Issue Brief

April 2026
No: 499

From Proxies to Platforms: How AI Is Reshaping the Character of Conflict

Lt Gen A B Shivane
PVSM, AVSM, VSM (Retd)

From Proxies to Platforms: How AI Is Reshaping the Character of Conflict

Abstract

This paper explores how artificial intelligence is transforming the nature of conflict in South Asia, shifting it from proxy-based violence to hybrid warfare driven by technology. It contends that the growing use of artificial intelligence is gradually but profoundly changing the character of conflict within India's security landscape. What was once primarily shaped by geography and traditional asymmetry is now influenced by data, speed, and the spread of technology. Recent trends show that accessible tools like unmanned systems, encrypted platforms, and synthetic media are broadening options for both state and non-state actors. This impacts not only operational domains but also attribution, escalation management, and public perception. India's progress has been significant in certain areas, but it remains inconsistent across institutions. The main challenge is to ensure that doctrinal, technological, and societal measures evolve in harmony with these emerging threats.

Keywords: Artificial Intelligence, Hybrid Warfare, Cognitive Security, Drone Warfare, Counter-Terrorism

Artificial Intelligence and the Face of Hybrid Conflicts

Artificial Intelligence (AI) is no longer an emerging technology associated with warfare; instead, it has become a disruptive reality impacting the character of conflicts (UNSC, 2022). Globally, it has become an adjunct to a more ancient and well-known weapon of destabilisation viz. terrorism and tools of dark states in creating turmoil (UN Office of Counter-Terrorism). In India, convergence is taking place across multiple fronts and domains. On one hand, Pakistan is aiding and abetting proxy groups as an instrument of state policy on the western front, with a spillover to the heartland. On the other hand, China is shifting the technological asymmetry by disrupting the pace of technological innovation and obscuring the transfer of dual-use systems on the northern front. The internal domain manifests as AI disruptions across kinetic and non-kinetic fronts and poses the foremost threat to the cognitive domain. The concept of artificial intelligence and irregular warfare is changing the grammar of regional security. India today is not threatened speculatively, but structurally (UN Office of Counter-Terrorism).

India's Structural Exposure Across Multiple Fronts

India's recent operational experience underlines this structural shift. Operation Sindoor, wherein Pakistan's cross-border terror infrastructure was targeted with calibrated precision in a multi-domain warfare, the brutal clash in Galwan that unveiled the truth of the disputed borders, and the recent terror attack in the hinterland, demonstrated how digital warfare and AI integrated with state and nonstate actors could pose a serious threat to India's national security.

India's adversaries test the nation across physical, informational and technological domains. The battlefield is no longer linear; it is embedded within disruptive technological systems. What took days to manifest now takes seconds, by means of encrypted messages, drone surveillance, satellite updates and amplification of synthetic media. These actions are not exclusive; they indicate an adaptive enemy that has learnt India's thresholds and diluted India's response cycles.

Table 1: Recent Operational Signals and AI-Linked Security Implications

Event	Nature of Challenge	Technological Dimension	Strategic Lesson
Operation Sindoor	Cross-border terror infrastructure	High-altitude military stand-off	Hybrid local-cross-border coordination
Galwan Confrontation	High-altitude military stand-off	Surveillance systems, information management, cyber signalling and deep fakes	Border incidents now operate under persistent technological observation
Recent Major Terror Attacks in India	Hybrid local cross-border coordination	Encrypted communication, online radicalisation, and potential drone logistics	Internal security and external sponsorship increasingly overlap

Source: Author's own

Technological Diffusion and the Adaptability of Terror Networks

Terrorist groups in and around South Asia have been known to use asymmetric ingenuity in the past. They have rapidly learnt to embrace technological diffusion and have been using improvised explosive devices (IEDs), satellite phones and encrypted messages. Moreover, with open-source machine learning libraries, facial recognition modules, and synthetic media generators, commercial AI-enabled technologies are no longer the preserve of high-end militaries (SIPRI, 2024). They are available, cheap and not easy to track. These tools are thus more precise and time efficient, and reduce the distance between the means and the end in the hands of non-state actors.

The Unmanned Domain and the Changing Geometry of Conflict

The most noticeable is manifested in the world of the unmanned. Drones have already changed the pattern of infiltration along the Line of Control and the International Border. What started as infrequent narcotics deliveries has developed into an orderly reconnaissance and deliveries of payloads. Artificial intelligence increases this evolution. Terrain-mapping algorithms enable autonomous movement through complex valleys. Pattern recognition systems enable drones to detect troop concentrations, vehicle convoys/supply dumps with greater accuracy. Swarm logic allows coordination of various low-cost platforms without a direct human operator (SIPRI, 2025). It is now possible to challenge physical geometry with AI asymmetry, which previously needed physical mobilisation to interfere, with a small investment in technology.

Cost, Deniability and Psychological Leverage

The cost disparity is evident. An open-source AI-enabled autonomous first-person-view drone can cost a fraction of a traditional weapons system. But it can destroy radar facilities, interfere with ammunition or hit targets with precision. The cognitive impact of attended deniability is disproportionate. The defender experiences attribution problems and escalation threats. This lop-sidedness fits in the long history of plausible deniability by Pakistan, whereby state sponsorship is hidden behind non-state actors.

The Cognitive Battlefield: Deepfakes, Malware and Trust Deficit

Cyberspace augments the threat. Malware has now evolved through artificial intelligence, which adjusts phishing campaigns to individual officers, units or institutions. Artificial voices and video may pass as commanders in a crisis, creating confusion during crucial moments. Deepfake propaganda can stir up trouble, create atrocities or enhance sectarian divisions. Radical networks leverage generative models to produce high-volume, emotionally appealing content that bypasses the usual moderation filters. This is not only recruitment but orchestrated cognitive disruption (GCTF).

China, Dual-Use Technology and Grey-Zone Pressure

The role China plays in this changing matrix warrants serious evaluation. The PLA modernisation focuses on intelligentised warfare, incorporating data, autonomy, and precision. Although China does not officially support the spread of terrorism, its growing technology system provides avenues of spread. Repurposing dual-use platforms that were exported under commercial labels may be possible, provided the labels are reused. Access to mid-tier unmanned systems and surveillance technologies is further deepened in Pakistan through joint research programs and economic corridor initiatives. Even small advancements in sensors, communications, or data processing can lead to significant improvements in the operational capacity of proxy actors (UNSC, 2023).

In the case of Beijing, South Asia provides an experiment of strategic pressure. China makes the security environment of Pakistan difficult without a direct clash by strengthening the technological base of Pakistan. The trend reflects the broader geopolitical rivalry, in which grey-zone policies replace overt aggression. India should not then take artificial intelligence-powered terrorism as a single case of a domestic security threat, but as a geopolitical power struggle in the region.

India's Response: Progress But Needs More Coherence

India has begun responding, but responses have not been uniform. The armed forces have outlined roadmaps for integrating artificial intelligence that focus on predictive analytics, autonomous systems, and multi-domain awareness. Native loitering munitions, the automated radars, and satellite-based surveillance are used to improve tracking and response. The units are trained through simulation-based preparation to operate drone swarms and hybrid attacks. Intelligence agencies increasingly use data fusion and analysis algorithms to monitor suspicious transactions and communications.

Nonetheless, there are gaps in dogma and institutional voids. The work on inter-service interoperability is still in progress. The procurement cycle is slow in keeping pace with technological change. Reliance on foreign parts carries the risk of supply interruptions or latent risks. The legacy of bureaucratic lethargy and the 'procedures over outcomes' syndrome retards the translation of innovation into operational deployment. On the other hand, non-state actors operate autonomously, with access and without procedural chains.

The greater issue is the preparedness of regulations and society. Man-made media can spark communal tensions in a few hours. Artificial intelligence-driven financial fraud may victimise military families or veterans. Schools and governments do not have the means to see through manipulated content. The legal system struggles to categorise and prosecute other emerging forms of digital sabotage. India is at risk of combating a twenty-first-century menace with twentieth-century tools, without achieving rapid adaptation.

Towards a Comprehensive National Response

The response must be comprehensive. To begin with, "India has to integrate artificial intelligence literacy into its security architecture and professional military education (PME)". Algorithmic decision making, data ethics, and counter-autonomy tactics must be incorporated into officer training academies and police institutions. Counter-unmanned systems specialised units should be increased, which, in turn, should be equipped with electronic warfare and directed energy research capabilities. Sharing real-time data between military and civilian agencies should be the norm, not the exception.

Second, "technological self-reliance is a strategic imperative". Investment in local semiconductor fabrication, edge computing and secure communication protocols mitigates local exposure to external leverage. Indigenous datasets reflecting the linguistic and geographic diversity of India can be collected more quickly through public-private partnerships with research institutions. Defence start-up accelerators are innovation ecosystems designed to align with operational feedback loops that require rapid iteration.

Third, "intelligence reform should be futuristic and not reactive". An artificial intelligence-specific national cell could combine signals intelligence, cyber forensics, financial tracking and open source analysis. Constant surveillance of procurement networks, such as dark web markets, would open up supply chains working with militant organisations. Human intelligence is critical, especially in border communities, where people are susceptible to recruitment or even coercion.

Fourth, "innovation should be met by regulatory clarity". Deterring technology can be achieved through clear labelling standards for synthetic media, compulsory reporting of flags on imported drones, and strong disincentives against technology diversion. Services with operations in India should have quick take down mechanisms for confirmed deepfakes and terror propaganda. The judicial ability to comprehend and utilise digital evidence should increase.

Fifth, "deterrence should be supported by diplomacy". Participation in forums like the Quad and other similar coalitions can set standards for responsible artificial intelligence exports. Even in the presence of limited transparency and confidence-building mechanisms with the neighbours, accidental escalation resulting from misattributed drone incidents can be mitigated. Meanwhile, India should send its message loud and clear by stating that proxy warfare, under the disguise of artificial intelligence, will not protect the act of sponsorship.

Lastly, "resilience in society is a strategic asset, and a National Citizens Security Culture is an imperative". Hype/Panic can be flattened by running public awareness campaigns about the concept of deepfakes and digital manipulation. The integration of digital literacy into the learning curriculum empowers long-term immunity. The communities integrated into surveillance and reporting networks can turn 'vulnerability into partnership'.

Conclusion: Adapting Faster Than the Adversary

Artificial intelligence does not create new fault lines in South Asia; it sharpens those that already exist. What has changed is the pace, scale and opacity of conflict. Decisions that once unfolded over days can now escalate within minutes, while actions that demanded sustained effort to uncover can be concealed or distorted with relative ease.

India's strengths are evident: a deep pool of technological talent, a vibrant start-up ecosystem, and rich experience in counter-terrorism. Yet these advantages will matter only if they are brought together with purpose. The contest will not turn on a single platform or breakthrough. It will hinge on the ability to align policy, technology, training and doctrine into a coherent and responsive whole.

The use of artificial intelligence by terror outfits makes management of escalation more difficult and puts societal cohesion to the test. Hence, India needs to be proactive and pre-emptive, not reactive and defensive. India can turn 'vulnerability into strength' by mastering the technologies its adversaries use and developing them to align with democratic accountability. South Asians will not fear intelligent machines, but those who build them with a sense of purpose and national determination will prevail in the future of security.

Works Cited

Countering the Use of New and Emerging Technologies for Terrorist Purposes (2022). United Nations Security Council Counter-Terrorism Committee. https://www.un.org/securitycouncil/ctc/content/countering-use-new-and-emerging-technologies-terrorist-purposes.

Counter-Unmanned Aerial Systems and New, Emerging, and Disruptive Technologies Initiative. Global Counterterrorism Forum (GCTF). https://www.thegctf.org/Who-we-are/Structure/Initiatives/GCTF-Counter-Unmanned-Aerial-Systems-and-New-Emerging-and-Disruptive-Technologies-Initiative.

Cybersecurity and New Technologies. United Nations Office of Counter-Terrorism. https://www.un-.org/counterterrorism/en/cct/programme-projects/cybersecurity.

Military Expenditure Data and Analysis (2025). SIPRI. https://www.sipri.org/media/newsletter/2025-april.

Security Council Report on Terrorism and Emerging Technologies (2023). United Nations Security Council Counter-Terrorism Committee. S/2023/1035. https://docs.un.org/en/s/2023/1035.

Trends in International Arms Transfers, 2023 (2024). SIPRI. https://www.sipri.org/media/newsletter/2024-march.

United Nations Office of Counter-Terrorism. UN Counter-Terrorism Portal. https://www.un.org/counterterrorism/en.

About the Author

Lieutenant General A B Shivane, PVSM, AVSM, VSM (Retd), is a former DG Mechanised Forces and Strike Corps Commander with over 39 years of distinguished service. A scholar-warrior, a former consultant to the Ministry of Defence, he has authored 350-plus articles and four books. He is presently the Strategic Advisor to several organisations and think tanks.