The Algorithmic Age of Warfare: Lessons from Contemporary Conflicts and a Techno-Legal Framework for Autonomous Defensive Response in India

Commander Ravi Shankar NRK (Retd)[@]

Abstract

The fusion of Artificial Intelligence (AI) with drones, missiles, cyber capabilities and Intelligence, Surveillance and Reconnaissance is compressing modern warfare to machine speed. The Middle East has exposed the perils of algorithmic targeting outpacing human review; the Russia–Ukraine war has shown that combat AI must function at the tactical edge, unaided by cloud connectivity; and India's Operation Sindoor, read against China's 'Intelligentised Warfare' doctrine, shows Indo-Pacific decision cycles compressing to single-digit seconds. Together, these expose a 'Speed Versus Control' paradox that conventional 'Human-in-the-loop' doctrine cannot resolve once the engagement window narrows below the time a human needs to process a binary choice. This article does not propose a general AI-regulation framework; its scope is narrower — how India should govern AI's use in weapons and defensive-response systems built to counter machine-speed

[@]**Commander Ravi Shankar NRK (Retd)** is an independent researcher and the author of The Digital Armada (2026). A veteran of the Indian Navy with over 35 years of service across submarines, frontline warships, and major defence establishments, he has held senior leadership and program-management appointments overseeing the induction of combat systems, fleet logistics and mission-critical networks. His current research focuses on autonomous systems, algorithmic sovereignty, and artificial intelligence governance in the maritime domain.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

threats. It proposes a four-pillar techno-legal framework — Pre-Authorised Autonomous Defensive Response (PAADR), edge-first resilience with federated learning, a Joint Maritime Domain Awareness Data Architecture, and ring-fenced agile procurement — to reconcile algorithmic velocity with democratic accountability and India's obligations under international humanitarian law.

Introduction

The character of warfare has shifted structurally over the past decade. The battlefield no longer sits within the physical domains of land, sea, and air alone; it runs through the electromagnetic spectrum, data networks, space, and the cognitive domain. Military superiority increasingly depends on data dominance, network integration, and the speed of decision-making, with Artificial Intelligence (AI) serving as the cognitive spine linking Intelligence, Surveillance And Reconnaissance (ISR), cyber operations, space assets, and precision strike.

States embedding AI into their national security architectures are not merely enhancing existing capabilities; they are redefining what strategic advantage means, and that redefinition brings a governance problem that cannot be deferred: reconciling the lethal speed of these technologies with the legal requirement of meaningful human control.[1] This article confines itself to that narrower problem rather than to the broader debate over regulating AI development in India, which is already under way through the India AI Mission and related fora.[2] Its subject is AI's employment specifically within weapons and defensive-response systems. The Defence Research and Development Organisation's (DRDO) 2024 Evaluating Trustworthy AI (ETAI) Framework and India's own submission to the United Nations' (UN) Secretary-General already establish safety, transparency, fairness, and human oversight as governing principles in the military domain.

In the military domain, safety, transparency, fairness, and human oversight are already established as governing principles.[3], [4] The question is operational, not declaratory: how those principles

survive an engagement window that has collapsed to single-digit seconds.

The analysis that follows draws on a structured comparison of three theatres—the Middle East, Russia–Ukraine, and the Indo-Pacific, including Operation Sindoor—chosen because each isolates a distinct variable bearing on weapons-employment governance: human oversight under high-tempo targeting, resilience under sustained electronic warfare, and the compressed decision cycles of a two-front, nuclear-armed threat environment, respectively. Evidence is drawn from open-source operational reporting cross-checked across independent accounts, India's primary governance documents, and comparative defence-budget data. Where a single-source claim could not be independently corroborated, it has been qualified in the text rather than treated as settled.

Review of Literature

Existing scholarship falls into three strands that, read separately, leave the question of weapons employment unanswered. The first, on 'Meaningful Human Control' (MHC), is analytically rich but operationally thin: Williams's critique of the MHC debate argues that the 'Meaningful Human' at its centre reflects a narrow, Western conception of agency that says little about what happens once the physics of an engagement make real-time deliberation impossible.[5] Indian commentary has tended toward the cautious end of this debate—writing from the Centre for Land Warfare Studies argues that algorithms cannot substitute for human judgement of context and consequence, and that the 'Decide' function of the Observe–Orient–Decide–Act loop should stay with humans[6]—without engaging the empirical reality that a strict human-in-the-loop requirement is already being overtaken by combat tempo. The second strand is institutional: Saini's assessment for the Council for Strategic and Defence Research documents India's fragmented AI funding and the absence of a unified inter-service data architecture in granular detail, but is oriented toward capability-building rather than the governance of weapons employment.[7] The third is doctrinal — the ETAI Framework and India's UN Secretary-General submission state principles of safety, oversight and International Humanitarian Law

(IHL) compliance without an engineering specification for how those principles hold once the decision window collapses.[8] Read together, the gap is precise: ethics and law theorise control without confronting engagement physics; institutional analysis documents capability gaps without addressing employment governance; and doctrine states principles without architecture. This article sits at the intersection of the three, using the operational record below to derive design constraints for a bounded architecture rather than a general governance principle.

Trends and Dynamics in Contemporary Conflicts

The Middle East: ISR, Missiles and the Erosion of Human Oversight. In Gaza and Lebanon, Israeli forces are reported to have used AI decision-support systems such as 'Lavender' and 'The Gospel' to generate targeting recommendations at a pace producing a reported 45-fold increase in operational tempo.[9] That speed produced 'Automation Bias': operators reportedly spent only about 20 seconds verifying AI-generated targets before authorising strikes, reducing human review to a rubber stamp while the ethical guardrails distinguishing combatants from civilians progressively gave way.[10] Israel's Operation Rising Lion and the United States' (US) strike codenamed Midnight Hammer confirmed that AI-integrated air power can project long-range strikes across considerable distances,[11] while Houthi drone and missile attacks in the Red Sea have forced coalition navies into sustained air defence with engagement windows measured in tens of seconds—a preview of what platform-centric the Indian Ocean area defence will struggle to match.[12]

The Russia–Ukraine Theatre: Drone Swarms and Edge-AI Resilience. Ukraine has shown that centralised cloud dependence is a critical vulnerability under sustained electronic warfare. During Operation Spider Web, drones whose remote links were severed completed strikes autonomously using onboard visual-recognition algorithms; platforms such as the Saker Scout now navigate without global positioning system or cloud connectivity.[13] Persistent wiper-malware and disinformation campaigns aimed at logistics and command networks, run from the war's opening hours, reinforce the

same lesson: any system India fields must degrade gracefully, not catastrophically, the moment connectivity is denied.[14]

The Indo-Pacific and South Asia: Operation Sindoor and Intelligentised Warfare. Operation Sindoor in May 2025 offers India's own evidence. Over a 4-day window, 23 AI applications were reportedly unified for a common battlefield picture, and the Electronic Intelligence Collation and Analysis System, trained on 26 years of archival data, achieved roughly 94 per cent accuracy in identifying hostile radar and missile units.[15] Separately, the Army's Akashteer air-defence network—built by Bharat Electronics with DRDO and Indian Space Research Organisation, fusing tactical radars, low-level radars and the Akash weapon system into one operating picture — was credited with directing interceptions along the western front. It is worth being precise here: contemporaneous reporting described this as 'Automated operations for faster response' and 'Decentralised engagement authority' at forward nodes, rather than a fully autonomous killweb; the more expansive 'AI-driven' description appears mainly in later trade commentary.[16] The verifiable claim is narrower but still significant—Akashteer compressed detection-to-engagement time by pushing authority to automated forward nodes, the design principle this article's first pillar seeks to generalise.

AI-Enabled Military Threats. China's 'Intelligentised Warfare' doctrine, backed by a military–civil fusion strategy that transfers commercial AI advances into battlefield deployment with little friction, has produced platforms such as the JARI-USV-A 'Orca' unmanned surface vessel, a stealth platform reportedly capable of ranges beyond 4,000 nautical miles and vertical missile launches.[17] Pakistan is separately pursuing AI-enabled drone-swarm programmes and an expanding inventory of cruise missiles such as the Harbah, raising the prospect of a future crisis combining both threat streams.[18] Along the Line of Actual Control, both India and China have fielded long-endurance drones and AI-assisted change detection, compressing the warning time on which conventional crisis signalling and restraint have traditionally relied.[19]

Lessons Learnt: The Speed Versus Control Paradox

Taken together, these theatres expose a tension that India's own ETAI doctrine, resting on a strict human-in-the-loop mandate, does not resolve.[20] Against a hypersonic missile or a saturation drone swarm, the engagement window from detection to impact can compress to 25 to 40 seconds, while human decision-making under stress requires 8 to 12 seconds simply to process a binary choice.[21] At that timescale, an operator cannot fuse sensor data, classify a threat and authorise a response; forcing the attempt converts a commander into a liability shield rather than an agent of genuine moral control—a distinction with legal as well as ethical weight, since a decision made without room for deliberation cannot straightforwardly satisfy the accountability human-in-the-loop doctrine is meant to guarantee. Adversaries operating under less restrictive doctrines—the US' 'AI-First' posture and China's intelligentised warfare—are engineering autonomous engagement precisely to exploit that latency.[22] A related consequence is doctrinal: deterrence in South Asia has rested on the threat of punishment, which presumes an adversary has time to receive a signal and revise intent; algorithmic warfare compresses every stage of that sequence, favouring deterrence-by-denial and demonstrably resilient defensive autonomy over speculative retaliation.

Strategic Implications for India: A Techno-Legal Framework for Autonomous Defensive Response

Resolving this paradox requires an engineered architecture, not a restated commitment to oversight that the record above shows has already been overtaken. The ETAI Framework and India's UN Security General submission supply the governing principles; what follows operationalises them.[23]

Pillar One: Resolving the Speed Paradox Through Pre-Authorised Autonomous Defensive Response (PAADR). The armed forces should institute a PAADR framework, legally and technically pre-authorising bounded, autonomous terminal-defence actions—activating close-in weapon systems, releasing decoys—before an engagement occurs rather than during it. Activation would

require simultaneous hardware-encoded conditions: an active hostile radar or terminal-guidance signature, independent sensor corroboration, and a computed impact probability above a pre-authorised, operationally and legally validated threshold—85 per cent is used here only as an illustrative figure, not a proposed Indian standard; the actual value is a calibration question for the weapons-review process described below, not one this article can settle in the abstract. PAADR would be confined to terminal self-defence, excluding offensive tasking, with the commanding officer retaining standing authority to deactivate it. Crucially, human decision-making is relocated rather than removed: it is exercised prospectively, in designing trigger conditions and in a mandatory Article 36-style weapons review, rather than in real time, where it cannot meaningfully be exercised at all.[24] The argument is not that prospective authorisation by itself constitutes meaningful human control; rather, it is that control must be distributed across system design, weapons review, operational constraints, standing command authority and the ability to intervene or deactivate, of which prospective authorisation is one component among several. Understood that way, the architecture is designed to operationalise the cardinal IHL principles in a manner that real-time human review under hypervelocity conditions cannot easily match: distinction is supported through the narrowness of the trigger set itself, since only objects exhibiting a verified attack signature can activate the system; proportionality is supported by confining permissible action to defensive, terminal-phase responses with pre-set collateral limits; and precaution is supported through the mandatory review—though actual compliance in any given engagement remains a facts-and-circumstances question the architecture cannot guarantee in advance. The benefit is concrete, not rhetorical—it converts a commander's choice between a legally fraught snap decision and a fatal delay into an auditable, improvable, peacetime one, and it is that relocation of judgement, not the removal of it, that makes PAADR defensible.

Pillar Two: Edge-First Resilience and Federated Learning. AI systems must be deployed through hardware-isolated, air-gapped modules that can function at the tactical edge without internet or

satellite connectivity, treating jamming and denial as baseline design conditions. This must also address a specifically Indian problem: a model trained on Rajasthan's desert terrain can fail outright in Ladakh's high-altitude conditions, where lighting, thermal signature and atmosphere differ fundamentally.[25] ETAI-mandated uncertainty estimation, which hands control back to a human when confidence drops, must be built in from the outset so unfamiliar conditions default to caution rather than false confidence—and air-gapped deployment simultaneously narrows the attack surface for adversarial data poisoning. For cross-domain ISR, federated learning allows models to train locally on platforms such as P-8I aircraft or Kalvari-class submarines, sharing only encrypted model updates rather than sensitive raw data such as submarine acoustic signatures—preserving both data sovereignty and bandwidth discipline.[26]

Pillar Three: Breaking Institutional Silos for ISR Integration. India's three services operate largely distinct legacy systems reflecting decades of separate modernisation, a fragmentation that is doctrinal before it is technical: without a shared operational picture, PAADR-style prospective authorisation cannot scale beyond single-platform defence to a genuinely joint defensive network. The framework calls for a Joint Maritime Domain Awareness Data Architecture—a unified defence data cloud paralleling the 'Directorate of AI' and data-cloud already recommended independently within the Integrated Defence Staff — standardising formats across the Defence Intelligence Agency, service intelligence wings and civilian space agencies, and fusing satellite, coastal radar and drone inputs through platforms such as TRIDENT-SAMUDRA to automate detection of 'Dark Vessels' and grey-zone maritime militia, the category of threat hardest to counter precisely because it sits below the threshold that triggers a conventional platform-centric response.[27, 28]

Pillar Four: Agile Procurement and Ring-Fenced Budgeting. India has no single dedicated military-AI budget line; funding is drawn from annual service-specific earmarks of roughly INR 100 cr from each of the Army, Navy and Air Force plus a further INR 100 cr from the Defence AI Project Agency—about INR 400 cr (USD 46 mn) a year in total, under three per cent of estimated Chinese military AI

spending and dwarfed by the US Department of War's FY2026 request of USD 13.4 bn in standalone autonomy funding.[29] India's civilian India AI Mission budget was itself halved, from INR 2,000 cr to INR 1,000 cr, in the same cycle.[30] Three-to-five-year hardware acquisition cycles are structurally incompatible with software-defined AI, which needs continuous retraining against evolving threats and adversarial poisoning. India should ring-fence one per cent of the capital defence budget for AI software, R&D and edge computing infrastructure—roughly a fivefold increase over current dedicated spending—and decouple procurement from hardware timelines through agile framework contracts and deeper engagement with the domestic start-up ecosystem through initiatives such as iDEX, which has already shown, through contracts such as the roughly INR 100 cr award to the counter-drone start-up Indrajaal, that faster-cycle procurement is administratively possible within existing law. Money alone will not close the gap: the two-to-three-year officer rotation policy that serves broad command experience is directly at odds with the multi-year specialisation AI stewardship requires, moving personnel out just as they accumulate the depth needed to supervise these systems critically rather than defer to them. A specialised AI cadre, complemented by lateral recruitment of civilian data scientists on competitive terms, would address that retention problem directly.[31]

Conclusion

AI's fusion with drones, missiles, cyber capabilities and ISR is an operating reality, not a future one. The Middle East, Ukraine and South Asia show algorithmic speed as a genuine force multiplier and equally show the risks of deploying it without engineered governance—automation bias, unaccountable escalation, and acute vulnerability to electronic and cyber warfare. This article has deliberately not proposed a general AI regulation framework; it has argued that the narrower problem of weapons employment governance requires its own architecture, built on the recognition that meaningful human control, once an engagement window shrinks to single-digit seconds, must be exercised prospectively rather than in real time. Pre-Authorised Autonomous Defensive Response, edge-first hardware built for India's own terrain diversity, a unified ISR data

architecture, and procurement and talent reform matched to software-defined tempo together constitute a defensible answer to the speed-versus-control paradox—one designed to keep India's defensive posture within its IHL obligations through explicit constraints, review and accountability.

Translating this into practice will require the Ministry of Defence, DRDO, the three services, the domestic start-up ecosystem and the diplomatic community—which will need to explain India's approach in forums such as the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems—to move in step, which they do not customarily do. Three concrete steps would begin that process: piloting PAADR's trigger logic and legal-review procedure in the next major tri-service exercise cycle; publishing an Indian doctrinal statement on prospective human control, consistent with but distinct from the ETAI Framework, that other states could examine and, if they choose, adopt; and instituting an annual, parliamentary-facing review of the ring-fenced AI allocation proposed above, so the commitment is tracked rather than merely announced. The conflicts of this decade leave little room for gradualism; they will reward states that decide, deliberately and in peacetime, what algorithmic power they are prepared to wield and under what constraints, rather than states that let the battlespace decide for them.

Endnotes

1 Defence Research and Development Organisation, *Evaluating Trustworthy AI (ETAI) Framework: Version 1.0* (New Delhi: Scientific Analysis Group, Oct 2024).

2 Anita Bhatt, “Artificial Intelligence and India’s Emerging Role in Global Digital Governance”, *International Journal for Multidisciplinary Research* 8, no. 2 (2026), accessed 18 Mar 2026, https://www.ijfmr.com/research-paper.php?id=70753

3 DRDO, *ETAI Framework*, op. cit.

4 Permanent Mission of India to the United Nations, “AI in the Military Domain and Its Implications for International Peace and Security”, national submission pursuant to United Nations General Assembly Resolution 79/239, updated version (2025), Accessed 18 Mar 2026, https://docs-library.unoda.org/General_Assembly_First_Committee_-Eightieth_session_%282025%29/79-239-India-rev-EN.pdf

5 John Williams, “Locating LAWS: Lethal Autonomous Weapons, Epistemic Space, and ‘Meaningful Human’ Control”, *Journal of Global Security Studies* 6, no. 4 (Dec 2021): ogab015, accessed 19 Mar 2026, https://doi.org/10.1093/jogss/ogab015

6 Meya Kelkar, “Artificial Intelligence in Military Decision Making—A Case for the Human to Stay in the OODA Loop”, Centre for Land Warfare Studies, 06 Jan 2024, accessed 19 Mar 2026, https://claws.co.in/artificial-intelligence-in-military-decision-making-a-case-for-the-human-to-stay-in-the-ooda-loop/

7 Gaurav Saini, *India’s Approach to Military AI: Strategy, Governance, and Challenges* (New Delhi: Council for Strategic and Defense Research, Feb 2026), accessed 20 Mar 2026, https://csdronline.com/indias-approach-to-military-ai-strategy-governance-and-challenges/

8 DRDO, *ETAI Framework*, op. cit.; Permanent Mission of India, UNSG submission, op. cit.

9 Ehab Khalifa, “Blind Technology: Israel’s AI Deployment in Gaza and Lebanon Wars”, Future for Advanced Research and Studies, 07 Oct 2024, accessed 20 Mar 2026, https://futureuae.com/en-US/Mainpage/Item/9735/blind-technology-israels-ai-deployment-in-gaza-and-lebanon-wars

10 Khalifa, op. cit.

11 Michael N. Schmitt, "Israel's Operation Rising Lion and the Right of Self-Defense", *Lieber Institute West Point*, 16 Jun 2025, accessed 21 Mar 2026, https://lieber.westpoint.edu/israels-operation-rising-lion-right-of-self-defense/

12 Wolf-Christian Paes, Edward Beales, Fabian Hinz, and Albert Vidal, *Navigating Troubled Waters: The Houthis’ Campaign in the Red Sea and the Gulf of Aden* (London: International Institute for Strategic Studies, Dec 2024), accessed 21 Mar 2026, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/12/navigating-troubled-waters.pdf

13 Katja Bego, “Ukraine’s Operation Spider’s Web Is a Game-Changer for Modern Drone Warfare. NATO Should Pay Attention”, Chatham House, 06 Jun 2025, updated 17 Jul 2025, accessed 21 Mar 2026, https://www.chathamhouse.org/2025/06/ukraines-operation-spiders-web-game-changer-modern-drone-warfare-nato-should-pay-attention

14 Microsoft Threat Intelligence, *An Overview of Russia’s Cyberattack Activity in Ukraine* (Redmond, WA: Microsoft, 27 Apr 2022), accessed 21 Mar 2026, https://www.microsoft.com/en-us/security/security-insider/threat-landscape/special-report-ukraine; European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024* (Heraklion: ENISA, 2024), accessed 21 Mar 2026, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

15 D. P. Pandey, “Operation Sindoor: Air Power as Enforcer of National Will”, *Journal of the United Service Institution of India* 155, no. 642 (Oct-Dec 2025): 586–96, accessed 22 Mar 2026, https://usiofindia.org/pdf/USI_Journal_2025_Oct-De_4.pdf; Lieutenant General Rajiv Kumar Sahni, quoted in Snehesh Alex Philip, “Op Sindoor Is India’s First AI-Enabled Operation. How ‘Heavy Use’ of Modern Tech by Army Played Out”, *ThePrint*, 07 Oct 2025, accessed 22 Mar 2026, https://theprint.in/defence/op-sindoor-is-indias-first-ai-enabled-operation-how-heavy-use-of-modern-tech-by-army-played-out/2758797/

16 Operation Sindoor: Akashteer Leads AI-Driven Strikes on Terror Launch Pads”, *News on Air*, 16 May 2025, accessed 22 Mar 2026, https://www.newsonair.gov.in/operation-sindoor-akashteer-leads-ai-driven-strikes-on-terror-launch-pads/, Kalyan Ray, “Operation Sindoor: Indian Army’s Home-Grown Akashteer Air Defence Systems Block Pakistan’s Air Adventure”, *Deccan Herald*, 14 May 2025, https://www.deccanherald.com/india/operation-sindoor-indian-armys-home-grown-akashteer-air-defence-systems-block-pakistans-air-adventure-3540833; cf. Tapanjana Rudra, “Operation Sindoor: How AI-Powered Air Defence System Akashteer Shielded India,” *Inc42*, 17 May 2025, accessed 02 Mar 2026, https://inc42.com/features/operation-sindoor-how-ai-powered-air-defence-system-akashteer-shielded-india/

17 Lora Saalman, *AI in Chinese, Indian and US Nuclear Postures, Norms and Systems* (Stockholm: Stockholm International Peace Research Institute, Feb 2026), 20–21, accessed 23 Mar 2026, https://www.sipri.org/sites/default/files/2026-02/2602_ai_integration.pdf; “China’s JARI USV A Orca Unmanned Vessel with VLS Revealed at Zhuhai”, *Army Recognition*, 12 Nov 2024, https://www.armyrecognition.com/archives/archives-naval-defense/2024/chinas-jari-usv-a-orca-unmanned-vessel-with-vls-revealed-at-zhuhai

18 Quwa Team, “GIDS Harbah NG Anti-Ship Cruise Missile (ASCM)”, *Quwa*, 27 Nov 2024, accessed Aug 2026, accessed 23 Mar 2026, https://quwa.org/pakistan/munitions/gids-harbah-ng-anti-ship-missile/;

19 Saalman, op. cit., 25–28

20 20. DRDO, ETAI Framework, op. cit., 4–8.

21 Richard H. Speier, “Hypersonic Missiles: A New Proliferation Challenge”, RAND, 29 Mar 2018, accessed 23 Mar 2026, https://www.rand.org/pubs/commentary/2018/03/hypersonic-missiles-a-new-proliferation-challenge.html

22 U.S. Department of War, *Artificial Intelligence Strategy for the Department of War: Accelerating America’s Military AI Dominance* (Washington, DC: Department of War, 09 Jan 2026), accessed 23 Mar 2026, https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF

23 DRDO, ETAI Framework, op. cit.; Permanent Mission of India, UNSG submission, op. cit.

24 Protocol Additional to the Geneva Conventions of 12 Aug 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 08 Jun 1977, art. 36, accessed 24 Mar 2026, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36.

25 Saini, op. cit., 11.

26 Shankar, The Digital Armada, op. cit., chap. 12.

27 Saini, op. cit., 3, 15–16.

28 Saini, op. cit., 12–14.

29 Saini, op. cit., 14.

30 Saini, op. cit., 12–13, 15–16.