustenance. Numerous OSINT practitioners including veterans, independent defence analysts, and private research collectives released high-resolution Synthetic Aperture Radar (SAR) and Electro-Optical (EO) imagery within 6–18 hours of the reported strikes. These assessments identified precise locations, crater dimensions, and patterns of damage, reaching both military professionals and the general public directly. While the armed forces possess dedicated Post Strike Damage Assessment (PSDA) mechanisms, such OSINT inputs supplemented internal assessments, particularly in the early stages. On the Pakistani side, individuals publicly claimed the establishment of OSINT Cells intended to analyse open-source data and relay findings to military authorities in near real timeframe.

Vectoring and target refinement also benefited immensely from OSINT based on social media, primarily Telegram. Multiple Telegram groups collated and disseminated granular data, including radar site coordinates, convoy movements, fuel storage locations, and surface-to-air missile deployment patterns. Aggregation of such data enabled pattern recognition and contributed to the refinement of targeting decisions. While the extent of direct operational integration remains opaque, the availability of such information undeniably compressed sensor-to-shooter timelines in the digital domain. This effect, in particular, has become more profound in the Russia-Ukraine War.

During the India-Pakistan conflict, social media also functioned as a powerful morale sustainer by shaping the digital psychological ecosystem. The perception reinforced by OSINT-verified evidence that India was prevailing contributed to elevated public confidence and high morale among military personnel. Another significant impact of social media pertained to legal posturing and escalation dominance. Both sides sought to establish legitimacy through what may be termed a “digital justification

Social media has become deeply embedded not only in narrative formation and morale sustenance but also as an integral component of the digital kill chain.

The conflict marks a decisive shift from social media as a peripheral informational tool to a core opinion-maker and operational enabler.

architecture,” grounded largely in the social media discourse. Also, social media became an instrument of escalation control and strategic signalling. India consistently articulated that its initial strikes were justified actions and limited to terrorist infrastructure only, and that subsequent targeting of Pakistani military installations occurred solely in response to Pakistani actions. The messaging was duly calibrated for domestic as well as international audiences.

RUSSIA–UKRAINE WAR (SINCE FEBRUARY 2022)

The second military conflict for studying the role of social media is the Russia–Ukraine War, which commenced in February 2022, and continues till date as one of the longest-duration inter-state wars of the post–Cold War era. During the course of the war, the character of warfare as also the role of social media, have evolved substantially. Social media has become deeply embedded not only in narrative formation and morale sustenance but also as an integral component of the digital kill chain. The conflict marks a decisive shift from social media as a peripheral informational tool to a core opinion-maker and operational enabler.

In the aftermath of the outbreak of hostilities, reliance on social media for news consumption increased sharply. By May 2022, approximately 77 per cent of Ukrainians reported using social networks as their primary source of news, up from 62 per cent in 2020.¹⁰ In 2025, preference for usage of social media platforms for news among the Ukrainian population has been: Telegram - 65.7 per cent, YouTube - 61.2 per cent, Facebook - 57.8

10. *Social Media are the Most Popular Source of Information among Ukrainians, but TV is the more Trusted One—Survey*, Institute of Mass Information, June 2, 2022, <https://imi.org.ua/en/news/social-media-are-the-most-popular-source-of-information-among-ukrainians-but-tv-is-the-more-trusted-i45921>

per cent, Viber - 48 per cent and Instagram - 29.1 per cent.¹¹

Social Media as a Military Tool

In the initial phases of the war, Ukraine rapidly integrated social media into its fire execution architecture. Informal civilian networks and volunteer groups supplied actionable intelligence, including real-time locations of Russian troop concentrations, force movements, artillery positions, fuel depots, and air defence systems to enable near real-time detection, classification, targeting, and post-strike verification targets. In an innovative manner, the Ukrainian government quickly adapted its DIIA (an acronym for “the state and me”) app, launched in 2020 as part of digital transformation, with eVorog

(e-Enemy) Chatbot over Telegram in March 2022.¹² It enables verified users to report Russian troop movements, equipment locations, and suspected collaborators. The app requires users to authenticate via an e-passport system, and users can upload photos and videos of enemy assets. The app automatically attaches a timestamp and geolocation, turning raw civilian sightings into actionable “civil intelligence” for the armed forces. Once submitted, these crowd-sourced reports are aggregated and fed into-

In the initial phases of the war, Ukraine rapidly integrated social media into its fire execution architecture. Informal civilian networks and volunteer groups supplied actionable intelligence, including real-time locations of Russian troop concentrations, force movements, artillery positions, fuel depots, and air defence systems to enable near real-time detection, classification, targeting, and post-strike verification targets.

11. *What Social Media Do Ukrainians Use?*, OPORA Survey (2025), https://www.oporaua.org/en/polit_ad/24068-mediaspozhyvannia-ukrayintsiv-v-umovakh-povnomasshtabnoyi-viini-opituvannia-opori-24068

12. Chandler Governance, “Delivering Digital Transformation in Ukraine”, *Governance Matters Magazine*, <https://chandlergovernance.com/governancematters/delivering-digital-transformation-in-ukraine>

centralised military systems.¹³ In the beginning of June 2023, Ukraine's Vice Prime Minister Mykhailo Fedorov reported that 6,74,000 Ukrainians had already used the eVorog chatbot for reporting on the Russian military.^{14, 15} Similarly, the ePPO app has been used extensively by the Ukrainians to report about aerial threats.¹⁶

Ukraine's early and innovative employment of low-cost First Person View (FPV) drones proved significant at the tactical level, and the targeting ecosystem became increasingly refined over time. Studies and expert analyses indicate that Ukraine's battlefield targeting cycle underwent major compression during the conflict. While the early phases often saw intelligence processing and strike coordination take many hours, integrated drone Intelligence, Surveillance, Reconnaissance (ISR) and digital battlefield management systems enabled sensor-to-shooter cycles measured in minutes by 2025.¹⁷ Social media platforms continued to facilitate strike validation and generate cues for follow-on attacks or repeat punishment to target(s).

The Russian military adopted a parallel, though a structurally distinct, approach. Pro-Kremlin military bloggers ("milbloggers"), operating through Telegram-based 'Z' channels, played a dual role: shaping domestic opinion and acting as distributed reconnaissance nodes. The Russian social media functioned not merely as a commentary space but as a sensor network feeding inputs to shooters. For generation of civilian intelligence, Russian launched various Telegram-based apps such as Cyber Squad (Кибердружина),

-
13. Mykhailo Fedorov, "How the War Makes Ukraine Leap Forward in Digitalization," German Marshall Fund of the United States, May 19, 2022, <https://idnext.eu/a-citizen-like-chatbot-allows-ukrainians-to-report-to-the-government-when-they-spot-russian-troops-heres-how-it-works>.
 14. "People's Intelligence: 674,000 Ukrainians Have Already Used the Enemy Chatbot," UNN (Ukrainian National News), June 13, 2025, <https://unn.ua/en/news/peoples-intelligence-674000-ukrainians-have-already-used-the-enemy-chatbot>.
 15. "Drone-Assisted Targeting and the Emerging Operational Tempo in the Russo-Ukrainian War," CTC Sentinel, March 2025, https://ctc.westpoint.edu/wp-content/uploads/2025/03/CTC-SENTINEL-032025_cover-article.pdf
 16. "Ukrainian App Allows Civilians to Report Russian Missile Sights to Air Defense," *The Jerusalem Post*, October 16, 2022, <https://www.jpost.com/international/article-719836>.
 17. Lieutenant General Philip Campose (Retd), "What Indian Military can Learn from Ukraine's Optimisation of Drone Warfare," *The Week*, October 29, 2025, <https://www.theweek.in/news/defence/2025/10/29/ukraine-optimisation-of-drone-warfare-and-lessons-for-the-indian-military.html>

Z-Pentest/Cyber Army of Russia, Privet Bot, Amina (Tracking App) Premise (to pay individuals in occupied Ukrainian territories to take photos of infrastructure and military assets) and the most significant one, Radar.NF (Радар.НФ). The Radar app, launched in September 2023, functioned on the 'point and report' mode of the phone and was significant in gathering real-time data on Ukrainian drones and missiles.¹⁸

Both sides increasingly employed Artificial Intelligence (AI)-enabled image classification tools, for analysing imagery circulating on social media to conduct automated damage assessments and to determine whether repeat strikes were required. On both sides, non-state civilian actors, operating through open digital networks, have emerged as precision-strike multipliers, fundamentally altering traditional assumptions about military exclusivity over targeting processes.

Post-strike damage assessment based on high-resolution commercial satellite imagery from providers such as Maxar Technologies and Capella Space, routinely supported or refuted official claims of damage. On multiple occasions, Russian assertions of having destroyed Ukrainian air defence systems such as S-300 batteries were publicly disproven within hours through OSINT-based geolocation and imagery analysis circulated on social media. This continuous cycle of public verification imposed reputational costs on inaccurate claims and significantly constrained narrative manipulation.

Another consequential effect of the pervasive social media use was the erosion of traditional deception, concealment, and denial techniques. Persistent reporting, rapid dissemination of imagery, and crowd-sourced analysis rendered deception increasingly difficult, costly, and time-sensitive. The window for exploiting ambiguity narrowed considerably, compelling both sides to adapt camouflage, decoy, and dispersal measures at greater expense.

18. "Russia Asks Citizens to Use New App to Report Drones and Other Attacks," *The Washington Post*, September 20, 2023, <https://www.washingtonpost.com/world/2023/09/20/russia-app-drone-citizens-war/>.

ISRAEL–HAMAS WAR (2023–24)

The recent Israel-Hamas War is the third recent phenomenon under examination to understand the role of social media during an armed conflict. On October 7, 2023, Hamas launched a coordinated surprise attack in southern Israel, including an assault on the Nova music festival near Re'im, where approximately 360 civilians were killed. The *blitzkrieg* operation by Hamas resulted in the deaths of around 200 people and the abduction of approximately 250 individuals. In response, Israel initiated immediate air strikes and subsequently launched a full-scale ground offensive in the Gaza Strip on October 27, 2023. In the course of the operations, Israel also conducted strikes against Hezbollah, the Houthis, and Iran-linked organisations, thus, extending military action into Lebanon, Syria, Yemen and Iran. Following sustained diplomatic engagement, led by the United States, a ceasefire became effective from January 19, 2025.¹⁹

The conflict demonstrated a dense and volatile information environment characterised by real-time contestation, unprecedented civilian visibility, high kinetic tempo, and rapid global emotional contagion. In this conflict, social media was not merely a parallel theatre but functioned as a primary domain through which the conflict was experienced, interpreted, and judged by global audiences.

Social Media Campaign by Hamas

In its opening salvo, Hamas exploited social media with considerable effectiveness to generate psychological shock and trauma. GoPro-recorded attack footage, images and videos of abducted hostages, and mobile phone recordings were rapidly disseminated across digital platforms. Hamas initially framed its messaging around a “victory” narrative against a formidable enemy, which subsequently transitioned into a carefully curated victimhood and resilience narrative. This shift was deliberate and instrumental. Visual representations of civilian suffering in Gaza

19. “Timeline and Overview of the 2023 Israel-Hamas War,” Britannica, <https://www.britannica.com/event/Israel-Hamas-War>

were weaponised to generate coercive political pressure, particularly on governments sensitive to public opinion and humanitarian norms.

The cognitive and digital campaign by Hamas and its affiliates appeared premeditated, relying on emotionally evocative content framing and ideological polarisation. The effects of kinetic actions were magnified through short and highly visceral video clips circulated via TikTok, Telegram, and WhatsApp, which emerged as the fastest transmission vectors for the masses. Hamas demonstrated how a non-state actor, unencumbered by institutional hierarchies, legal accountability, or fact-checking constraints, could dominate the information warfare space through first-mover advantage and rapid upload cycles. Between October 7 and November 17, 2023, TikTok alone removed over 1.16 million videos related to the conflict which violated its guidelines on account of violence, terrorism, hate speech, and misinformation. Further, approximately 9,33,000 bot-generated comments associated with conflict-related hashtags were also deleted.²⁰

IDF Engagement on Social Media

The Israel Defence Forces (IDF) responded with a more institutionalised and structured information strategy and showcased remarkable adaptability. Their counter-narrative relied on rebuttal mechanisms, amplification of official messaging, evidence-based claims, emphasis on lawful targeting, hostage recovery efforts, moral framing, and counter-terrorism justification. In the immediate aftermath of the October 7, attacks, Israel's Ministry of Foreign Affairs and the IDF significantly expanded their digital outreach. Between October 6 and 12, 2023, the Foreign Ministry's account grew from approximately 9,38,000 to 1.2 million followers, while the IDF's official account expanded from around 1.5 million to over 2 million followers.²¹ This surge reflected the centrality of the digital battlespace.

20. "Our Continued Actions to Protect the TikTok Community During the Israel-Hamas War," TikTok Newsroom, November 23, 2023, <https://newsroom.tiktok.com/our-continued-actions-to-protect-the-tiktok-community-during-the-israel-hamas-war>

21. "In Israel-Hamas Conflict, Social Media Become Tools of Propaganda and Disinformation," DFRLab, October 12, 2023, <https://dfrlab.org/2023/10/12/in-israel-hamas-conflict-social-media-become-tools-of-propaganda-and-disinformation/>

The Israel– Hamas conflict unfolded within a far denser information environment and a geographically compressed battlespace, resulting in significantly accelerated decision and verification cycles. OSINT assessments were often produced within minutes rather than hours.

Effects Achieved by Social Media in the Conflict

The war illustrated the capacity of social media to mobilise global public opinion, particularly in Western capitals and university campuses. Large numbers of non-combatants, including students, diaspora communities, activists, and ideologically aligned individuals even geographically far removed from the conflict, actively participated in legitimising one side

while delegitimising the other. Public discourse, rather than state authority alone, increasingly defined the perceived morality and legitimacy of the war, with social media platforms assuming a different character; TikTok, Instagram, and WhatsApp primarily transmitted emotionally charged content; Telegram carried more sustained operational and war-related information; and X emerged as the preferred platform for analytical debate, OSINT dissemination, and adjudication of contested claims.

Open-source intelligence–based claim verification mirrored patterns observed in Operation Sindoor and the Russia–Ukraine War, but with notable differences. The Israel–Hamas conflict unfolded within a far denser information environment and a geographically compressed battlespace, resulting in significantly accelerated decision and verification cycles. OSINT assessments were often produced within minutes rather than hours. Similarly, the cycles of narrative and audit were also faster. The explosion at the Al-Ahli Arab Hospital in Gaza on October 17, 2023, which resulted in substantial civilian casualties, with estimates ranging from 100 to 500 victims, had both sides issuing competing accounts almost immediately. Within hours, OSINT analysts leveraged social media circulated videos, geolocation, trajectory

analysis, and crater assessment to challenge and refine official claims.²²

In this conflict too, the legitimacy contest was effectively adjudicated in the digital sphere, with social media functioning as a quasi-referee among competing narratives. As a corollary, the traditional authority of legacy media such as official briefings, mainstream news outlets, and television broadcasts was visibly diminished. Their role increasingly shifted from primary narrators to secondary amplifiers or interpreters of evidence already circulating within the social media–OSINT ecosystem. In the whole gambit, social media emerged as the primary medium for delivery of effect, underscoring that narrative formation often precedes and outpaces post-strike damage assessment and factual verification cycles.

Social media platforms served as the primary arena in which initial perceptions were formed, contested, and stabilised. Truth remained fluid and disputed, while social media functioned as the principal mechanism through which public opinion was shaped.

COMPARATIVE ANALYSIS

A comparative assessment of these conflicts—the India–Pakistan conflict of May 2025, the ongoing Russia–Ukraine War, and the Israel–Hamas war of 2023–24—reveals several convergent patterns of strategic significance. First, the meaning and interpretation of war now begin to crystallise well before evidence-based assessments are disseminated through official channels. Narrative formation precedes factual verification. In all three cases, social media platforms served as the primary arena in which initial perceptions were formed, contested, and stabilised. Truth remained fluid and disputed, while social media functioned as the principal mechanism through which public opinion was shaped. Warfare has, thus, become increasingly social, distributed, participatory, and audience-driven. The armed forces are now

22. Human Rights Watch, “Gaza: Findings on October 17 al-Ahli Hospital Explosion”, <https://www.hrw.org/news/2023/11/26/gaza-findings-october-17-al-ahli-hospital-explosion>

compelled to fight simultaneously in the kinetic domain and within the global digital public sphere.

Second, no state or institution retains monopoly control over the digital information environment. Mass participation, often unstructured and spontaneous, defines the cognitive battlespace. Across all three conflicts, platforms such as TikTok, Instagram, and WhatsApp primarily amplified emotionally charged content, while Telegram and X emerged as key conduits for operational information, analytical discourse, and OSINT dissemination. This functional differentiation across platforms reflects an emergent ecology in which content type, speed, and audience segmentation determine strategic impact.

Third, non-state actors have emerged as consequential precision multipliers. OSINT analysts, civilian volunteers, drone engineers, independent researchers, diaspora activists, and digital influencers have performed functions traditionally associated with state militaries and intelligence agencies. Their roles have included target identification, damage assessment, technical innovation in drone employment, emotional amplification, coercive influence on political decision-makers, and mobilisation of transnational public opinion. In several instances, these activities preceded and shaped diplomatic manoeuvres, effectively preempting formal state engagement.

Fourth, claims regarding strikes, damage, and operational success are now subject to rapid verification through OSINT, with findings disseminated almost instantaneously to global audiences. False or exaggerated claims are quickly repudiated, often resulting in significant credibility costs for government agencies. Conversely, claims that align with independently verifiable evidence enhance institutional credibility. Social media has, thus, assumed the role of a near real-time referee and validator of contested claims.

Fifth, social media has evolved into a global marketplace of legitimacy in which public verdicts are rendered on the justifiability and proportionality of military actions.²³ Legitimacy is no longer conferred solely through

23. Andrew Hoskins and Ben O'Loughlin, *War and Media: The Emergence of Diffused War* (Cambridge: Polity Press, 2015), pp. 78–82.

international law, state declarations, or institutional diplomacy; it is increasingly mediated through digitally networked publics. In each of the examined conflicts, the perceived moral standing of belligerents was shaped as much by social media narratives and visual evidence as by formal legal arguments.

Finally, social media has transcended its traditional role as a communication medium and has become an integral component of the digital kill chain. Across all three conflicts, social media enabled military functions such as intelligence generation, munition vectoring, target refinement, and post-strike damage assessment. Platforms facilitated the identification of geo-tagged targets, continuous surveillance of force movement, dissemination of sensor data, and provision of extended sensing inputs to shooters. The FPV drone ecosystem in the Russia–Ukraine War, in particular, demonstrated the unequivocal utility of social media-enabled networks in compressing sensor-to-shooter timelines and enhancing precision in kinetic operations.

Taken together, these convergent trends indicate that future conflicts will be defined as much by contests over perception, legitimacy, and information dominance as by conventional military superiority. For the armed forces, the imperative is clear: operational success in contemporary warfare demands doctrinal, organisational, and technological integration of the digital-cognitive domain alongside traditional kinetic capabilities.

EMERGING TRENDS AND RECOMMENDATIONS

The growing centrality of social media in contemporary armed conflict must be acknowledged explicitly. Social media is no longer a peripheral information tool; it has emerged as an integral component of both the digital kill chain and the cognitive kill chain. It is evident that in future conflicts, social media will be the primary medium through which news of strikes will first emerge and accompanying narratives will get established during the opening salvo. Thereafter, social media will continue to outpace legacy media and official briefings in shaping perceptions. By the time formal statements are released through traditional channels, the informational

centre of gravity on social media will have shifted to subsequent developments, rendering delayed responses ineffective. To remain synchronised with this accelerated tempo, the Indian armed forces must institutionalise mechanisms for proactive and responsive engagement with social media. The recent reorganisation of the Command Cyber Operation and Support Wing and the decision to raise the Information Operation Group and Information Operation Detachments are much needed and welcome steps. These new organisations must be fully aligned to leverage the power of social media.

The establishment of dedicated social media cells at brigade, division, and equivalent headquarters across the three Services is an inescapable requirement. These cells should operate under clearly defined protocols enabling the rapid release of curated and verified content, supported by authenticated imagery and evidence. Their mandate must include countering disinformation and sustaining a continuous cycle of timely, factual public communication. At operational and tactical headquarters, standard operating procedures must strike a careful balance between operational security and the imperative of rapid, credible public communication. At higher levels, information warfare doctrine and policies require revision to formally integrate social media with explicit instructions on information release authorities, legal constraints, and ethical boundaries.

The exponential proliferation of advanced civilian technologies has fundamentally transformed open-source intelligence. OSINT today frequently complements, and, in certain cases, rivals, traditional military intelligence. A diverse ecosystem of civilian analysts, technologists, and enthusiasts now generates military-grade intelligence on a continuous basis, rendering their contributions invaluable during conflict. This valuable resource must be tapped by the Indian armed forces intensely and purposefully by establishing OSINT liaison cells at the tactical and operational levels. These cells should maintain structured engagement with credible OSINT communities and social media groups specialising in geospatial analysis, imagery interpretation, and technical forensics. At the Service headquarters

level, select OSINT groups may be discreetly resourced and aligned to Service-specific requirements under conditions of plausible deniability. Such arrangements would allow the armed forces to benefit from civilian innovation while mitigating the reputational risk in case of any ethical or legal infringement by these groups.

Recent conflicts have also demonstrated that OSINT-enabled targeting is no longer theoretical but operationally consequential. Memoranda of Understanding (MoUs) with commercial satellite imagery providers and trusted OSINT networks will be essential for timely access to high-resolution electro-optical and synthetic aperture radar imagery. Further, effective exploitation of OSINT-enabled targeting will require doctrinal adaptation, organisational restructuring, and clearly articulated protocols governing preliminary target indicators, corroboration standards, and validation thresholds. These frameworks need to be defined clearly in order to translate OSINT into kinetic effects.

Fact-checking and authentication have emerged as among the most effective counters to propaganda and disinformation. As elucidated above in respect of all three wars, OSINT-based evidence circulating on social media not only repudiated false claims but also imposed substantial credibility costs on the actors propagating them. Conversely, verifiable and transparent claims strengthened institutional legitimacy. It is evident that a rapid and credible fact-checking mechanism can arrest misinformation campaigns in their early stages, before they achieve critical mass. Existing public relations architectures in our armed forces possess limited capability in this domain. Information operation warfare cells at various headquarters must, therefore, be reoriented and resourced to maintain continuous monitoring of digital platforms, identify emerging disinformation, and disseminate evidence-backed rebuttals at speed. This capability will inevitably require sustained investment in commercial imagery procurement, structured collaboration with civilian analysts, and paid access to specialised OSINT products.

Artificial Intelligence (AI) offers significant potential advantages during conflicts. AI-enabled tools can assist in segregating propaganda

Social media has undergone a qualitative transformation in both significance and utility, emerging as a core variable of the contemporary battlespace. It now operates simultaneously within the cognitive and kinetic dimensions of warfare, with both domains increasingly fused.

from authentic information, generating actionable intelligence, collating evidence to counter disinformation, facilitating targeting processes, and creating dynamic repositories of verified content. It is recommended that the Indian armed forces must pursue the development of customised AI solutions tailored to Service-specific operational requirements and the task could be accomplished by specialised public and private sector agencies under the appropriate oversight of the Services.

Social media must be fully integrated into the military training and preparedness cycles. Major war games and field exercises should explicitly incorporate social media dynamics for narrative shaping, psychological operations, targeting support, and post-strike damage assessment. Such simulations will enable commanders and staff to internalise the realities of operating under conditions of persistent digital scrutiny and contested legitimacy, thereby enhancing preparedness for future conflict.

CONCLUSION

The armed conflicts examined in this study unequivocally demonstrate that social media has undergone a qualitative transformation in both significance and utility, emerging as a core variable of the contemporary battlespace. It now operates simultaneously within the cognitive and kinetic dimensions of warfare, with both domains increasingly fused. Social media has become integral to the conduct and outcomes of modern conflict, shaping perceptions, enabling operational effects, and influencing strategic decision-making. Actors who leverage social media effectively for narrative formation, legitimacy contests, intelligence generation, targeting,

and post-strike damage assessment, will gain substantial advantage over their adversaries.

For the Indian armed forces, the lessons emerging from these conflicts should serve as a call for reorientation and reforms in order to enable effective usage of social media. Treating social media as an ancillary or supporting function is no longer tenable; it must instead be incorporated as an integral element of force design and operational planning. Future conflicts are likely to be characterised by high-tempo social media campaigns, contested and rapidly

shifting narratives, disputed battle damage claims, dense OSINT-driven information environments, and digital war in the cognitive domain. Under such conditions, social media will directly influence legitimacy claims, institutional credibility, diplomatic manoeuvrability, operational advantage, and escalation control.

The measures recommended in this paper, doctrinal and policy revisions to formally integrate social media, formulation of clear standard operating procedures and engagement protocols, establishment of MoUs with commercial imagery providers and credible OSINT networks, structured liaison with civilian analytical communities, and the creation of dedicated social media cells at brigade, division, and equivalent headquarters across the Services, will be immensely valuable in leveraging social media during conflicts.

The logic for reform is straightforward. The role and impact of social media have been empirically established across major conflicts fought within the span of the last five years. This trajectory is unlikely to reverse. The imperative for India, therefore, is not merely to adapt reactively but to prepare proactively in order to remain ahead of the curve where possible, or at least,

The role and impact of social media have been empirically established across major conflicts fought within the span of the last five years. This trajectory is unlikely to reverse. The imperative for India, therefore, is not merely to adapt reactively but to prepare proactively in order to remain ahead of the curve.

to retain the capacity to operate effectively within an increasingly volatile and contested information environment. Failure to do so risks conceding decisive advantage not on the battlefield alone, but in the broader contest where wars are interpreted, legitimised, and ultimately judged.