USI Occasional Paper

No 7 - 2026

(Estd. 1870)

Colonel Satish Kumar Sinha
Colonel Subodh Shahi

About the Occasional Paper

This occasional paper examines the joint United States-Israel air campaigns - Operations Epic Fury and Roaring Lion-against Iran and analyses their strategic, operational, and doctrinal implications for contemporary warfare. The study explores the political and military objectives of the campaigns, the pursuit of air superiority through intelligence-led targeting, the role of integrated air and missile defence systems, and the increasing influence of Artificial Intelligence (AI) in planning and execution. It assesses the effectiveness and limitations of air power, intelligence, and manned–unmanned teaming, while highlighting the evolving character of conflict in an era of multi-domain operations. Drawing lessons from the successes and shortcomings of all participants, this paper identifies critical implications for India's air defence architecture, command and control systems, intelligence integration, force protection, and theatre command structures. It argues that future military advantage will depend increasingly on networked systems, doctrinal coherence, AI-enabled decision support, and anticipatory adaptation.

Introduction

"Smartphones are potential weapons. They blur the boundaries between war and daily life. Apps and platforms do not just tell the story of conflict; they can directly shape military operations"

- Matthew Ford, Senior Lecturer in War Studies, Swedish Defence University[1]

Social media emerged in the early 2000s and, owing to its distinctive characteristics—including rapid proliferation and instantaneous dissemination of information, interactive content, and the relative anonymity afforded to users—has evolved into a powerful and pervasive force across multiple domains of contemporary society. With accelerated evolution, it has grown much beyond its original function of being a benign platform for interpersonal communication. 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 space, 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. These include facilitating storytelling, real-time documentation, organising search-and-rescue efforts, disseminating propaganda, mobilising domestic and transnational supporters, enabling fundraising, 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 from an armed forces analysis perspective. Such an understanding is critical to enable militaries to harness its potential while simultaneously countering adversarial exploitation.

Three-armed conflicts over the past five years have witnessed a significantly expanded role for social media: the India–Pakistan limited military confrontation of May 2025 comprising India's Operation Sindoor and Pakistan's Operation Bunyan-um-Marsoos; the Israel–Hamas conflict commencing in Oct 2023; and the ongoing Russia–Ukraine conflict since Feb 2022. These conflicts differ markedly in their 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, 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 (PSBDA) are aided by social media.[3] Open-source imagery, geo-located 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, crowdsourced analysis, and independent open-source investigations have grown manifold and 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 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 against the allegedly Pakistan-sponsored terrorist attack on tourists at Pahalgam[4] in Anantnag district, Jammu and Kashmir, on 22 Apr 2025, India conducted a series of non-contact precision strikes against the terrorist infrastructure in Pakistan on the night of 06–07 May. Islamabad responded with counter-strikes on 08 May, following which the Indian Armed Forces (IAF) expanded the spatial scope of operations, targeting eleven military installations across Pakistan. India also employed a range of advanced precision-strike capabilities, including fighter aircraft such as the Rafale and Su-30MKI, and missiles including the BrahMos, and Harop loitering munitions. Pakistan deployed J-10, JF-17, and F-16 fighter aircraft, Babur ground-launched cruise missiles, Ra'ad II air-launched cruise missiles, HQ-9 systems, and unmanned aerial systems including Turkish-origin Anka drones.[5]

With ceasefire coming into effect on 10 May, which was first announced on social media platform Truth Social by United States (US) President Donald Trump[6], and then confirmed by respective ministerial representatives of the two states[7], the non-contact kinetic phase of the conflict reached a conclusion, limiting the duration of the conflict to 72–96 hrs.

The outcome of the conflict remained contested. Meanwhile, a parallel war unfolded in the digital and cognitive domains through different 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, a determinative role too.

Social Media as a Tool in Cognitive Domain

Approximately, 54 per cent of Indians turn to social media for factual information and news.[8] Widespread reliance on social media for news during the conflict is axiomatic. The digital space, comprising of both social as well as traditional media, soon got flooded with conflicting narratives, misinformation, disinformation, and propaganda.[9] Sensing the huge impact of inimical elements in social media space, the Government of India on 08 May directed social media companies, primarily X, to block approximately 8,000 accounts in order to curb the circulation of misinformation, disinformation, and provocative content.[10] This action came a week after India, in Apr 2025, banned 16 Pakistan-based YouTube channels and restricted access to other Pakistani social media outlets which were deemed to be disseminating misleading or inflammatory material.[11] These measures reflected an explicit recognition of the strategic importance of the information environment during a conflict.

Immediately after the strikes, India as well as Pakistan released their statements to harness the 'The First Mover' advantages. While Pakistan, through its Inter-Services Public Relations apparatus, affiliated news outlets, and social media handles, attempted to create ambiguities akin to those witnessed after the Balakot strike in Feb 2019, the Indian narrative was relatively more grounded in evidentiary material, particularly visual evidence and satellite imagery. Pakistan's Defence Minister Khawaja Asif attracted bad press and loss of credibility for citing social media as a proof during an interview with CNN on 08 May to support his claim of Pakistan having shot down five Indian fighter aircrafts.[12] On the Indian side too, some social media handles shared fabricated imagery, leading to some damage to the credibility. Uzair Rizvi, a Delhi-based fact-checker and media literacy trainer, observed that it felt as if a month's worth of misinformation has bombarded social media within the first few hours.[13]

Interestingly, the evolution of information environment played a significant role in checking veracity of competing claims. It emerged clearly that claims made by either party were subjected to intense scrutiny, weighed against Open-Source Intelligence (OSINT)-driven evidence by multiple actors, and the state's ability to monopolise the truth stood significantly diminished.

Over time, the Indian narrative gained a perceptible advantage due to its high-link ability to readily and publicly prove its claims with accessible evidence. In

addition, the magnification of the Indian narrative through large diaspora globally also contributed positively.

Social Media as a Cog in Digital Kill Chain

In addition to being a front runner in the battle of narratives, during the conflict, social media performed four specific military functions: intelligence generation, targeting, PSBDA, and morale sustenance. Several individuals posted numerous pictures and videos of military personnel and equipment with clearly identifiable landmarks or embedded geolocation data such as radar site coordinates, convoy movements, fuel storage locations, and surface-to-air missile deployment patterns. On the Pakistani side, individuals including self-styled strategic analysist Zaid Hamid publicly claimed to have established OSINT cells, which intended to analyse open-source data and disseminate findings to military authorities in near real-time. On both sides, analysis of data generated from social media became a valuable source of intelligence. Precise and time-sensitive inputs derived from social media platforms, particularly Telegram, facilitated target refinement and vectoring. While the extent of integration of intelligence generation from social media and vectoring of munition by the Indian or Pakistan military remains unclear, this phenomenon has become far more profound in the Russia–Ukraine conflict.

PSBDA was immensely augmented by inputs from numerous OSINT practitioners including veterans, independent defence analysts, and private researchers who

used high-resolution synthetic aperture radar and electro-optical imagery. High-resolution Maxar imagery and images from Indian satellites were extensively used by analysts who often produced assessment of the strikes within 06-18 hrs of engagement. These reports carried minute details of strikes such as precise locations, crater dimensions, and patterns of damage. Besides enriching military PSBDA, the public availability of such assessments on social media captured public attention and emerged as a centrepiece in adjudicating the legitimacy of competing claims.

During the conflict, social media also played a pivotal role in sustaining morale of general public as well as military personnel. The digital ecosystem, largely dominated by social media, disseminated verifiable evidence that reinforced the perception of India's operational advantage. This perception contributed to elevated public confidence and sustained 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 news media and social media discourse, justifying the use of force and the selection of targets. Social media also emerged as an instrument of escalation control and strategic signalling. India consistently articulated that its initial strikes were legitimate and proportionate actions limited to terrorist infrastructure, and that subsequent

targeting of Pakistani military installations occurred solely in response to Islamabad's actions. The messaging was duly calibrated for both domestic as well as international audiences.

Russia–Ukraine Conflict (Feb 2022-Ongoing)

Another case study to understand the role of social media is the Russia–Ukraine conflict, which commenced in Feb 2022 and continues till date as one of the longest surviving interstate conflicts of the post-Cold War era. During the entire duration, the character of warfare along with 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 as an operational enabler.

In the aftermath of 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.[14] In 2025, preference for usage of social media platforms for news among Ukrainian population has been 65.7 per cent on Telegram, 61.2 per cent on YouTube, 57.8 per cent on Facebook, 48 per cent on Viber, and 29.1per cent on Instagram.[15]

Social Media as a Military Tool

In the initial phases of this conflict, 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 (AD) systems to enable near real-time detection, classification, targeting, and post-strike verification targets. In an innovative manner, the Ukrainian government quickly launched its DIIA—an acronym for Ukrainian phrase *Держава і Я* (Derzhava i Ya), which translates to 'The State and I'—application in 2020 as part of Ukraine's digital transformation, with the introduction of eVorog (eEnemy) chatbot over Telegram in Mar 2022.[16] It enables verified users to report Russian troop movements, equipment locations, and suspected collaborators. The application requires users to authenticate via an e-passport system, and they can upload photos and videos of enemy assets. The application automatically attaches a timestamp and geolocation, turning raw civilian sightings into actionable 'Civil Intelligence' for the armed forces. Once submitted, these crowdsourced reports are aggregated and fed into centralised military systems.[17] In the beginning of Jun 2023, Ukraine's Vice Prime Minister Mykhailo Fedorov reported that 6,74,000 Ukrainians had already used the eVorog chatbot for reporting on Russian military activity.[18] Similarly, the *Protypovitryana Oborona* (ePPO or electronic

AD) application has been used extensively by Ukrainians to report on aerial threats.[19]

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 has undergone major compression during the conflict.[20] While the early phases of the conflict often required several hours for intelligence processing and strike coordination, the integration of drone-based intelligence, surveillance, and reconnaissance with digital battlefield management systems had reduced sensor-to-shooter cycles to a matter of minutes by 2025.[21] Social media platforms continue to facilitate strike validation and generate cues for follow-on attacks or repeat punishment to target(s).

The Russian military adopted a parallel, though structurally distinct, approach. Pro-Kremlin military bloggers or 'Milbloggers' operating through Telegram-based 'Z' channels played a dual role—shaping domestic opinion and acting as distributed reconnaissance nodes. Russian social media functioned not merely as a commentary space but as a sensor network feeding inputs to shooters. For generation of civilian intelligence, Russia launched various telegram-based apps such as *Кибердружина* (Cyber Squad), Z-Pentest or Cyber Army of Russia, Privet Bot, Amina (tracking app), and *Радар.НФ* (Radar.NF), the most significant one. The application

launched in Sep 2023, functions on 'Point-and-Report' mode on mobile phones, and has been significant in gathering real-time data on Ukrainian drones and missiles.[22]

Both sides increasingly employed Artificial Intelligence (AI)-enabled image classification tools, 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 the targeting processes.

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

Another consequential effect of pervasive social media use has been the erosion of traditional deception, concealment, and denial techniques. Persistent reporting, rapid dissemination of imagery, and crowdsourced analysis

have rendered deception increasingly difficult, costly, and time-sensitive. The window for exploiting ambiguity has narrowed considerably, compelling both sides to adapt camouflage, decoy, and dispersal measures at greater expense.

Israel–Hamas Conflict (2023–Ongoing)

The recent Israel-Hamas conflict is the third recent phenomenon under examination to understand the role of social media during armed conflict. On 07 Oct 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* (light warfare) operation by Hamas resulted in 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 27 Oct 2023. During the operations, Israel also conducted strikes against the Hezbollah, Houthis, and other Iran-linked organisations, thus extending its military action into Lebanon, Syria, Yemen, and Iran. Following sustained diplomatic engagement led by the US, a ceasefire was finalised to be effective from 19 Jan 2025.[23]

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 functioned as the primary domain

through which the conflict was seen, perceived, and judged across the world.

Social Media Exploitation by Hamas

As revealed by Israel Defense Forces (IDF) investigations, Hamas collected sensitive intelligence on IDF bases and equipment from soldiers' social media activity for years prior to the raid on IDF army bases in Oct 2023. Reportedly, Hamas had established a social media intelligence unit in 2018 which expanded to approximately 2,500 individuals and tracked nearly 1,00,000 IDF military personnel through social media. Hamas also reportedly learned, through social media posts by IDF personnel, about a hidden kill switch on the Merkava Mark 4, Israel's most advanced main battle tank, that could disable the vehicle and render it inoperable. Reportedly, Hamas employed this technique during attacks on IDF bases, especially while assaulting Nahal Oz base, where 53 soldiers were killed and 10 were taken hostage.[24]

Immediately after the attack, Hamas rapidly released GoPro-recorded attack footage, images, and videos of abducted hostages, and mobile phone recordings. The operation was showcased by Hamas as 'Victory' against a formidable enemy[25], in parallel to broader narratives centred on 'Victimhood' and 'Resilience'. An argument can be made that visual representations of civilian suffering in Gaza generated coercive political pressure by mobilising international support, particularly within western democracies.

The cognitive and digital campaign by Hamas relied on circulating emotionally evocative content and fostering an ideological polarisation. The effects of kinetic actions were magnified and amplified through short and highly visceral video clips circulated via TikTok, Telegram, and WhatsApp, which emerged as the fastest transmission vectors for masses. Hamas demonstrated how a non-state actor, unencumbered by institutional hierarchies, legal accountability, or fact-checking constraints, could leverage social media to dominate the digital information space. The scale and intensity of uploading content is evident from the fact that between 07 Oct and 17 Nov 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.[26]

Israel Defense Forces Engagement on Social Media

The IDF responded with a more institutionalised and structured information strategy and showcased remarkable adaptability. Its 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 07 Oct attacks, Israel's Ministry of Foreign Affairs and IDF significantly expanded their digital outreach. Between 06

and 12 Oct 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 two million followers.[27] This surge reflected the centrality of the digital battlespace.

The IDF, especially its intelligence outfit, Unit 8200, extensively used AI-based programme 'Lavender' with considerable inputs drawn from social media to mark all suspected operatives of Hamas which proved crucial for targeting.[28] Similarly, another AI-based targeting tool used by IDF, *Habsora* (Hebrew for 'The Gospel') synthesised all data and produced a target list with due prioritisation, enabling bombing in exponentially high numbers. According to Lieutenant General Aviv Kochavi (Retd), Chief of the General Staff of the IDF, the Gospel system generated 100 targets a day during Israel's 11-day war with Hamas in May 2021.[29] Hence, according to figures released by the IDF, during the first 35 days of the war Israel attacked 15,000 targets in Gaza.[30]

Effects Achieved by Social Media during 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, many of whom were geographically far removed from the conflict, actively participated in legitimising one side while delegitimising the other. The contest over legitimacy and morality was

largely decided by public discourse spearheaded on social media. Various social media platforms acquired distinct roles; 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 the adjudication of contested claims.

The patterns observed regarding OSINT-based claim verification in Operation Sindoor and the Russia–Ukraine conflict also prevailed during this event. However, since the tactical battle area featured a far denser information environment within a geographically compressed space, input availability was more intense and claim verification cycles were much faster often occurring within minutes rather than hours. The explosion at Al-Ahli Arab Hospital in Gaza on 17 Oct 2023, which resulted in 100-500 civilian casualties, witnessed rapid shifts in blames. However, within hours, OSINT analysts leveraged social media circulated videos, geolocation, trajectory analysis, and crater assessment to challenge, corroborate, and refine official claims.[31]

In this conflict too, social media played the role of a quasi-referee in deciding the legitimacy contest in the digital sphere. As a corollary, the authority and credibility 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 and OSINT ecosystem. The conflict revealed that the social media-based narrative formation and PSBDA precedes the official narrative and formal factual verification cycles.

Comparative Analysis

A comparative examination of above-mentioned conflicts points to a common recurring patterns with both strategic and tactical implications. First, social media-based narrative preceded the official accounts. The meaning of events began to take shape well before evidence-based assessments emerged and narrative construction consistently outpaced the formal process of factual verification. During this early phase, truth remained contested and provisional, while social media played a decisive role in shaping public opinion. Consequently, social media prevailed as the primary arena in which early perceptions were formed, challenged, and subsequently settled. Warfare has, thus, become increasingly social, distributed, participatory, and audience-driven. Armed forces are now compelled to operate simultaneously in the kinetic battlespace and the global digital information environment.

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 the principal 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 that were 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 pre-empting 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, the 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.[32] Legitimacy is no longer conferred solely through international law, state declarations, or institutional diplomacy; it is increasingly mediated through digitally networked publics. In all the conflicts reviewed, judgments about the moral position of the warring sides were driven not only by legal arguments, but also by social media narratives and visual evidence.

Finally, social media has transcended its traditional role as a communication tool. It has become an operational enabler and an integral cog of the digital kill chain. These platforms aid intelligence generation, munition vectoring, target refinement, and PSBDA. During the conflicts under review, social media platforms were of immense value to identify location-tagged targets, track troop movements, share sensor data, and provide additional information for conducting attacks. The use of FPV drones in the Russia–Ukraine conflict clearly demonstrated how social media-enabled networks can shorten the time between detection and attack; thus, improving the accuracy of combat operations exponentially.

Viewed collectively, these patterns show that future conflicts will be influenced not only by military power, but also by struggles over perception, legitimacy,

and information control in which social media will play an important role in shaping narratives as also in facilitating military functions. Armed forces, therefore, need to embed digital and cognitive capabilities, particularly those related to social media, into their doctrine, organisation, and technology, alongside traditional kinetic power.

Emerging Trends and Recommendations

During conflicts, social media's centrality in information warfare and its increasing role in the digital kill chain are the most important trends. In the cognitive domain, social media is likely to remain a dominant player with considerable lead over legacy media. Most likely, it will be social media where the news of strikes will emerge first, and perceptions formed on social media will remain ahead of the official accounts released formally. By the time official and legacy media catch up with developments, social media's centre of gravity would have moved ahead to newer developments. Eliot Higgins, the founder of Bellingcat, a global OSINT agency, aptly remarked that the ubiquity of social media means that the 'Fog of War' is being replaced by a 'Firehose of Information'. In modern conflict, the first report of a tank crossing a border does not come from a satellite; it comes from a teenager's TikTok.[33] The digital space will also be highly crowded, with extensive public participation, while social media will generate and disseminate vast volumes of information ranging from verified facts to half-truths, misinformation, and deliberate falsehoods.

As an operational enabler, facilitating direct military places social media will be an invaluable asset for intelligence generation, targeting, and conducting PSBDA. The integration of social media into military systems, as witnessed in recent conflicts, is likely to intensify in future and confer-marked operational advantages. Further, the ubiquitous nature of social media will impact camouflage and concealment measures currently in use will require a review. In its role as a referee for settling competing claims with OSINT-backed evidence, social media will directly impact the credibility of official statements. In addition, social media is likely to play a noteworthy role in garnering legitimacy during conflict as well as in strategic signalling and escalation control.

The first and foremost recommendation for the Indian Armed Forces is to recognise formally and explicitly the pivotal role of social media during conflict. This will be the foundational step towards initiating requisite changes for integration and leveraging this powerful tool. The Indian Armed Forces must institutionalise the mechanisms for proactive and responsive engagement with social media. The recent re-organisation of Command Cyber Operation and Support Wing and the decision to raise 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. In addition, dedicated social media cells are required to be established at division, brigade, and

equivalent levels in the three services. These social media cells will monitor the social media traffic, filter out information of relevance, and issue prompt factual rebuttals accompanied by evidence to take the steam out of propaganda and misinformation. A delicate balance will have to be ensured to maintain operational security while divulging details to debunk adversarial narratives. At the higher echelons of the military, policies and guidelines must be framed to fully integrate social media in information warfare while defining the ethical, legal, and moral boundaries and codes of conduct.

Since the digital space is crowded with competing claims and initial narratives that rapidly gain momentum regardless of their veracity, it is recommended that a multi-level fact-checking mechanism be instituted to promptly refute frivolous claims before the adversary's narrative garners critical mass. The rebuttals must be prompt and duly supported by evidence. This requires continuous monitoring of the digital space, especially social media, speedy identification of propaganda, and dissemination of fact-based content. The formation headquarters must be suitably reoriented and resourced to execute this task.

OSINT has evolved to rival military intelligence in qualitative terms, and it scores over military intelligence quantitatively. Armed forces must take initiatives to formally tap the rich resource of OSINT through social media. While at the tactical level, a focussed and systematic monitoring is recommended; at the operational and

strategic levels, formal or informal engagement with trusted independent OSINT analysis groups will prove highly beneficial during times of conflict. Similarly, paid and confidential agreements or Memoranda of Understanding (MoU) with firms providing high quality military-grade satellite imagery will be a shot in the arm to image intelligence, an important input for targeting and carrying out PSBDA. As recent conflicts have demonstrated, claims made by either party are subjected to intense scrutiny. OSINT evidence further enhances legitimacy by enabling claims to be verified transparently. Conversely, it is imperative that one's own claims are firmly grounded in verifiable evidence, otherwise they risk losing credibility.

AI offers numerous advantages in sifting through huge volumes of social media data. It can be suitably customised to flag malicious content, segregate authentic inputs, assist in gathering actionable intelligence, and refine target information as well as prioritise targets for strikes, besides aiding own information campaign. The Indian Armed Forces must develop their own tailor-made AI solutions to cater for service specific requirements.

The social media dynamics must be dovetailed into war-games, table-top exercises, and major field exercises for narrative shaping, targeting support, and PSBDA. 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 paper unequivocally demonstrate that social media has emerged as a core variable of contemporary battlespace, which operates simultaneously in the cognitive as well as kinetic domains of warfare. It has become integral to the conduct and outcomes of modern conflict, shaping perception, enabling operational effects, and influencing strategic decision-making. Actors who will leverage social media effectively for narrative formation, legitimacy contests, intelligence generation, targeting, and PSBDA, will gain substantial advantages over their adversaries. Social media will directly influence legitimacy claims, institutional credibility, diplomatic manoeuvrability, operational advantage, and escalation control.

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. For the Indian Armed Forces, the lessons emerging from examination of three aforementioned conflicts of the recent times should serve as an alarm bell for reorienting the existing structures and initiating requisite reforms in order to be ready for effective usage of social media in future conflicts.

The measures recommended in this occasional paper as policy revisions will be immensely valuable in leveraging social media during conflict. These include formally integrating social media, formulating clear standard protocols, and signing of MOUs with commercial imagery providers and credible OSINT networks. There should also be provisions for structured liaison with civilian analytical communities and creation of dedicated social media cells at brigade, division, and equivalent headquarters across the services.

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 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, 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.

Endnotes

---

[1] Matthew Ford, "How Smartphones are Changing the Reality of War", *Swedish Defence University*, 26 Aug 2025, accessed 30 Jan 2026, https://www.fhs.se/en/swedish-defence-university/stories/2025-08-26-how-smartphones-are-changing-the-reality-of-war.html

[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.

[3] StratCom COE, "Social Media as a Tool of Hybrid Warfare", *NATO Strategic Communications Centre of Excellence*, pp 23-27, 2016, accessed 24 Jan 2026, https://stratcomcoe.org/publications/social-media-as-a-tool-of-hybrid-warfare/177

[4] News on AIR, "NIA Files Chargesheet In Pahalgam Terror Attack Case", *Akashvani News*, 16 Dec 2025, accessed 20 Jan 2026, https://newsonair.gov.in/nia-files-chargesheet-in-pahalgam-terror-attack-case/

[5] Agencies, "Dummy Aircraft to BrahMos and Rafale Jets, How India Tactically Planned Counter-Offensive Against Pakistan", *Indian Defence News*, 16 May 2025, accessed 25 Jan 2026, https://www.indiandefensenews.in/2025/05/dummy-aircraft-to-brahmos-and-rafale.html

[6] Post by Donald Trump, *Truth Social*, 10 May 2025, accessed 20 Jan 2026, https://truthsocial.com/@realDonaldTrump/114483405683675564

[7] Post by Dr S Jaishankar, "X", 10 May 2025, accessed 20 Jan 2026, https://x.com/DrSJaishankar/status/1921183635274608685

[8] PTI, "54 per cent people in India turn to social media for factual info: Oxford University Press study," *The Tribune (India)*, 28 Jun 2022, accessed 22 Jan 2026, https://www.tribuneindia.com/news/nation/54-per-cent-people-in-india-turn-to-social-media-for-factual-info-oxford-university-press-study-407736/

[9] Christopher Clary, "Four Days in May: The India-Pakistan Crisis of 2025", *Stimson Center*, 28 May 2025, accessed 30 Jan 2026, https://www.stimson.org/2025/four-days-in-may-the-india-pakistan-crisis-of-2025/

[10] Debanish Achom, "X to Block Over 8,000 Accounts in India After Government Order", *NDTV*, 08 May 2025, accessed 30 Jan 2026, https://www.ndtv.com/india-news/x-to-block-over-8-000-accounts-in-india-after-government-order-8366168

[11] TOI News Desk, "'Provocative, communal content': Centre bans Pakistan YouTube channels, flags 'misinformation'", *The Times of India*, 28 Apr 2025, accessed 01 Feb 2026, https://timesofindia.indiatimes.com/india/provocative-communal-content-centre-bans-pakistan-youtube-channels-flags-misinformation/articleshow/120685473.cms

[12] ET Online, "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*, 08 May 2025, accessed 30 Jan 2026,

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

[13] Raksha Kumar, "Truth is the casualty": How Indian fact-checkers debunked false claims during the India-Pakistan crisis", *Reuters Institute for the Study of Journalism*, 29 May 2025, accessed 29 Jan 2026, https://reutersinstitute.politics.ox.ac.uk/news/truth-casualty-how-indian-fact-checkers-debunked-false-claims-during-india-pakistan-crisis

[14] "Social media are the most popular source of information among Ukrainians, but TV is the more trusted one: Survey", *Institute of Mass Information*, 02 Jun 2022, accessed 30 Jan 2026, https://imi.org.ua/en/news/social-media-are-the-most-popular-source-of-information-among-ukrainians-but-tv-is-the-more-trusted-i45921

[15] "What Social Media Do Ukrainians Use?", *OPORA Survey,* 2025, accessed 20 Jan 2026, https://www.oporaua.org/en/polit_ad/24068-mediaspozhivannia-ukrayintsiv-v-umovakh-povnomasshtabnoyi-viini-opituvannia-opori-24068

[16] Valeriya Ionan, "Delivering Digital Transformation in Ukraine", *Governance Matters Magazine,* May 2023, accessed 16 Jan 2026, https://chandlergovernance.com/governancematters/delivering-digital-transformation-in-ukraine

[17] Darina Dvornichenko, "How the War Makes Ukraine Leap Forward in Digitalization", *German Marshall Fund of the United States*, 19 May 2022, accessed 30 Jan 2026, https://idnext.eu/a-citizen-like-chatbot-allows-ukrainians-to-report-to-the-government-when-they-spot-russian-troops-heres-how-it-works

[18] UNN, "People's Intelligence: 674,000 Ukrainians Have Already Used the eEnemy Chatbot", *Ukrainian National News*, 13 Jun 2025, accessed 29 Jan 2026, https://unn.ua/en/news/peoples-intelligence-674000-ukrainians-have-already-used-the-eenemy-chatbot

[19] Jerusalem Post Staff, "Ukrainian App Allows Civilians to Report Russian Missile Sights to Air Defense", *The Jerusalem Post*, 16 Oct 2022, accessed 28 Jan 2026, https://www.jpost.com/international/article-719836

[20] Don Rassler and Yannick Veilleux-Lepage, "Drone-Assisted Targeting and the Emerging Operational Tempo in the Russo-Ukrainian War", *CTC Sentinel,* Mar 2025, accessed 28 Jan 2026, https://ctc.westpoint.edu/wp-content/uploads/2025/03/CTC-SENTINEL-032025_cover-article.pdf

[21] Lt Gen Philip Campose (Retd), "What Indian military can learn from Ukraine's optimisation of drone warfare", *The Week*, 29 Oct 2025, accessed 29 Jan 2026, https://www.theweek.in/news/defence/2025/10/29/ukraine-optimisation-of-drone-warfare-and-lessons-for-the-indian-military.html

[22] WP Staff, "Russia Asks Citizens to Use New App to Report Drones and Other Attacks", *The Washington Post*, 20 Sep 2023, accessed 28 Jan 2026, https://www.washingtonpost.com/world/2023/09/20/russia-app-drone-citizens-war/

[23] Britannica Editors, "Timeline and Overview of the 2023 Israel-Hamas War", *Britannica,* 07 Jul 2026, accessed 29 Jan 2026, https://www.britannica.com/event/Israel-Hamas-War

[24] TOI Staff and Emanuel Fabian, "Hamas Spent Years Mining IDF Troops' Social Media for Intel on Bases, Tanks–Report", *The Times of Israel*, 28 Nov 2023, accessed 29 Jan 2026, https://www.timesofisrael.com/hamas-spent-years-mining-idf-troops-social-media-for-intel-on-bases-tanks-report/

[25] "Hamas Promotes a "Victory" Narrative for Gaza Strip War", *The Amit Terrorism and Intelligence Research Institute,* 17 Feb 2025, accessed 25 Jan 2026, https://www.terrorism-info.org.il/en/hamas-promotes-a-victory-narrative-for-gaza-strip-war/

[26] *TikTok*, "Our continued actions to protect the TikTok community during the Israel-Hamas war", TikTok Newsroom, 23 Nov 2023, accessed 28 Jan 2026, https://newsroom.tiktok.com/our-continued-actions-to-protect-the-tiktok-community-during-the-israel-hamas-war

[27] Dina Sadek and Layla Mashkoor, "In Israel-Hamas conflict, social media become tools of propaganda and disinformation", *DFRLab*, 12 Oct 2023, accessed 01 Feb 2026, https://dfrlab.org/2023/10/12/in-israel-hamas-conflict-social-media-become-tools-of-propaganda-and-disinformation/

[28] Yuval Abraham, "'Lavender': The AI machine directing Israel's bombing in Gaza", *+972 Magazine*, 03 Apr 2024, accessed 02 Feb 2026, https://www.972mag.com/lavender-ai-israeli-army-gaza/

[29] Harry Davies, Bethan McKernan, and Dan Sabbagh, "'The Gospel': How Israel uses AI to select targets for bombing in Gaza", *The Guardian,* 01 Dec 2023, accessed 03 Feb 2026, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets

[30] Ibid.

[31] "Gaza: Findings on October 17 al-Ahli Hospital Explosion", *Human Rights Watch,* 26 Nov 2023, accessed 03 Feb 2026, https://www.hrw.org/news/2023/11/26/gaza-findings-october-17-al-ahli-hospital-explosion

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

[33] Eliot Higgins, *We Are Bellingcat: An Intelligence Agency for the People* (London: Bloomsbury Publishing, 2021).

About the Author

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 terrains, and has served tenure at Army Headquarters, foreign course, and deployment abroad in United Nations Mission. His academic interests include national security and impact of technology on warfare. Currently, he is pursuing a PhD in Defence and Strategic Studies.

Colonel Subodh Shahi, PhD (Retd) is an expert in defence and strategic studies. He is presently serving as Associate Professor and Director at Amity Institute of Defence and Strategic Studies.

About the United Service Institution of India (USI)

The USI was founded in 1870 by a soldier scholar, Colonel (later Major General) Sir Charles MacGregor 'For the furtherance of interest and knowledge in the Art, Science and Literature of National Security in general and Defence Services, in particular'. It commenced publishing its Journal in 1871. The USI also publishes reports of its members and research scholars as books, monographs, and occasional papers (pertaining to security matters). The present Director General is Vice Admiral Sanjay J Singh, SYSM, PVSM, AVSM, NM, PhD (Retd).

(Estd. 1870)

United Service Institution of India (USI)

Rao Tula Ram Marg, Opposite Signals Enclave,
New Delhi-110057

Tele: 2086 2316/ Fax: 2086 2315,
E-mail: dircpl@usiofindia.org

₹ 250