CENTRE FOR AEROSPACE POWER AND STRATEGIC STUDIES

In Focus

New Delhi

CAPSS In Focus: 29/2026

29 May 2026

Artificial Intelligence in Warfare: Evolution, Challenges, and Military Leadership

Air Vice Marshal Prashant Mohan (Retd)

Source: Created by author using Chatgpt AI

Keywords: AI in warfare, Algorithmic Battle Management, Indian Defence Modernisation, Military Leadership, AI-Governance

Introduction

John Boyd's Observe, Orient, Decide, Act (OODA) loop theory posited adaptive decision-making as the pivotal variable in war.[1] The military value of satellite-enabled information sharing during the 1991 Gulf War inspired Arthur Cebrowski's Network Centric Warfare (NCW) thesis.[2] The United States (US) integrated Artificial Intelligence (AI) and unmanned systems into the NCW to develop Decision Centric Warfare (DCW).[3] Project Maven, launched in April 2017, operationalised deep-learning computer vision to detect and classify objects in full-motion Intelligence, Surveillance, and Reconnaissance (ISR) video at machine speed.[4] From the mid-2010s, the US, China, Russia, and Israel fast-tracked autonomous swarming drones and AI-enabled command-and-control.[5] The US Third Offset Strategy (2014), China's Intelligentised Warfare doctrine (2019), and Russia's President Vladimir Putin's 2017 declaration that the first nation to achieve true AI would 'rule the world' collectively signalled the great-power AI competition.[6]

Russia–Ukraine War

Russia's invasion of Ukraine constitutes the first military conflict in which both belligerents systematically employed AI for military purposes.[7] Ukraine for battlefield facial recognition, AI-assisted signals analysis, and AI-enhanced cyber defences against Russian cyberattacks.[8] Russia fielded AI-enabled loitering munitions, automated targeting, electronic warfare systems, and generative AI for disinformation campaigns at an industrial scale.[9] The war demonstrated that neither side had resolved the governance questions of accountability.

Operations Epic Fury and Roaring Lion

AI was central to targeting, campaign planning, and multi-domain orchestration in Operations Epic Fury and Roaring Lion.[10] AI-supported Air Force mission planning and navigation.[11] Fusing intelligence from multiple sources into a common operating picture, Palantir's Maven enabled strike coordination across domains—operationally impossible through human-only analysis. Maven reduced target-identification time to under one minute.[12] Using real-time data at Al Udeid, AI autonomously flagged threats and issued engagement authorisations.[13] On the Israeli side, the 'Tashan' system identified Iranian ballistic-missile launch points in real time to enable counter-battery strikes before launchers could relocate.[14] 'Rom' maintained continuous hostile-drone alerts, while the 'Bina' Unit generated situational assessments—including civilian-casualty risk estimates.[15] The

"National Message" platform predicted interception-fragment trajectories to enable geographically precise public warnings.[16]

AI-Induced Challenges

Operational success has left a trail of unresolved legal, ethical, and institutional challenges. At 41 missiles per hour in the opening 24 hours, *real-time target verification* was functionally challenging.[17] A US missile strike on a girls' school in Minab, Iran—killing more than 175 civilians, predominantly children—was attributed to outdated mapping data. Researchers characterised the Maven Smart System, generating 3,000 targeting options daily, rendering meaningful human review nearly impractical due to "*automation bias*": the human in the approval chain becomes just a procedural formality.[18]

AI targeting recommendations, unlike conventional intelligence assessments, are embedded in billions of opaque parameters. Anthropic's chief executive acknowledged he could not guarantee the reliability of his systems and thus was designated a "supply chain risk" by the Pentagon for this *unpredictability and black-box behaviour*—a candid admission that even developers cannot fully explain particular outputs.[19]

The Anthropic–Pentagon dispute exposed the *governance void*. The Pentagon demanded Claude for "all lawful purposes," including fully autonomous lethal weapons; Anthropic refused to remove two ethical guardrails and was blacklisted. Claude nonetheless continued to operate within Maven on classified military networks. No legal or institutional framework existed to determine accountability for this outcome.[20]

Finally, *AI misalignment*—divergence between AI behaviour and human intent arising from biased training data or distributional shift—poses risks. Technologies perfected by one nation can be adapted and weaponised against it.[21] The central challenge is structural: AI has outpaced every governance mechanism designed to keep humans in meaningful control.

Role of Military Leadership

The basics of military leadership in the AI era are *governance*. Speed divorced from scrutiny is institutionalised recklessness. Leadership must treat oversight architecture as a prerequisite to capability expansion. No AI-generated targeting recommendation should proceed to engagement without structured, two-step human authorisation. Approval interfaces should not be ceremonial. This should be a binding standard.[22]

Leadership has to focus on *doctrine*. Rules of engagement must specify where AI may autonomously generate targets, where human deliberation is mandatory, and what categories of targets are categorically excluded from AI-only recommendations. Operational tempo must not be permitted to override oversight architecture.[23] The US DoD's January 2026 *AI Acceleration Strategy*—mandating a 'wartime approach' to transform the force into an 'AI-first' organisation—illustrates both ambition and risk: private-sector integration at scale amplifies capability but multiplies the dependencies and failure modes that adversaries can exploit.[24]

Doctrine, in turn, must drive Professional Military Education (PME). The Iran campaign exposed a structural gap between AI integration and human preparedness: cognitive demands and speed of decision-making tested operator training.[25] AI excels at pattern-matching. It is limited in contextual, ethically weighted reasoning, which can affect independent judgment. PME must therefore cultivate the habit of questioning AI outputs. The practice of demanding multiple analytical perspectives before a decision is taken must be ingrained. Future leaders must be trained to synthesise technology with judgement, but at a far greater speed and under far greater escalatory pressure.

Finally, AI-related vulnerabilities—infrastructure dependencies, adversarial manipulation, and single points of failure—transcend service boundaries and demand an all-of-government response. Leadership must ensure that capability development does not outpace the legal frameworks and ethical guardrails.

India's AI-Warfare Readiness

India's strategic environment demands an urgent yet rigorous integration of AI into warfare. The People's Liberation Army (PLA) has structured its entire modernisation trajectory around AI integration. Baidu, Alibaba, and Tencent are systematically co-opted for military AI development.[26] Pakistan's Centre of Artificial Intelligence and Computing (CENTAIC) is transferring AI capabilities to Pakistan's military.[27] During Operation *Sindoor*, Pakistan appeared to receive real-time satellite intelligence and AI-backed targeting support through this channel.[28] India thus confronts a two-front AI challenge.

India's AI-warfare programme has achieved tangible operational credibility. Operation *Sindoor* marked India's first officially acknowledged operational deployment of AI for targeting.[29] Institutionally, the Defence AI Council (DAIC), the Defence AI Project Agency (DAIPA), and the Innovations for Defence Excellence (iDEX) ecosystem have been operational since 2019.[30] The 2022 Artificial Intelligence in Defence (AIDef) symposium launched 75 AI-enabled defence products,

and the ETAI (Evaluating Trustworthy Artificial Intelligence) trustworthy AI framework was released in October 2024.[31]

Three structural gaps, however, critically constrain India's AI-warfare readiness. First, *technology sovereignty*: i.e. India's AI workloads run on foreign cloud infrastructure with critical chips manufactured in Taiwan and China.[32] Second, *inter-service fragmentation*: the services develop AI capabilities in parallel silos with limited doctrine integration.[33] Third, *procurement cycle mismatch*: the standard capital acquisition lifecycle runs five to seven years, while AI and drone technologies evolve much faster—meaning a system procured to counter the 2024 PLA threat will arrive in 2030.[34]

To bridge these gaps, *technology sovereignty* must be treated as a national security imperative. The India AI Mission, the sovereign cloud initiative, and the Defence Research and Development Organisation's (DRDO) semiconductor and edge-computing programmes should be prioritised as strategic initiatives.[35] A *joint AI operations architecture* with a permanent tri-service AI fusion cell, unified data standards, a common doctrine on autonomous targeting, and a formal AI accountability framework is required.[36] *PME must be redesigned* for the AI era. India can field AI-enabled systems; the unresolved question is whether its commanders are trained to govern them under the compressed timelines and escalatory pressures posed by nuclear-armed adversaries.

Conclusion

The 2026 Iran-Israel-US conflict has confirmed that AI is the organising principle of future military campaigns. The tempo of AI-assisted operations achieved in Operation Epic Fury was unprecedented, as was the governance failure of the Anthropic–Pentagon dispute. The accountability vacuum created by legal frameworks, procurement standards, and ethical doctrine that do not keep pace with technology is a major concern.

For India, the challenge is strategic, institutional, and educational. The PLA's intelligentised warfare doctrine and Pakistan's CENTAIC's AI capabilities constitute a two-front AI threat. Institutional architecture must be tied to a clear doctrine specifying the scope of AI use. Technology sovereignty must be treated as a national security imperative; inter-service silos must be dissolved; and PME must be restructured for an AI-era conflict. Ultimately, it is military leadership—through doctrine, education, and institutional example—that will determine whether AI remains a force multiplier under human command or becomes an opaque accelerant of escalation in India's next crisis.

Notes:-

[1] Stephen Robinson, "The Korean War and the OODA Loop: What Happened to the Kill Ratio?" *Ballons to Drones,* April 03, 2025, https://balloonstodrones.com/2025/04/03/the-korean-war-and-the-ooda-loop-what-happened-to-the-kill-ratio/. Accessed on May 18, 2026.

[2] Arthur K. Cebrowski and John H. Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings of the US Naval Institute* vol. 124, no. 1, January 1998, pp. 28–35. https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future. Accessed on May 18, 2026.

[3] Bryan Clark, Dan Patt, and Timothy A. Walton, "Advancing Decision-Centric Warfare," *Hudson Institute,* June 29, 2021, https://www.hudson.org/national-security-defense/advancing-decision-centric-warfare-gaining-advantage-through-force-design-and-mission-integration. Accessed on May 18, 2026.

[4] Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," U.S. Department of Defense, July 21, 2017, https://www.war.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/. Accessed on May 18, 2026.

[5] Alistair MacDonald, "AI-Powered Drone Swarms Have Now Entered the Battlefield," *The Wall Street Journal*, September 02, 2025. https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05. Accessed on May 18, 2026.

[6] Koichiro Takagi, "Artificial Intelligence and Future Warfare," *Hudson Institute,* November 23, 2022, https://www.hudson.org/defense-strategy/artificial-intelligence-future-warfare. Accessed on May 18, 2026.

[7] Vitaliy Goncharuk, "Russia's War in Ukraine: Artificial Intelligence in Defence of Ukraine," *International Centre for Defence and Security,* September 27, 2024, https://icds.ee/en/russias-war-in-ukraine-artificial-intelligence-in-defence-of-ukraine/. Accessed on May 18, 2026.

[8] Sam Bendett, "Roles and Implications of AI in the Russian-Ukrainian Conflict," *Russia Matters,* July 20, 2023, https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict. Accessed on May 18, 2026.

[9] "Russia Using Generative AI to Ramp Up Disinformation, Says Ukraine Minister" *Reuters,* October 16, 2024, https://www.reuters.com/technology/artificial-intelligence/russia-using-generative-ai-ramp-up-disinformation-says-ukraine-minister-2024-10-16/. Accessed on May 18, 2026.

[10] Yehoshua Kalisky and Ido Karp, "AI Use in Operation Roaring Lion," *Institute for National Security Studies,* March 11, 2026, https://www.inss.org.il/social_media/ai-use-in-operation-roaring-lion/. Accessed on May 18, 2026.

[11] Omer Kabir, "From Drones to Warnings: IDF Expands Use of AI in Active Combat against Iran," *Calcalist Tech*, March 30, 2026, https://www.calcalistech.com/ctechnews/article/hyguzhoo11l. Accessed on May 18, 2026.

[12] Artur Markus, "Palantir's Maven Smart System Running on Anthropic's Claude Powers 11,000+ US Strikes in Iran," *Artur Markus,* April 23, 2026, https://www.arturmarkus.com/palantirs-maven-smart-system-running-on-anthropics-claude-powers-11000-us-strikes-in-iran-dod-designates-it-official-programme-of-record-with-25000-military-accounts-deployed/. Accessed on May 18, 2026.

[13] Israel Wullman, "Shaping the New Battlefield: How the IDF Uses AI to Sync Hundreds of Strikes in Iran and Lebanon," *Ynet News*, March 31, 2026, https://www.ynetnews.com/tech-and-digital/article/bk3000ltobe. Accessed on May 19, 2026.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17]Anna Hehir, "AI Warfare Is Outpacing Our Ability to Control It," *Tech Policy Press,* April 03, 2026, https://www.techpolicy.press/ai-warfare-is-outpacing-our-ability-to-control-it/. Accessed on May 19, 2026.

[18] Zaza Tsotniashvili, "Algorithmic Warfare in the Iran Conflict: AI-Driven Decision Compression, the Erosion of Human Oversight, and Accountability Gaps in Contemporary Military Operations," *Zenodo,* March 04, 2026, https://zenodo.org/records/18859998. Accessed on May 19, 2026.

[19] Denise Garcia, "AI in Military Decision-Making: The Global Governance Challenge," *Global Catastrophic Risks 2026*, *Global Challenges Foundation,* 2026, pp. 38–43, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://globalchallenges.org/app/uploads/2025/12/Global-Catastrophic-Risks-2026.pdf#:~:text=Risk%204%20%E2%80%93%20AI%20in,Northeastern%20University%20and%20Commissioner%20at. Accessed on May 18, 2026.

[20] Tal Pinkasovich, "The Paradox Machine: How the AI That Was Banned Won the War," *The Jerusalem Post*, March 22, 2026, https://www.jpost.com/defense-and-tech/article-890738. Accessed on May 19, 2026.

[21] Craig Albert, "Operation Epic Fury: The Promises and Perils of AI Warfare," *The Hill*, March 20, 2026, https://thehill.com/opinion/technology/5790157-ai-military-revolution-warfare/. Accessed on May 19, 2026.

[22] Michael Klare, "AI Plays Major Role in the War on Iran," *Arms Control Today*, May 2026, https://www.armscontrol.org/act/2026-05/news/ai-plays-major-role-war-iran. Accessed on May 19, 2026.

[23] Hadas Lorber, "'AI-First' Warfare: America's Algorithmic Edge in Operation Epic Fury," *The Jerusalem Post*, March 3, 2026, https://www.jpost.com/defense-and-tech/article-888633. Accessed on May 19, 2026.

[24] Daniel Mercer, "Department of War Integrates OpenAI ChatGPT Into GenAI.mil Platform For 3 million Personnel," *The Defense Watch,* February 9, 2026, https://thedefensewatch.com/cyber-space-defense/pentagon-genai-mil-adds-chatgpt. Accessed on May 19, 2026.

[25] Amanda Collazzo, "Warfare at the Speed of Thought: Balancing AI and Critical Thinking for the Military Leaders of Tomorrow," *Modern War Institute at West Point,* February 21, 2025, https://mwi.westpoint.edu/warfare-at-the-speed-of-thought-balancing-ai-and-critical-thinking-for-the-military-leaders-of-tomorrow/. Accessed on May 19, 2026.

[26] Harsh V. Pant and Angad Singh, "AI in Modern Warfare: India's Strategic Challenges and Opportunities," *Observer Research Foundation,* February 27, 2026, https://www.orfonline.org/expert-speak/ai-in-modern-warfare-india-s-strategic-challenges-and-opportunities. Accessed on May 19, 2026.

[27] Diana George, "China's Invisible Hand? CENTAIC Emerges as Nerve Centre of Pakistan's AI-Driven Air Force," *Times Now World,* August 07, 2025, https://www.timesnownews.com/world/asia/china-invisible-hand-centaic-emerges-as-nerve-centre-of-pakistan-ai-driven-air-force-article-152425022. Accessed on May 19, 2026.

[28] Satyen K. Bordoloi, "The Major Threat to India's AI War Capability: Lack of Indigenous AI," *Sify,* August 12, 2025, https://www.sify.com/ai-analytics/the-major-threat-to-indias-ai-war-capability-lack-of-indigenous-ai/. Accessed on May 19, 2026.

[29] Rajiv Kumar Sahni, "AI Gives India 94% Precision Edge in Operation Sindoor," *The Defense Post*, October 07, 2025, https://www.google.com/search?q=%22AI+Gives+India+94%25+Precision+Edge+in+Operation+Sindoor%2C%22&oq=%22AI+Gives+India+94%25+Precision+Edge+in+Operation+Sindoor%2C%22&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQIRigATIHCAIQIRigATIHCAMQIRigATIHCAQQIRigATIHCAUQIRiPAjIHCAYQIRiPAtIBCDE1MDdqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8. Accessed on May 20, 2026.

[30] Press Information Bureau, Government of India, "Task Force for Implementation of AI," March 28, 2022, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mod.gov.in/sites/default/files/PRESS%20RELEASE%20%20rajy%20sabha.pdf. Accessed on May 20, 2026.

[31] Press Information Bureau, Government of India, "Raksha Mantri launches 75 Artificial Intelligence products/technologies during first-ever 'AI in Defence' symposium & exhibition in New Delhi; Terms AI as a revolutionary step in the development of humanity," July 11, 2022, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1840740&reg=3&lang=2. Accessed on May 19, 2026.

[32] Anjul Sahu, "Top 5 Sovereign AI Cloud Providers in India: Leading the AI Factory Revolution," *Cloud Raft,* March 05, 2026, https://www.cloudraft.io/blog/top-5-sovereign-ai-cloud-in-india . Accessed on May 20, 2026.

[33] Soumya Awasthi, "Artificial Intelligence and India's National Security," *Observer Research Foundation,* March 29, 2026, https://www.orfonline.org/expert-speak/artificial-intelligence-and-india-s-national-security. Accessed on May 20, 2026.

[34] Rahul Verma, "PLA Drone Threat and India's High-Altitude Procurement Reforms," *Indian Aerospace and Defence Bulletin*, May 12, 2026, https://www.iadb.in/2026/05/12/pla-drone-threat-indias-high-altitude-procurement-reforms/. Accessed on May 20, 2026.

[35] Nisha Holla, "Operationalising India's Sovereign AI Stack: From Intent to Capability," *Observer Research Foundation,* February 19, 2026, https://www.orfonline.org/expert-speak/operationalising-india-s-sovereign-ai-stack-from-intent-to-capability. Accessed on May 20, 2026.

[36] DS Hooda, "Implementing Artificial Intelligence in the Indian Military," *Delhi Policy Group*, February 16, 2023, https://www.delhipolicygroup.org/publication/policy-briefs/implementing-artificial-intelligence-in-the-indian-military.html. Accessed on May 20, 2026.