National Maritime Foundation

https://maritimeindia.org/

ARTIFICIAL INTELLIGENCE AND THE TRANSFORMATION OF MODERN WARFARE: ISR, TARGETING, AND INDIA'S STRATEGIC CHALLENGE

Captain KS Vikramaditya, Indian Navy

INTRODUCTION

1. The character of warfare is undergoing a profound transformation, driven not merely by the introduction of new platforms or weapons, but by the emergence of data as the central element of combat power. Modern battlefields are increasingly saturated with sensors, ranging from satellites and unmanned aerial systems, to electronic intelligence platforms and open-source data streams, producing volumes of information that far exceed human capacity to process in real time.[1] In this environment, the decisive advantage no longer lies solely in possessing superior platforms, but in the ability to rapidly ingest, fuse, interpret, and act upon data. Artificial Intelligence (AI) has emerged as the critical enabler of this transformation.[2]

2. At its core, AI is reshaping warfare by compressing the traditional "kill chain", the sequence of steps from detection and identification of a target to engagement and assessment. Historically, this process has been labour-intensive and time-consuming, requiring multiple layers of human analysis and coordination. However, AI-enabled systems are increasingly capable of automating key stages of this chain, particularly in intelligence, surveillance, and reconnaissance (ISR), threat evaluation, and target prioritisation.[3] The result is a shift from deliberative, human-paced decision-making to near real-time, algorithmically assisted operations.

3. This transformation is underway as we speak. Contemporary conflicts, particularly in Ukraine and across the Middle East, provide clear evidence of how AI and autonomy are altering the conduct of warfare. In Ukraine, the widespread use of unmanned systems ranging from inexpensive first-person-view (FPV) drones to more sophisticated loitering munitions has demonstrated the growing importance of scalable, data-driven targeting.[4] Similarly, Iran's deployment of systems such as the *Shahed*-series drones, and Russia's adaptation of these

---

[1] C. Heitzenrater et al., "How Artificial Intelligence Could Reshape Four Essential Competitions in Future Warfare", RAND Corporation, 2026.
https://www.rand.org/content/dam/rand/pubs/research_reports/RRA4300/RRA4316-1/RAND_RRA4316-1.pdf

[2] Michael C. Horowitz et al., "Artificial Intelligence and International Security", Center for a New American Security (CNAS), July 2018.
https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

[3] U.S. Department of Defense, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy".
https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

[4] Jack Watling, Nick Reynolds, Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine, Royal United Services Institute (RUSI), May 2023.
https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine

platforms into the *Geran* series, illustrate how relatively low-cost systems can achieve strategic impact when combined with persistent ISR and coordinated targeting.[5]

4. Parallel to these developments, state-of-the-art military AI programmes, such as the United States Department of Defence's Project *Maven*, highlight the institutionalisation of AI within command-and-control architectures. Initially conceived as a tool for analysing full-motion video from unmanned systems, *Maven* has evolved into a broader data-centric platform capable of integrating information from a wide array of sensors, generating a common operational picture (COP), and supporting targeting workflows.[6]

5. The convergence of AI-enabled data fusion and autonomous systems represents a fundamental shift in military power. Unmanned platforms, whether aerial, maritime, or subsurface, are no longer merely remote-controlled assets but are becoming capable of independent perception, decision-making, and action within defined parameters. AI enhances these systems by enabling operation in contested environments, such as under conditions of electronic warfare or Global Navigation Satellite System (GNSS) denial — improving target discrimination and allowing coordinated behaviour among multiple platforms.

6. This paper argues that the transformation from platform-centric to data-centric warfare is not a future prospect but a present reality — and that India, operating in a two-front threat environment against adversaries who are structurally ahead in this transition, faces a compounding strategic disadvantage that platform investment alone cannot address. The challenge is not the absence of capability in isolation, but the absence of the network architecture, data standards, and institutional frameworks that would allow existing and future capabilities to function as a coherent, AI-enabled operational system. Addressing this gap requires not incremental modernisation but a dual-track response: immediate, operationally bounded AI deployments that deliver tangible value, while simultaneously building the foundational data and network architecture that long-term transformation demands. The paper proceeds by examining AI's role in ISR, threat evaluation, autonomous targeting, and contested battlespace dynamics — grounding the analysis in contemporary conflict evidence — before diagnosing India's specific structural lacunae and proposing a phased, actionable response.

EVOLUTION OF WARFARE: FROM PLATFORM-CENTRIC TO NETWORK-CENTRIC TO DATA-CENTRIC (ALGORITHMIC WARFARE)

7. The evolution of warfare in the modern era represents a layered progression through distinct paradigms, each building upon the last. The trajectory moves from platform-centric warfare to network-centric warfare (NCW), and now toward data-centric or algorithmic warfare, where artificial intelligence functions as the central enabler.

---

[5] Matthew Bint, Fabian Hinz, "Russia doubles down on the Shahed", International Institute for Strategic Studies (IISS), 11 April 2025. https://www.iiss.org/online-analysis/military-balance/2025/04/russia-doubles-down-on-the-shahed/#:~:text=In%202022%2C%20Iran%20began%20supplying%20Shahed%20131,Russian%20use%20in%20the%20war%20in%20Ukraine

[6] Gregory C. Allen, "Six Questions Every DOD AI and Autonomy Program Manager Needs to Be Prepared to Answer", Center for Strategic and International Studies (CSIS), May 2023. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/230515_Allen_Six_Questions.pdf?VersionId=zdOM8qS30hmQRV_4JjbPTMzLukCCm3Bk#.
Also see: Gregory C. Allen, "Project *Maven* Brings AI to the Fight Against ISIS", Center for a New American Security (CNAS), 21 December 2017.
https://www.cnas.org/publications/commentary/project-*Maven*-brings-ai-to-the-fight-against-isis

8. In the platform-centric paradigm, which dominated much of industrial-era warfare and persisted into the late twentieth century, combat power was primarily derived from individual platforms — tanks, aircraft, ships, and artillery systems. These platforms operated largely as discrete units, with limited real-time integration. Superiority was achieved through qualitative advantages in platform capability or quantitative advantages in mass. Information flows were hierarchical and often delayed, constraining the speed and flexibility of decision-making.

9. The emergence of network-centric warfare in the 1990s and early 2000s marked the first major departure from this model. NCW sought to connect sensors, decision-makers, and shooters through robust communication networks, enabling shared situational awareness across the force. The central idea was that networking geographically dispersed forces would generate increased combat power through information superiority.[7] By linking platforms into a unified network, militaries could reduce uncertainty, improve coordination, and accelerate decision cycles. The success of this approach was evident in operations such as the Gulf War and subsequent conflicts, where NCW enabled highly coordinated (and effective) operations.

10. However, while NCW significantly improved the flow and accessibility of information, it remained fundamentally dependent on human operators for interpretation and decision-making. As the number and diversity of sensors increased, the nature of the data itself became more complex. Operators were required not only to process vast quantities of information from multiple sources — imagery, signals, telemetry, and reports — but also to interpret behavioural patterns and pattern-of-life observations derived from persistent surveillance.[8] These datasets were often heterogeneous in format, temporally distributed, and in many cases available in raw or semi-processed forms, requiring significant cognitive effort to correlate and contextualise.

11. This introduced a deeper limitation. The challenge was not simply that there was too much data, but that the data embodied multi-dimensional relationships across time, space, and behaviour, all of which exceeded human cognitive capacity to fully exploit in real time. For instance, identifying a target based on a single image or signal is a relatively bounded task. However, identifying a target based on deviations from established behavioural patterns over time, such as changes in movement routines, communication signatures, or logistical flows, requires the integration of diverse data streams and the recognition of subtle, often non-linear patterns. Network-centric systems, while effective in distributing such data, lacked the inherent capability to extract these deeper insights.

12. It is within this context that the shift toward data-centric or algorithmic warfare emerges. The defining feature of this paradigm is not merely the presence of networks, but the integration of artificial intelligence to process, fuse, and interpret data at scale. AI transforms networks from passive conduits of information into active systems capable of generating insight. In contrast to NCW, where the emphasis was on connectivity, data-centric warfare emphasises comprehension and decision advantage. This distinction is critical. Network-centric systems answer the question, *"Who knows what?"* Data-centric, AI-enabled systems answer, *"What does it mean, and what should be done?"*

---

[7] David S. Alberts, John J. Garstka, Frederick P. Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority", Command and Control Research Program (DoD), 1999. https://apps.dtic.mil/sti/tr/pdf/ADA406255.pdf

[8] Jan Girman, "Pattern-of-life analysis for intelligence", Cambridge Intelligence, 05 August 2025. https://cambridge-intelligence.com/pattern-of-life-analysis/

13. Artificial intelligence enables this transition by automating key cognitive functions — pattern recognition, anomaly detection, correlation across disparate data sources, and predictive analysis. Crucially, it enables the extraction of meaning not only from structured data, but also from unstructured and behaviourally rich datasets, including full-motion video, signal environments, and long-duration pattern-of-life observations. These capabilities allow for the creation of a dynamic, continuously updated understanding of the battlespace.

14. The evolution from NCW to data-centric warfare also reflects a shift in the locus of combat power — from the ability to share information across platforms to the exploitation of data more effectively than the adversary. This includes not only faster processing, but also deeper understanding and more accurate prediction of adversary behaviour. As a result, the battlespace becomes increasingly defined by the competition between algorithms as much as between platforms.

15. Contemporary conflicts illustrate this transition in practice. In Ukraine, both sides operate within highly networked environments, utilising drones, satellite communications, and digital coordination tools. However, the increasing incorporation of AI, whether in the form of automated targeting aids, image recognition systems, or navigation algorithms, demonstrates the move beyond simple connectivity toward algorithmic exploitation of data. Similarly, systems such as the United States' Project *Maven* mentioned earlier represent the institutionalisation of this paradigm, where data from multiple sources is not only shared but actively processed and transformed into operational outputs.

16. This evolution is reflected in doctrinal constructs such as the US Combined Joint All-Domain Command and Control (CJADC2). While CJADC2 emerged from the principles of NCW, it now depends fundamentally on artificial intelligence which shifts it from a system that merely shares information to one that generates actionable understanding — thus transforming CJADC2 from a connectivity-driven framework into a data-centric decision architecture capable of supporting operations at scale.[9]

17. Despite its advantages, the transition to data-centric warfare introduces new challenges. The reliance on AI for data interpretation raises concerns regarding reliability, transparency, and human oversight. While networks expanded the reach of information, AI concentrates interpretive power within algorithms, potentially obscuring the basis for decisions. This creates dissonance between speed and control, as the drive to accelerate decision-making may come at the cost of reduced human scrutiny.

18. Thus, the evolution from platform-centric to data-centric warfare represents not just a technological progression, but a fundamental shift that underpins the future of warfare — a future that is already upon us.

AI IN ISR: FROM DATA COLLECTION TO DECISION ADVANTAGE

19. If network-centric warfare sought to connect sensors, decision-makers, and shooters, the next step in military evolution has been to extract meaning from the data those networks produce. Nowhere is this more important than in intelligence, surveillance, and reconnaissance

[9] U.S. Department of Defense, "Summary of the Joint All-Domain Command and Control Strategy", March 2022. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

(ISR). Contemporary ISR architectures gather data from a growing range of sources, including satellites, unmanned aerial systems, synthetic-aperture radar, electro-optical and infrared sensors, communications intercepts, and increasingly, open-source and commercially available data. The US Department of Defence's own data strategy explicitly recognises that survival on the modern battlefield depends on making connections among data from diverse sources[10] and using analytic tools to generate superior situational awareness and precision effects.[11]

20. The significance of AI in this context lies not merely in speed, but in the conversion of fragmented and heterogeneous information into operationally useful understanding. Traditional ISR systems could collect and disseminate data, but they remained heavily dependent on human analysts to classify, correlate, and interpret inputs. As data volumes increased, this model became progressively less viable. CSET's 2025 study on AI for military decision-making notes that commanders increasingly seek AI-enabled decision support because they must integrate large amounts of information quickly under conditions of severe time pressure. That study identifies data fusion, computer vision, anomaly detection, and recommendation systems as core enabling technologies in contemporary military AI decision-support systems.[12]

21. This is especially relevant in ISR because the challenge is not simply to detect objects, but to infer significance. A radar return, a thermal image, a moving vehicle, a set of emissions, or a recurring travel pattern, may each be individually unremarkable. Their operational meaning often emerges only when they are correlated across time, space, and mode of collection. AI allows that correlation to take place at a scale and speed that human analysts alone cannot sustain.[13] In practical terms, this means AI can assist in object detection, geospatial analysis, change detection, anomaly identification, and pattern-of-life assessment; but more importantly, it can help transform raw collection into a common operational picture that is usable for planning, targeting, and force protection.[14]

22. Project *Maven* is the most important contemporary example of this shift from collection-centric ISR to AI-enabled exploitation. Gregory Allen's 2017 CNAS commentary on Project *Maven* explained that the programme aimed to use computer vision to help analysts sift through massive quantities of drone video more rapidly and accurately.[15] That initial formulation is crucial because it captures the original military problem AI was meant to solve: not the absence of collection, but the inability to exploit collection efficiently enough.

23. Over time, however, *Maven* evolved from a narrowly scoped imagery-analysis effort into a broader architecture for AI-enabled military decision support. *Defense One* reported in 2022 that the National Geospatial-Intelligence Agency would take over Project *Maven*, describing it as a flagship Pentagon AI programme designed to identify objects within vast volumes of surveillance data.[16] By 2024, CSET's report *Building the Tech Coalition* showed that *Maven* had

---

[10] U.S. Department of Defense, "DOD Data Strategy", Oct 2020.
https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF
[11] U.S. Department of Defense, "Summary of the Department of Defense Artificial Intelligence Strategy", Feb 2019.
https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF
[12] Emelia S Probasco, Helen Toner, Matthew Burtell, Tim G J Rudner "AI for Military Decision-Making", Center for Security and Emerging Technology (CSET), April 2025.
https://cset.georgetown.edu/wp-content/uploads/CSET-AI-for-Military-Decision-Making.pdf
[13] Probasco et al., AI for Military Decision-Making".
[14] U.S. Department of Defense, "Summary of the Department of Defense Artificial Intelligence Strategy".
[15] Gregory C. Allen, "Project *Maven* brings AI to the fight against ISIS", Center for a New American Security (CNAS), 21 Dec 2017.
https://www.cnas.org/publications/commentary/project-*Maven*-brings-ai-to-the-fight-against-isis
[16] Patrick Tucker, "NGA Will Take Over Pentagon's Flagship AI Program", Defense One, 25 Apr 2022.
https://www.defenseone.com/technology/2022/04/nga-will-take-over-pentagons-flagship-ai-program/366098/

moved well beyond simple object recognition.[17] It had become part of a broader operational workflow linking software, AI models, analysts, and targeting processes in support of the US 18th Airborne Corps, drastically reducing the time and manpower needed to generate targeting outputs. CSET describes this as a case of operationalising software and artificial intelligence for clear military advantage, rather than just experimenting with AI in isolation.

24. The ISR significance of *Maven* is, therefore, twofold. First, it demonstrates that AI can improve the throughput of ISR analysis by reducing the time required to move from raw sensor data to interpreted intelligence.[18] Second, and more importantly, it shows that AI in ISR is no longer confined to the back-end analytic function. It is increasingly embedded within a larger chain that connects sensing, analysis, prioritisation, and operational action.[19] In this sense, AI-enabled ISR does not simply support commanders with "more" information; it supports them with more filtered, prioritised, and actionable understanding. This is a qualitatively different function from traditional ISR exploitation, and it is one reason why AI has become central to debates over contemporary command-and-control systems.

25. However, the integration of AI into ISR workflows introduces a parallel set of risks that must be carefully considered. As CSET's 2025 study stresses, AI-enabled military decision-support systems can enhance situational awareness and accelerate decisions, but they also introduce risks if their scope, limitations, and failure modes are poorly understood. In an ISR setting, those risks are especially acute because the outputs of AI systems may carry an aura of technical authority that encourages overconfidence.[20] A model may successfully identify patterns in imagery, emissions, or behavioural data, yet still be wrong in ways that are difficult for operators to detect under time pressure. The problem is not only technical error; it is also the propensity of human users to defer to automated recommendations, especially when the system is embedded in high-tempo operational workflows.

26. More broadly, AI in ISR should be understood as the foundation upon which several other military applications rest. Threat evaluation and resource allocation depend on reliable and timely battlespace understanding. Autonomous systems depend on machine perception and environment recognition. Counter-UAV operations depend on rapid classification and discrimination amid clutter, deception, and time compression. In all these areas, ISR is not merely a supporting function, it is the cognitive substrate of military action. The importance of AI therefore lies not just in helping militaries collate data, but in determining what this data means and what needs to be done about it.

AI IN THREAT EVALUATION AND RESOURCE ALLOCATION (TERA)

27. The transformation of ISR through artificial intelligence finds its most consequential downstream expression in threat evaluation and resource allocation. While ISR provides the processed understanding of the battlespace, it is within TERA that decisions are made regarding which targets matter, how they should be prioritised, and what resources should be allocated to act upon them. Conventional command-and-control systems have long employed rule-based

---

[17] Emelia S. Probasco, "Building the Tech Coalition: How Project *Maven* and the U.S. 18th Airborne Corps Operationalized Software and Artificial Intelligence for the Department of Defense", Center for Security and Emerging Technology (CSET), Aug 2024.
https://cset.georgetown.edu/wp-content/uploads/CSET-Building-the-Tech-Coalition-1.pdf
[18]Probasco, "Building the Tech Coalition".
[19] Probasco, "AI for Military Decision-Making".
[20] Probasco, "AI for Military Decision-Making".

frameworks and predefined engagement protocols for this purpose — effective in stable and predictable environments but inherently limited when confronted with the scale, variability, and ambiguity of contemporary battlespaces. Artificial intelligence does not replace these systems but transcends their limitations by enabling adaptive, data-driven decision-making - continuously learning from incoming data, recognising previously unseen patterns, and updating assessments dynamically in ways that deterministic, rules-based logic cannot.

28. At the core of this challenge lies the compression of decision time. Modern battlefields — characterised by drone warfare, electronic contestation, and distributed operations, operate at a tempo that increasingly exceeds human cognitive and organisational capacity. AI addresses this by enabling the automation and augmentation of key cognitive functions: prioritisation, classification, prediction, and optimisation.[21] Threat evaluation, in its most basic form, involves determining whether a detected entity constitutes a legitimate and significant target — a determination which, in contemporary warfare, requires assessment across behavioural patterns, historical activity, environmental conditions, and correlations across multiple data sources simultaneously. AI enables this multi-dimensional assessment at a scale and speed that human operators alone cannot sustain, whether in identifying hostile movement patterns through signals correlation, discriminating swarm threats from benign objects in counter-UAV operations, or detecting anomalous vessel behaviour in congested maritime environments. CSET's analysis highlights that recommendation systems and optimisation algorithms can assist commanders in selecting courses of action that maximise operational effectiveness under constraints.[22]

29. The distinction between rule-based and AI-enabled systems becomes particularly evident in counter-UAV operations. A conventional system may rely on predefined thresholds - such as speed, altitude, or trajectory - to classify and prioritise incoming aerial objects. However, in a swarm scenario involving dozens or hundreds of low-cost drones, such rule-based approaches can quickly become saturated or fail to account for adaptive adversary behaviour. AI-enabled systems, by contrast, can analyse patterns across multiple targets simultaneously, identify coordinated swarm dynamics, and prioritise threats based on collective behaviour rather than isolated parameters. This enables more effective allocation of limited defensive resources under conditions of extreme time compression.

30. Resource allocation — matching available kinetic, electronic warfare, and cyber response options to prioritised threats — represents the final step in this chain. In conventional systems this process is time-consuming and coordination-intensive, requiring communication across multiple command layers. AI enables a more integrated approach by linking threat evaluation directly with resource assignment, allowing near real-time decision support: recommending optimal interceptor allocation against incoming drones, or determining whether a target should be engaged immediately or monitored further based on evolving intelligence.

31. The integration of AI into TERA also introduces significant risks. The compression of decision time reduces opportunities for human oversight, increasing the likelihood that errors in data or model assumptions translate directly into operational consequences. Moreover, automation bias — the tendency identified earlier to defer to AI outputs without sufficient scrutiny — is particularly acute in TERA contexts because the recommendations generated are directly action-linked. In ISR, a misclassified object delays understanding. In TERA, a misclassified threat triggers a response.[23] The effectiveness of AI-enabled decision support systems depends not only on their technical performance but on the extent to which human

---

[21] U.S. Department of Defense, "Defense Artificial Intelligence Strategy".
[22] Probasco, "AI for Military Decision-Making".
[23] Probasco, "AI for Military Decision-Making".

users understand their limitations and remain actively engaged — a balance that will become increasingly difficult to maintain as AI systems are integrated more deeply into targeting workflows and the boundaries between decision support and decision-making become progressively blurred.

AI, AUTONOMOUS SYSTEMS, AND THE TRANSFORMATION OF TARGETING

32. The integration of artificial intelligence into targeting workflows represents the most consequential expression of the broader shift from human-paced to algorithmically assisted warfare. At the foundation of this transformation lies machine perception — the ability of AI-driven systems to detect, classify, and track objects across cluttered, contested, and dynamic environments without dependence on predefined signatures or continuous operator input. Unlike traditional rule-based systems, which depend on predefined signatures or operator input, AI-driven platforms increasingly operate in a goal-oriented manner, where the objective is defined but the method of execution is determined by the machine itself.[24] This enables dynamic adaptation to changing conditions and a degree of operational independence that is particularly significant in high-tempo environments where manual analysis is infeasible.

33. One of the most significant operational implications of AI-enabled systems lies in their ability to function under conditions where traditional navigation and targeting aids such as Global Navigation Satellite Systems (GNSS) are degraded or denied. AI-enabled systems do not "restore" GNSS in denied environments, rather, they reduce dependence on it by inferring position and motion from other sensors and continuously correcting drift through sensor fusion.[25] In practice, this involves combining inertial navigation with visual inertial odometry, LiDAR or radar odometry, terrain-relative navigation, SAR or map matching, and signals of opportunity. AI contributes by improving feature extraction, scene recognition, map correlation, spoofing detection, and the adaptive weighting of conflicting sensor inputs. The result is not perfect navigation, but resilient navigation — sufficient for continued mission execution even when satellite signals are jammed, spoofed, or unavailable.[26]

34. Beyond navigation, AI enhances target discrimination — the ability to distinguish between legitimate military objectives and non-targets in environments where civilian and military patterns overlap. AI-enabled systems can analyse visual signatures, behavioural patterns, and contextual indicators simultaneously, supporting more nuanced identification in the dynamic and ambiguous contexts that characterise contemporary conflict.

35. The operational consequences of this shift are particularly evident in the increasing use of AI-assisted targeting systems. Advances in machine learning have enabled target recommendations at a scale impossible through traditional methods — reflecting a shift toward machine-driven acceleration of the observe-orient-decide-act (OODA) loop.[27] In Ukraine, the widespread use of drones and real-time ISR has created a battlespace in which targets emerge, move, and disappear rapidly, placing a premium on speed while introducing significant ambiguity, particularly in urban environments where civilian and military activity intersect.[28]

---

[24] Scharre, Army of None: Autonomous Weapons and the Future of War (New York: W.W. Norton, 2018), 36–37, 39–40. Available at https://ftp.idu.ac.id/wp-content/uploads/ebook/tdg/MILITARY%20PLATFORM%20DESIGN/Army%20of%20None%20Autonomous%20Weapons%20and%20the%20Future%20of%20War.pdf

[25] UAV Navigation, "AI-Based Navigation in GNSS-Denied Areas", Company Blog, 02 October 2023. https://www.uavnavigation.com/company/blog/ai-based-navigation-gnss-denied-areas#:~:text=A%20key%20component%20of%20AI,external%20inputs%20like%20satellite%20signals

[26] Elif Ece Elmas, Mustafa Alkan, "Multi-sensor Data Fusion for Autonomous Unmanned Aerial Vehicle Navigation in GPS Denied Environments", International Journal of Computing, 23(4) 2024, 625-636, 31 December 2024. https://computingonline.net/files/journals/1/archieve/IJC_2024_23_4_12.pdf

[27] Scharre, Army of None, 30–31.

[28] Jack Watling and Nick Reynolds, Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine.

36. More explicit concerns regarding AI-enabled targeting have emerged in the context of Israeli military operations in Gaza. Open-source investigative reporting has described the use of several AI-assisted systems, including *Lavender*, *Where's Daddy?*, and *The Gospel*, designed to support large-scale target generation and prioritisation.[29] These systems reportedly draw upon extensive datasets, including communications metadata, pattern-of-life indicators, and behavioural associations, to identify individuals and infrastructure for potential targeting.

37. The system referred to as *Lavender* has been described as generating lists of potential targets based on probabilistic assessments of affiliation, while *Where's Daddy?* has reportedly been used to track individuals to residential locations in order to facilitate targeting decisions. *The Gospel*, in turn, has been associated with the rapid generation of infrastructure-related targets, significantly expanding the scope and speed of target identification.[30]

38. Taken together, these systems illustrate a shift toward what may be characterised as an AI-driven targeting pipeline, in which multiple stages of the targeting process — identification, correlation, prioritisation, and tracking — are increasingly supported by automated or semi-automated systems.

39. While these systems are intended to enhance operational efficiency, they have generated significant debate among analysts regarding the extent to which human oversight can be meaningfully exercised at such scale. Particularly contentious is the use of behavioural and network-based indicators to identify targets, where individuals may be flagged based on patterns of association or movement rather than direct evidence of hostile activity. In densely populated environments, this approach carries a heightened risk of misclassification. The deeper concern is structural rather than individual: that under conditions of sustained operational pressure, the human role in AI-assisted targeting may contract not through deliberate policy but through the cumulative weight of volume and tempo — with operators functioning as approval nodes rather than independent evaluators, not because they choose to but because the system architecture subliminally guides them to do so.

40. Project *Maven* illustrates both the advantages and the structural risks of this transformation. By enabling automated analysis of full-motion video and other ISR data, *Maven* significantly increased the speed at which objects could be detected, classified, and flagged.[31] The targeting process conventionally comprises six sequential stages: identification, localisation, filtering for lawful and valid targets, prioritisation, assignment to firing units, and engagement. Recent reporting suggests that AI-enabled systems such as *Maven* are capable of performing up to four of these six stages autonomously.[32] The operational impact is substantial: target nomination rates have increased from approximately 30 to 80 targets per hour,[33] with elements of the targeting cycle completed in less than a minute.[34] The manpower implications are equally significant. Whereas targeting operations during Operation IRAQI FREEDOM relied on

---

[29] Dr. Ehab Khalifa, "Blind Technology: Israel's AI Deployment in Gaza and Lebanon Wars", Future for Advanced Research and Studies, 07 October 2024. Future Center - Israel's AI Deployment in Gaza and Lebanon Wars

[30] Michael N. Schmitt, "Israel – Hamas 2024 Symposium – The Gospel, Lavender, and the Law of Armed Conflict", Lieber Institute, West Point, 28 June 2024. Israel – Hamas 2024 Symposium - The Gospel, Lavender, and the Law of Armed Conflict - Lieber Institute West Point

[31] Gregory C. Allen, "Project *Maven* Brings AI to the Fight Against ISIS".

[32] Probasco, "Building the Tech Coalition".

[33] Katrina Manson, "US Military operators started out skeptical about AI, but now they are the ones developing and using Project *Maven* to identify targets on the battlefield", Bloomberg Businessweek, 28 February 2024. https://www.bloomberg.com/features/2024-ai-warfare-project-*Maven*/

[34] Todd South, "This system may allow small Army teams to probe 1,000 targets per hour", DefenseNews, 22 August 2024. https://www.defensenews.com/news/your-army/2024/08/21/this-system-could-allow-sm all-army-teams-to-hit-1000-targets-per-hour/

analytical cells of roughly 2,000 personnel, comparable outputs have been achieved by the US 18th Airborne Corps using a cell of 20.[35]

41. In February of 2024, Project *Maven* was employed to support target refinement for airstrikes in Iraq and Syria and was reportedly involved in over 85 strike operations. During the same period, it was also utilised to detect and track rocket launchers in Yemen, as well as surface vessels in the Red Sea, some of which were subsequently engaged and destroyed.[36] More broadly, *Maven* functions as a shared data and AI-enabled system within CENTCOM, integrating inputs from approximately 179 live data feeds across command and control, fires, force protection, and sustainment functions.[37] Taken together, these developments point to a fundamental transformation in the nature of targeting: from a process constrained by human and rule-based analytical capacity, to one defined by machine-enabled scale and speed.

42. However, the concern highlighted earlier — as autonomy increases, human roles would shift toward supervisory control rather than direct decision-making — raises important questions about the adequacy of human oversight in high-speed engagements. The airstrike on the Shajareh Tayyebeh girls' elementary school in Minab, Iran, on the first day of Operation EPIC FURY (28 February 2026), which killed more than 165 civilians — the majority of them schoolchildren — has raised substantive questions about the role of AI-assisted targeting systems in generating the strike. Investigations by the Washington Post, TIME, CBC, and Amnesty International, concluded that the US was likely responsible, with sources familiar with the internal investigation indicating that the school had been incorrectly tagged as a military facility in intelligence databases.[38] More than forty US senators demanded answers from the Department of Defence regarding the strike and associated civilian casualties.[39] Legal analysts, including in a formal targeting analysis published by *Just Security*, raised specific concerns about the use of the *Maven* Smart System — which had been employed to generate targeting packages for the operation at a scale of up to 1,000 per hour — and the adequacy of human verification within the targeting pipeline.[40] While definitive attribution to any specific system remains contested, the incident illustrates, with tragic clarity, how AI-assisted targeting pipelines operating at machine speed and scale can translate intelligence errors into irreversible kinetic consequences before human verification can intervene.

43. The transition to algorithmic warfare fundamentally recalibrates the traditional escalation ladder. *By compressing the "kill chain" to machine speed and generating target nominations at a scale that generates a "structural lacuna" in human verification, the "strategic pause" — that critical window for political deliberation and de-escalation — is effectively marginalised.* This creates a dangerously lower threshold

---

[35] Probasco, "Building the Tech Coalition".
[36] Katrina Manson, "US Used AI to Help Find Middle East Targets for Airstrikes", Bloomberg, 26 February 2024. AI Airstrikes: Pentagon Used the Tech to Find Middle East Targets - Bloomberg
[37] Sydney J Freedberg Jr, "Success begets challenges': NGA struggles to meet rising demand for *Maven* AI", Breaking Defense, 03 September 2024. 'Success begets challenges': NGA struggles to meet rising demand for *Maven* AI - Breaking Defense
[38] Joby Warrick and Missy Ryan, "Evidence suggests the deadly blast at an Iranian school was likely a US airstrike", The Washington Post, 6 March 2026. https://www.washingtonpost.com/world/2026/03/06/iran-minab-girls-school-airstrike-us-israel/f04850c8-1988-11f1-aef0-0aac8e8e94db_story.html
[39] Tim Kaine, "Kaine & Colleagues Lead More Than 40 Senators in Demanding Answers from the Department of Defense on Elementary School Strike and Civilian Casualties in Iran", 11 March 2026. https://www.kaine.senate.gov/press-releases/kaine-and-colleagues-lead-more-than-40-senators-in-demanding-answers-from-the-department-of-defense-on-elementary-school-strike-and-civilian-casualties-in-iran
[40] Joseph N Orenstein, "When Intelligence Fails: A Legal Targeting Analysis of the Minab School Strike", Just Security, 26 March 2026. https://www.justsecurity.org/134350/legal-analysis-minab-school-strike/#:~:text=Introduction,Corps%20(IRGC)%20naval%20base

for kinetic engagement, where tactical-level algorithmic errors or keyword-driven misclassifications can rapidly catalyse into a strategic-level crisis. In such an environment, the risk is no longer limited to localised failures of distinction. Rather, it manifests as a systemic acceleration of conflict that may outpace the capacity of political leadership to intervene or signal restraint.

44. Ultimately, the integration of artificial intelligence into autonomous and targeting systems represents a fundamental shift in the character of warfare. The central challenge for modern militaries, however, is not simply to develop more capable AI-enabled systems, but to ensure that the increasing speed and scale of machine-driven warfare is adequately tempered by robust frameworks of human oversight, accountability, and operational validation.

AI vs AI WARFARE: COUNTER-UAV, ELECTRONIC WARFARE, AND THE CONTESTED BATTLESPACE

45. The integration of artificial intelligence into contemporary military systems has not only accelerated offensive targeting capabilities but has also fundamentally reshaped defensive architectures and countermeasure strategies. As AI-enabled systems compress detection-to-engagement timelines, adversaries are simultaneously deploying adaptive countermeasures, giving rise to an emerging paradigm best understood as "AI versus AI warfare". In such an environment, operational advantage is no longer determined solely by the ability to generate targets, but by the ability to degrade, disrupt, and outpace the adversary's decision-making systems within tightly contested operational timelines.

46. This transformation is most visible in the domain of counter-unmanned aerial systems (C-UAS), which the NATO Joint Air Power Competence Centre (JAPCC) characterises as a *"wicked problem"* requiring a comprehensive, multi-domain approach rather than a single technological solution.[41] The proliferation of low-cost drones in conflicts such as that in Ukraine has created a battlespace defined by persistent surveillance, distributed targeting, and continuous strike cycles, exposing the limitations of traditional air defence systems designed for high-value, low-volume threats.[42] Modern C-UAS architectures have, therefore, evolved into layered, system-of-systems approaches, reflecting a broader conceptual shift: countering a drone is no longer limited to destroying a platform but involves disrupting an interconnected operational system comprising the vehicle, communication links, control architecture, and supporting infrastructure.[43]

47. Within such architectures, artificial intelligence plays a critical role in enabling real-time perception and decision-making. AI-enabled systems fuse inputs from radar, electro-optical/ infrared (EO/ IR), and radio frequency (RF) sensors to detect, classify, and track airborne threats. Unlike rule-based approaches dependent on predefined signatures, AI models analyse behavioural patterns, signal characteristics, and environmental context to distinguish hostile UAVs from benign objects. This capability is particularly decisive in saturated environments,

---

[41] Joint Air Power Competence Centre, "A Comprehensive Approach to Countering Unmanned Aircraft Systems", Introduction, January 2021. https://www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/

[42] Jack Watling and Nick Reynolds, "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine".

[43] Joint Air Power Competence Centre, "A Comprehensive Approach to Countering Unmanned Aircraft Systems", Chapter 2.

where the primary challenge is not detection, but rapid and accurate discrimination under severe time constraints.[44]

48. Electronic warfare (EW) has undergone a parallel transformation. Contemporary operations demonstrate that control of the electromagnetic spectrum is central to both offensive and defensive effectiveness. In Ukraine, the extensive use of GNSS jamming, signal interception, and command-link disruption, has forced a continuous cycle of adaptation between UAV systems and countermeasures.[45] The US Department of Defence's Electromagnetic Spectrum Superiority Strategy highlights the need for systems capable of operating dynamically within congested and contested spectrum environments, emphasising adaptability, speed, and resilience.[46]

49. AI enhances EW by enabling real-time signal detection, classification, and adaptive response. Traditional EW systems, reliant on static threat libraries and pre-programmed responses, are increasingly insufficient against agile and evolving adversary systems. AI-driven EW systems, by contrast, can identify previously unseen signal patterns, adjust jamming strategies dynamically, and prioritise targets based on operational relevance. This represents a transition from scripted electronic warfare to adaptive spectrum operations.[47]

50. The interaction between AI-enabled UAVs and AI-enabled EW systems illustrates the emergence of genuine AI versus AI engagements. Autonomous drones designed to operate under GNSS denial rely on onboard perception, visual navigation, and sensor fusion to maintain mission capability even in degraded environments. In response, EW systems attempt not only to disrupt communications but also to degrade onboard sensing and navigation processes through jamming, spoofing, and signal manipulation. The result is a dynamic contest in which each side seeks to impair the other's ability to sense, interpret, and act effectively across multiple domains.

51. A convergence toward AI-enabled defensive architectures is evident across multiple military systems. Israeli counter-UAS platforms such as Drone Dome integrate radar, electro-optical sensors, and electronic warfare components to detect and neutralise UAV threats, with AI supporting target classification in complex environments.[48] Russian electronic warfare systems, including SERP-VS[49] and Strizh-3, have demonstrated the ability to disrupt UAV navigation and communication links at scale, relying increasingly on automated signal detection and prioritisation. Similarly, US Army initiatives such as the Indirect Fire Protection Capability (IFPC)[50] reflect a shift toward integrated defensive architectures in which AI-assisted systems support threat evaluation, prioritisation, and resource allocation across multiple simultaneous engagements.

---

[44] Joint Air Power Competence Centre, "A Comprehensive Approach to Countering Unmanned Aircraft Systems", Chapter 6.
[45] Jack Watling and Nick Reynolds, "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine".
[46] US Department of Defense, Electromagnetic Spectrum Superiority Strategy, October 2020. https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/electromagnetic_spectrum_superiority_strategy.pdf
[47] US DoD, Electromagnetic Spectrum Superiority Strategy.
[48] RAFAEL, "Drone Dome Family". https://www.rafael.co.il/system/drone-dome-family/
[49] Rostec Media, "Rostec is Launching the Improved SERP Anti-Drone System Version", 27 March 2025. https://www.rostec.ru/en/media/news/rostec-is-launching-the-improved-serp-anti-drone-system-version/#start
[50] United States Government Accountability Office, "Army Modernization: Air and Missile Defense Efforts Would Benefit from Applying Leading Practices", GAO-25-107491, 17 June 2025. https://files.gao.gov/reports/GAO-25-107491/index.html

52. Taken together, these developments illustrate a broader transition from platform-centric air defence to data-centric defensive ecosystems. Here, effectiveness is determined less by individual platform capabilities and more by the speed, accuracy, and resilience of decision-making processes. AI is central to this shift.

53. The emergence of autonomous interceptor systems reinforces this trend. Drone-on-drone interception concepts, including developments such as Ukrainian anti-drone interceptor platforms (Sting, Bullet, Octopus, P1-SUN)[51] rely on onboard sensing and automated tracking to detect and engage hostile UAVs. These systems employ AI for trajectory prediction, target tracking, and engagement guidance,[52] operating at speeds that effectively exceed human (or rules-based systems) reaction times. As a result, both offensive and defensive aerial engagements are increasingly conducted at machine speed, with minimal direct human intervention. The strategic value of AI-augmented systems is reflected not only in their operational performance but in the demand for the battlefield datasets they generate — data that is increasingly recognised as a critical input for training the next generation of AI models under real operational conditions, as evidenced by the opening of Ukraine's battlefield data-archives to Western AI development programmes.[53]

54. This evolution has significant implications for command and control. As engagement timelines compress, centralised decision-making becomes increasingly impractical. Instead, decision authority is distributed across platforms, with AI systems operating within predefined parameters and rules of engagement. This reflects a shift toward decentralised, machine-assisted command structures, consistent with broader developments in multi-domain operations and integrated command frameworks.[54] *At a systemic level, AI versus AI warfare is best understood as a competition between opposing decision cycles, in which each side seeks to accelerate its own OODA loop while simultaneously degrading the adversary's through disruption, deception, and data manipulation.* This includes not only physical destruction of platforms, but also the injection of false signals, exploitation of algorithmic vulnerabilities, and degradation of data integrity.

55. In such engagements, the decisive variable is not firepower alone, but latency — the speed at which a system can sense, interpret, decide, and act relative to its adversary. AI enables this compression of decision time, but also introduces new vulnerabilities, including susceptibility to adversarial inputs, data poisoning, and model exploitation.

56. In this context, the ability to design resilient, adaptive, and secure AI-enabled architectures, while degrading those of the adversary, becomes central to operational success. For States that have not yet completed this transition, the AI versus AI dimension is not a future contingency but a present operational reality — one that defines the threat environment within which their structural gaps must be understood and urgently addressed. It is against this backdrop that the following section examines ***India's strategic challenges***.

---

[51] Shola Lawal, "What are the Ukrainian drone interceptors sent to counter Iranian attacks?", ALJazeera, 10 March 2026. https://www.aljazeera.com/news/2026/3/10/what-are-the-ukrainian-drone-interceptors-sent-to-counter-iranian-attacks#:~:text=Bullet:%20Developed%20in%20late%202025,the%20Ukrainian%20defence%20company%20ODIN

[52] Olena Kryzhanivska, "Stopping Shaheds: Ukraine's Solutions", Ukraine's Arms Monitor, 19 July 2025. https://ukrainesarmsmonitor.substack.com/p/stopping-shaheds-ukraines-solutions

[53] The Hindu technology Desk, "Ukraine opens battlefield data access to allies' AI models", 18 march 2026. https://www.thehindu.com/sci-tech/technology/ukraine-opens-battlefield-data-access-to-allies-ai-models/article70737918.ece

[54] U.S. Department of Defense, "Summary of the Joint All-Domain Command and Control Strategy".

STRATEGIC IMPLICATIONS FOR INDIA

India in an AI-Driven Battlespace

57. The character of warfare across India's primary theatres, is already shifting toward persistent surveillance, contested electromagnetic conditions, and compressed decision timelines. The proliferation of low-cost unmanned systems on the western front, the People's Liberation Army's emphasis on integrated ISR, electronic warfare, and data-driven, operational architectures along the northern borders, and the scale and ambiguity of the maritime domain collectively point to a battlespace that is increasingly data-intensive, time-sensitive, and contested.[55]

58. In this context, artificial intelligence is not an enabling add-on but a structural requirement. Without AI-assisted systems for data fusion, target identification, threat prioritisation, and decision support, the gap between information availability and operational action will continue to widen. This does not merely result in inefficiency, but in a structural erosion of decision advantage in environments where adversaries are increasingly leveraging automation and machine-assisted workflows. The challenge for India, therefore, is not whether to adopt AI-enabled approaches, but how fast can it do so, and whether the institutional will exists to match this operational urgency.

Structural Lacunae

59. Despite operating in an increasingly data-centric and contested battlespace, India's current military architecture continues to function within a predominantly platform-centric construct, with insufficient integration of data, decision-making, and operational processes. This misalignment is not attributable to a lack of technological capability alone. It reflects three fundamental problems that generate a cascade of specific operational deficits. These fundamental problems, and the structural issues that emanate from them, are examined below.

60. **Fundamental Problems**.

(a) **The Network Deficit: An Incomplete Transition to Network-Centric Warfare**. *India lacks the network architecture, data standards, interoperability frameworks, and indigenous training data that are the irreducible prerequisites for AI-enabled operations. What this means is that the challenge is not the absence of AI, but the absence of the foundation on which AI depends.* In this context, the following is relevant:

(i) The most fundamental constraint India faces is not technological but infrastructural. AI needs data. Data congregation requires networks. The simple fact is that India's networks are not there yet. Each of India's defence forces continues to operate its own data links, communication architectures, and information systems, many of which are fragmented across platforms and commands. Even within individual defence forces, multiple systems coexist at varying levels of interoperability, connected through partial interfaces rather than unified architectures. The tri-service network environment that would enable

---

[55] U.S. Department of Defense, "Annual report to Congress: Military and Security Developments Involving the People's Republic of China 2025". https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF

continuous, cross-domain exchange of information at operational speed, which is the baseline-condition of network-centric warfare, has not yet been achieved.

(ii) Much of the discourse on military AI focuses on the transition from network-centric to data-centric warfare. India has not yet completed the transition to network-centric warfare itself. It is not one step behind in the evolution toward algorithmic warfare but is, in all meaningful respects, two steps behind. The distance between India's current architecture and the data-centric operational model this paper describes is correspondingly greater than it may appear, and the path to closing it is correspondingly more demanding.[56]

(iii) Compounding this network deficit is the absence of common data standards. Even where connectivity exists, data generated across the three defence forces is not consistently standardised, interoperable, or accessible within a common framework. There is no shared data ontology — no common vocabulary and taxonomy defining how entities, events, locations, and relationships are labelled consistently across the three defence forces. Without this, AI models trained on data from one defence force cannot operate effectively on data from another, and multi-source fusion produces unreliable outputs.

(iv) Finally, India lacks a structured corpus of indigenous operational training data. AI systems — whether procured or indigenously developed — require large volumes of labelled, annotated data drawn from the specific terrain, threat environment, and sensor characteristics of the operational context in which they will be deployed. A model trained on imagery from European or Middle Eastern environments will not automatically perform reliably in the Thar Desert, the Himalayan frontier, or the littoral environments of the Indian Ocean Region. No systematic programme currently exists to build this corpus. This, in turn, means that every AI system that India fields will be operating with a foundational handicap. This must be addressed as a matter of the utmost priority.

(b) **The Institutional Culture: A Platform-Centric Legacy**. *Decades of service-centric acquisition, parallel development of incompatible systems, and the organisation of doctrine, command structures, and budgetary priorities around platforms rather than networks have produced an institutional culture that is structurally resistant to the data-driven integration that AI-enabled warfare requires.* The data deficit described above is not primarily a technical failure. Rather, it is the product of an institutional culture that has consistently prioritised platforms over networks and individual service requirements over joint interoperability. Acquisition-decisions have been made individually by each of the three defence forces, producing capable individual platforms that are, nevertheless, poorly connected to each other. Command structures have been organised around hierarchical, centralised decision-making that made sense in a platform-centric world but introduces critical latency in environments where decision cycles are measured in fractions of seconds. Doctrinal development has certainly not kept pace with the operational implications of networked and data-driven warfare. The result is an architecture in which the components exist, but the integration does not; one in which the institutional incentives that perpetuate this grossly sub-optimal condition remain largely intact. Overcoming this cultural inertia is as important as any specific

[56] Lt Gen A B Shivane PVSM, AVSM, VSM, "Networked Indian Army for Winning Edge", Defence and research Studies, 10 January 2026. https://dras.in/networked-indian-army-for-winning-edge/

technical investment, because even the most sophisticated AI systems will underperform in an institutional environment that is not organised to exploit them.

(c) **The Governance Gap: Building Responsibly While Building Urgently**. *As AI capabilities are developed and integrated, India will need governance and validation frameworks to ensure they are deployed safely and accountably. It is obvious that these should be built in parallel with capability development and not as a precondition that delays the latter.* The integration of AI into ISR, targeting, and command workflows will inevitably raise questions about how system performance is validated and how legal compliance is assured. India does not yet have a dedicated AI testing and certification capability, nor an established framework for ensuring that AI-assisted targeting workflows comply with the requirements of the Law of Armed Conflict. These are real gaps that will need to be addressed — particularly as international scrutiny of autonomous and AI-assisted weapons systems intensifies. However, the absence of fully mature governance frameworks should not be treated as a reason to delay capability-development. A more productive framing is that governance and capability must be built concurrently — with legal validation layers, human oversight mechanisms, and accountability frameworks, all embedded into systems as they are developed rather than being retrofitted after deployment. This is both, more responsible and more practical. It is significantly easier to build a lawfulness-filter into a target nomination system at the design stage than to add it to an operationally deployed system under time and resource pressure. The goal is not to allow governance to slow capability. It is to ensure that the capability India builds is one that it can deploy with confidence, sustain under scrutiny, and defend both operationally and legally.

61. **Structural Issues**. *The three fundamental problems identified above generate six specific structural deficits that manifest themselves across India's operational architecture. These are not independent problems, but emanations of the deeper institutional and infrastructural constraints described above - and they will not be resolved by addressing them individually without simultaneously tackling the root causes from which they derive. These structural deficits are: -*

(a) **Fragmented ISR Architecture**. India generates significant ISR data across satellites, unmanned systems, ground sensors, and signal intelligence assets. However, this data remains siloed across services and agencies with limited real-time fusion. The result is an ISR architecture that generates data it cannot fully exploit — the collection-exploitation gap that this paper has identified as the central ISR challenge manifesting itself most strikingly in India's specific institutional and technical context.[57]

(b) **Limited AI-enabled Targeting and TERA Capability**. Targeting processes remain reliant on human-driven, rule-based workflows operating on predefined signatures and deterministic logic. Systems such as naval Combat Management Systems (CMS), *Akashteer*, and the IACCS, provide structured engagement frameworks but are not adaptive to the ambiguity and volume of contemporary threat environments. Critically, there is no AI-assisted target nomination capability and no institutionalised lawfulness filter embedded in targeting workflows.

---

[57] Brig Ashis Bhattacharya (Retd), "Integrating ISR and Degradation into India's Theatre Command Model: A Warfighting Imperative", DEFSTRAT - Vol 19 Issue 1 Mar – Apr 2025, 15 April 2025. https://www.defstrat.com/magazine_articles/integrating-isr-and-degradation-into-indias-theatre-command-model-a-warfighting-imperative/#:~:text=A%20theatre%20commander%20requires%20real,Incremental%20Change%20to%20Transformational%20change

(c) **Weak Assured Positioning, Navigation, and Timing**. India's dependence on foreign GNSS, compounded by the ongoing degradation of NavIC due to atomic clock failures,[58] creates a critical vulnerability in contested electromagnetic environments.[59] Alternative navigation techniques — visual, terrain-relative, multi-sensor fusion — remain underdeveloped or insufficiently integrated into operational platforms. This is both a platform-centric acquisition failure — each programme solving its navigation problem independently — and a data deficit, as resilient navigation depends on the same sensor fusion and AI-assisted processing capabilities that the broader data architecture lacks.

(d) **Disaggregated Counter-UAS and Electronic Warfare Capability**. Counter-UAS and electronic warfare systems remain platform-centric and non-interoperable, with detection, classification, and response mechanisms operating independently rather than through shared decision logic. This creates exploitable gaps in coverage that are particularly acute in high-density drone environments where the challenge is swarm-management rather than individual platform-engagement[60] — a direct consequence of the platform-centric culture that has produced parallel, incompatible capability development across the defence forces.

(e) **Centralised and Sequential Command Structures**. India's command architecture introduces decision latency that becomes operationally critical as adversaries compress their own cycles through automation. The absence of distributed decision authority and machine-assisted decision-support means that the cognitive burden on human commanders increases precisely as time available decreases — a structural mismatch that is both a cultural legacy of platform-centric, hierarchical organisation and a technical consequence of the absent data architecture that would enable trusted AI-assisted decision support.

(f) **Absence of Indigenous Operational Training Data**. No systematic programme exists to extract, annotate, and label the operational data generated by India's existing ISR platforms into a structured training corpus. This means every AI system India procures or develops will be trained on foreign operational data — a foundational handicap that cannot be corrected after deployment and that must be addressed as a prerequisite to the entire AI capability development programme.

Operational Risks

62. The structural gaps identified above do not exist in a static environment. They are widening relative to two adversaries who are accelerating in the opposite direction — one that has already embedded AI-enabled warfare into its core operational doctrine, and another that increasingly operates as a forward node of that system. China's People's Liberation Army (PLA) has moved beyond experimentation, framing future operations explicitly around "intelligentized warfare" involving the integration of AI, big data, and autonomous systems into a "network

---

[58] Jacob Koshy, "Failure of atomic clock cripples ISRO's NavIC system", The Hindu, 15 March 2026. https://www.thehindu.com/sci-tech/science/isro-navic-system-atomic-clock-failure/article70743233.ece

[59] Defense Systems Information Analysis Center, "Assured Positioning, Navigation, and Timing (APNT)", Report Number: DSIAC-BCO-2021-163, January 2021. https://dsiac.dtic.mil/wp-content/uploads/2021/06/TI-Response-Report_DSIAC_Assured-Positioning-Navigation-and-Timing-APNT_1162023-1.pdf

[60] Akshat Upadhyay, "Counter UAS Technologies for India A Prognosis", Manohar Parrikar Institute for Defence Studies and Analyses, Journal of Defence Studies, Vol. 16, No. 4, October–December 2022, pp. 181–202. https://idsa.in/system/files/jds/jds-16-4_Akshat-Upadhyay_11.pdf

information system-of-systems" designed to rapidly identify adversary vulnerabilities and execute precision strikes across domains.[61] A February 2026 CSET analysis of thousands of PLA procurement requests confirmed that the PLA is actively acquiring AI decision-support systems, sensor enhancement tools, and data fusion algorithms across all operational domains, with acquisition timelines of as little as three to six months per system.[62] Pakistan, for its part, may not independently match the depth of China's technological ecosystem, but it increasingly operates as a forward node within it — with access to real-time AI-generated ISR, targeting, and electronic warfare outputs from Chinese systems, and potentially from Turkish platforms as well. The asymmetry that India faces is, therefore, not simply bilateral — it is structural, compounding, and already in motion. The risks that follow are operational consequences that are beginning to become evident.

63. **Decision Paralysis in High-Tempo Engagements**. *India's incomplete network architecture, centralised command structures, and GNSS dependence combine to create a decision cycle that is structurally slower than those of both its primary adversaries, with consequences that are most acute in missile defence, counter-UAS, and electronic warfare scenarios on both fronts.*

(a) Against China on the northern front, the decision-paralysis risk is most acute in the electromagnetic domain. The PLA has invested heavily in integrated electronic warfare and GNSS jamming capabilities specifically designed to degrade adversary navigation, communication, and ISR systems as a precursor to kinetic operations. Consider what happens when the PLA jams GPS along the LAC and India's platforms and surveillance assets, in the absence of alternative navigation capabilities, go blind at the moment when decision speed is most critical. The centralised command structures that characterise India's current architecture introduce additional latency. In a scenario where PLA systems are generating targeting outputs and engagement decisions at 'machine speed, India's human-driven decision loops, routing information upward through command chains before action can be authorised, risk being structurally outpaced before a single engagement has been completed.

(b) Against Pakistan on the Western Front, the risk manifests itself differently but is no less significant. Pakistan has been systematically deepening its integration within Chinese defence technology ecosystems - acquiring AI-assisted early warning platforms, electronic warfare systems, and precision strike architectures of Chinese origin, and establishing dedicated institutions such as the Centre for Artificial Intelligence and Computing (CENTAIC) within the Pakistan Air Force, focused on automating threat recognition, data fusion, and cognitive electronic warfare.[63] While confirmed evidence of shared real-time operational data links between Chinese and Pakistani systems does not yet exist, the trajectory of this integration - in terms of platform commonality, technology transfer, and doctrinal alignment - means that the decision-cycle disadvantage India faces on the northern front cannot be assumed to remain confined there. India, facing this composite threat architecture on the Western Front, cannot calibrate its response on the

---

[61] U.S. Department of Defense, "Annual report to Congress: Military and Security Developments Involving the People's Republic of China 2025". https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF

[62] Emelia Probasco, Sam Bresnick, and Cole McFaul, "China's Military AI Wish List: Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance, and Targeting (C5ISRT)", Center for Security and Emerging Technology (CSET), February 2026. https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-Military-AI-Wish-List.pdf

[63] Bilal Khan, "Next Generation Air Warfare in South Asia: Risks and Way Forward", South Asian Voices, Stimson Center, 02 January 2026. https://southasianvoices.org/sec-m-pk-r-next-gen-air-warfare-in-south-asia-1-1-2026/

assumption that Pakistani capability reflects only what Pakistan has indigenously developed. The combined weight of Chinese platform transfers, AI-assisted system architectures, and potentially Turkish unmanned systems experience represents a technology ceiling for Pakistani capability that is substantially higher than its organic development base would suggest — and one that is rising.

64. **ISR Saturation Without Exploitation**. *India's sensors will generate more data in a future high-intensity conflict than its manual analysis workflows can process, producing a paradox in which information abundance coexists with operational blindness, while adversaries operating AI-assisted ISR exploitation translate the same contested battlespace into actionable targeting.*

(a) The PLA's ISR architecture is explicitly designed to exploit precisely this asymmetry. Norinco's Intelligent Precision Strike System — demonstrated at the 2024 Zhuhai Airshow — autonomously fuses battlefield intelligence from multiple sources, models the operational environment in real time, and distributes targeting information for execution, with human authorisation required only at the point of firing.[64] This is not a developmental concept. It is a fielded capability that the PLA Information Support Force is integrating into its dynamic kill network architecture across domains. Against an adversary operating at this level of ISR exploitation, India's current model is not just slower, it is structurally incapable of generating the same quality of operational picture from the same data.

(b) The consequence, in a high-intensity scenario, is asymmetric situational awareness. Both sides operate sensors. Both sides generate data. But only one side converts that data into a continuously updated, AI-assisted common operational picture that links detection to targeting to engagement in a coherent pipeline. India thus faces a condition this paper has described as "data saturation without exploitation". In the Himalayan theatre, where terrain complexity, communication constraints, and the compressed geography of forward deployments already limit the decision space, this asymmetry is particularly acute. A PLA that can see the battlespace more completely and act upon it faster holds a structural advantage that platform quality alone cannot offset. For Pakistan, access to Chinese ISR outputs effectively extends this asymmetry to the Western Front.

65. **Asymmetric Escalation from Targeting Failures**. *The absence of AI-assisted validation, pattern analysis, and legal filtering in India's targeting workflows, combined with the extreme time pressure and fog of war that characterise high-tempo operations, creates conditions in which rule-based or manual targeting systems may produce unintended consequences with strategic implications disproportionate to their tactical origin.* Under conditions of extreme time pressure, degraded communications, electronic warfare-induced uncertainty, and simultaneous multi-domain threats, rule-based and manual targeting systems face a specific and dangerous failure mode: they must make decisions at a pace and volume that exceeds their design parameters, producing outputs that are locally plausible but operationally or legally flawed. A misclassified target, a pattern-of-life assessment that conflates civilian and military activity in a complex environment, or a prioritisation decision made on incomplete and rapidly changing information can generate escalatory consequences that political

---

[64] Tye Graham and Peter W. Singer, "New Products Show China's Quest to Automate Battle", Defense One, March 2, 2025. https://www.defenseone.com/threats/2025/03/new-products-show-chinas-quest-automate-battle/403387/

leadership cannot easily contain. The absence of Ai enabled systems does not merely create operational inefficiency - it creates the conditions under which tactically explicable but strategically damaging decisions are made, not through intent, but through the structural inability of conventional systems to cope with the demands placed upon them.

RECOMMENDATIONS: A DUAL-TRACK, PHASED ACTION PLAN

66. If the risks identified above are structural, the response must move beyond linear, top-down transformation models. The transition from current architectures to fully integrated, data-centric operations is inherently complex and cannot be executed as a single, sequential programme. Attempting to build comprehensive networked and data architectures before demonstrating operational value risks delay, institutional resistance, and fragmentation of effort.

67. A more effective approach lies in adopting a dual-track strategy. India must simultaneously pursue (i) localised, application-specific AI deployments that deliver immediate operational value, and (ii) the gradual construction of a unified data and network architecture that enables long-term transformation. Since AI systems derive effectiveness from the quality of data, workflows, and integration environments in which they operate,[65] the objective is not incrementalism, but structured acceleration, ensuring that near-term deployments are deliberately designed to feed into a scalable, integrated system.

Short-Term Priorities: Operational Gains with Foundational Alignment

68. In the immediate term, India should prioritise four high-impact, operationally bounded AI applications in clearly defined contexts where decision timelines are already compressed and data volumes are high. These deployments are not ends in themselves. Each must be designed with forward compatibility in mind, adhering to common data formats, metadata standards, and interface protocols so that they feed into the integrated architecture that the medium and long-term phases require.

69. **Border UAV Threat Fusion**. *Integrating existing sensor feeds into an AI-assisted classification system to enable faster and more accurate detection of unmanned aerial threats in forward areas.* In practice, feeds from existing battlefield surveillance radars, ground-based RF detection equipment, and forward-deployed EO/ IR cameras should be integrated into a single AI-assisted classification console at corps-level air defence operations rooms. The AI layer should perform three specific functions: automatically classify detected low-altitude objects — fixed-wing UAV, rotary UAV, bird, or unknown — within 8 seconds of detection; generate a threat confidence score with supporting sensor evidence displayed to the operator; and alert the operator only when confidence exceeds a defined threshold, reducing nuisance alerts and operator fatigue. The architecture should be open and modular, permitting iterative model retraining as new threat signatures emerge from operational experience.

70. **AI-Assisted ISR Exploitation**. *Applying AI-assisted analytics to footage from existing UAV fleets to transform ISR from a collection function into an exploitation function.* Rather than waiting for new platforms, AI-assisted video analytics should be applied to footage from the Heron and Searcher Mk-II fleets currently operated by the Army and Air Force. The tool should automatically flag frames containing vehicle concentrations above a defined threshold, changes in previously

[65] U.S. Department of Defense, "Summary of the 2018 DoD Artificial Intelligence Strategy, 2019".

surveilled infrastructure, and human activity patterns inconsistent with established pattern-of-life baselines. Flagged footage should be time-stamped, geotagged, and routed to analysts as prioritised clips rather than raw feeds, eliminating the current practice of analysts reviewing hours of footage manually.

71. **AI-Assisted Maritime Domain Awareness**. *Augmenting the existing maritime situational picture with behavioural analytics to enable proactive identification of vessels of interest in the Indian Ocean Region.* The existing Automatic Identification System (AIS) and sensor (radar, EO/ IR etc.) picture at the Information Management and Analysis Centre (IMAC), Gurugram, should be augmented with a behavioural analytics layer that automatically flags vessels exhibiting AIS spoofing or signal gaps exceeding defined parameters, loitering within specified maritime zones, and movement patterns correlated with previously identified vessels of interest. The system should generate a dynamic watchlist (AI generated and updated, not merely rule -based) of flagged contacts, ranked by anomaly score, for operator review.

72. **AI-Assisted Target Nomination**. *Developing and validating a prototype target nomination system in a controlled environment, with mandatory human oversight and legal compliance built into its architecture.* An AI-assisted target nomination prototype should be developed and validated in a controlled, non-operational environment before any operational integration is considered. The system should ingest multi-source inputs such as UAV imagery, SIGINT-correlated location data, pattern-of-life tracks, and ground sensor feeds, correlating them against a target database to generate ranked candidate nominations, each accompanied by a confidence score, contributing evidence, and a plain-language summary. Critically, a lawfulness filter, developed in consultation with the Judge Advocate General's Branch and screening every nomination against distinction, proportionality, and precaution criteria, must be an integral architectural component. Every nomination, its evidence basis, and the operator's decision must be logged in a tamper-proof audit trail to support both operational learning and post-engagement accountability. Validation should proceed in three stages: first against historical exercise datasets where ground truth is known; second in a live simulation environment under realistic time pressure; and third through a structured red team and independent legal assessment, stress-testing high-confidence nominations where underlying data is ambiguous. Operational deployment, even in limited form, should follow only upon successful completion of all three stages.

73. **Foundational Data Infrastructure**. *Building a structured, labelled dataset from existing ISR archives to underpin all current and future AI model development in Indian operational conditions.* DRDO's Centre for Artificial Intelligence and Robotics (CAIR), working with the intelligence directorates of the three services, should be tasked — with a deadline of 12 to 18 months —- to extract, annotate, and label a structured dataset from existing ISR archives, including a minimum of 500 hours of UAV footage, 12 months of IMAC maritime contact data, and six months of SIGINT-correlated geospatial tracks, tagged with environmental conditions, sensor parameters, and ground-truth outcomes where available. This dataset is the foundational asset upon which all subsequent AI model development depends. Without it, every system India procures or develops will be trained on foreign operational data and will perform sub optimally in Indian terrain, weather, and threat conditions. Common time-stamping and geospatial referencing standards must be established across all contributing systems from the outset.[66] In parallel, given the ongoing degradation of NavIC due to atomic clock failures, India should, within 12 months, establish a ground-based augmentation programme to compensate for current coverage gaps, coordinating between ISRO, the Department of Space, and the Ministry of Defence to ensure

[66] NATO, "Data Quality Framework for the Alliance", 29 August 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/08/29/data-quality-framework-for-the-alliance

that defence-critical positioning requirements are met through augmented and alternative sources while next-generation NavIC satellites with redundant clock architectures are developed.[67]

74. **AI Integration Cells**. *Establishing joint operational-technical cells within individual defence headquarters to embed AI as a core component of capability development rather than a peripheral technology initiative.* AI Integration Cells (AIICs) should be established within each of the three defence-headquarters and within HQ Integrated Defence Staff, within 12 months. Each cell should comprise AI and machine learning technical specialists drawn from DRDO, CDAC, and high-competence private sector organisations (including defence-focused startups), operational analysts with recent field experience, and a legal officer familiar with targeting laws and rules of engagement. Actively incorporating private sector and startup talent is not merely desirable but necessary. This is because several of India's most capable AI expertise in computer vision, sensor fusion, and anomaly detection, currently resides outside the public sector, and the AIICs should be structured to access it through defined secondment, contract, and partnership mechanisms. These cells should have direct access to operational commanders and a mandate to translate field requirements into deployable solutions within defined iteration cycles, ensuring that AI is embedded as a core component of operational planning rather than treated as a peripheral technology initiative. As these cells begin generating operational experience with AI-assisted systems, a parallel process of foundational revision of extant rules of engagement should commence, focused narrowly on defining the conditions under which AI-assisted outputs may inform operational decisions, and the human review requirements that apply at each stage. This is not the comprehensive doctrinal overhaul that mature AI integration will eventually require. It is the minimum legal and command framework without which responsible short-term deployment cannot proceed.

Medium-Term Priorities: Convergence into Integrated Architectures

75. *As initial short-term deployments mature and begin generating operational data and institutional learning, the focus should shift from localised applications to integration and convergence. The key requirement in this phase is the development of a coherent, AI-assisted ISR and targeting pipeline and the progressive integration of threat evaluation, electronic warfare, counter-UAS, and command systems into a unified data-driven architecture. Critically, the short-term deployments should not be treated as standalone systems but as the first components of this larger architecture, designed from the outset to plug into it.*

76. **AI-Assisted ISR and Targeting Pipeline**. *Building an integrated, multi-source ISR exploitation system that connects sensing, analysis, target nomination, and threat evaluation into a continuous operational pipeline.* The AI-assisted ISR and targeting pipeline is the medium-term's central capability requirement - the functional equivalent, in Indian operational terms, of what Project *Maven* has become for US Central Command. It should be built by progressively integrating the short-term deployments — the Border UAV Threat Fusion Node, the ISR Exploitation tool, and the IMAC Maritime Watchlist — into a common data ingestion and processing layer, rather than building from scratch. Specifically, the pipeline should achieve five sequential functions: ingestion and normalisation of multi-source data from UAVs, satellites, radars, SIGINT assets, and maritime sensors into a common format; AI-assisted fusion of these inputs into a continuously updated common operational picture; automated detection, classification, and pattern-of-life analysis generating flagged entities of interest; target nomination and filtering, with the lawfulness filter developed in the short-term prototype applied as a mandatory layer; and linkage to the TERA module for prioritisation and resource allocation recommendations. Each stage should have a defined human review point, and the pipeline should be designed so that the

[67] Jacob Koshy, "Failure of atomic clock cripples ISRO's NavIC system".

depth of human scrutiny scales inversely with time available, with more deliberate reviews in planned operations, and faster operator-assisted processing in time-critical scenarios. The DRDO, working with the three defence force intelligence directorates and private sector AI partners under the iDEX framework, should be the primary development authority, with HQ Integrated Defence Staff providing architectural oversight and interoperability standards.

77. **Threat Evaluation and Resource Allocation Module**. *Developing an AI-assisted TERA capability that translates ISR pipeline outputs into prioritised, time-sensitive response recommendations while preserving meaningful human decision authority.* The TERA module should be built as a direct downstream extension of the ISR and targeting pipeline, receiving its nominated entities of interest as inputs and generating prioritised response recommendations as outputs. It should perform three specific functions: (1) dynamic threat prioritisation, ranking detected threats by assessed severity, imminence, and mission relevance using a continuously updated weightage-model that can be adjusted by commanders based on operational context; (2) resource matching, recommending the optimal allocation of available kinetic, electronic warfare, and cyber response options against prioritised threats; and (3) escalation flagging, automatically identifying scenarios where the threat picture exceeds predefined thresholds and routing these to higher command levels with supporting evidence. A human-in-the-loop validation layer must be integral to the architecture at the prioritisation and resource matching stages, rather than being added as an afterthought. The system should present its recommendations with explicit confidence levels, contributing evidence, and alternative courses of action, so that commanders are making informed decisions rather than simply ratifying machine outputs. Particular attention should be paid to the interface design: recommendation displays should be structured to promote critical engagement rather than passive acceptance, directly countering the automation bias risk the paper has identified.

78. **Assured Positioning, Navigation, and Timing (PNT) Architecture**. *Building resilient, multi-source navigation capability that reduces dependence on GNSS and sustains operational effectiveness in contested electromagnetic environments.* The assured PNT vulnerability identified in the structural lacunae — GPS dependence compounded by NavIC degradation — cannot be addressed through platform-by-platform workarounds. What is required is a systematic, multi-source navigation framework that reduces GNSS dependence across all operational platforms simultaneously. The objective is not to replace GNSS but to reduce dependence on it by developing and integrating alternative navigation methods into operational platforms. Specifically, this requires: (1) the integration of inertial navigation systems with visual-inertial odometry, terrain-relative navigation, and LiDAR or radar odometry into a sensor fusion framework for autonomous and semi-autonomous platforms; (2) the development of AI-assisted spoofing detection capable of identifying GNSS signal manipulation in real time and automatically switching to alternative navigation sources; and (3) the establishment of a signals-of-opportunity navigation capability that exploits non-GNSS signals — including terrestrial broadcast, cellular, and other ambient electromagnetic sources — as positioning inputs in GNSS-denied environments. DRDO's navigation systems cluster, working with the Indian Space Research Organisation and private sector navigation technology firms, should be tasked to develop a modular, platform-agnostic assured PNT framework that can be integrated across UAV, missile, and manned platform programmes rather than developed separately for each.[68] The NavIC degradation issue must be treated as an urgent remediation priority in parallel, given its implications for both civil and military navigation infrastructure.

79. **Integrated Counter-UAS and Electronic Warfare Architecture**. India's current counter-UAS and electronic warfare capabilities are effective against isolated threats but are

[68] DSIAC, "Assured Positioning, Navigation and Timing (APNT) Overview".

structurally unsuited to high-density, multi-domain engagements. The medium-term objective is to integrate these into a layered, AI-assisted defensive architecture in which detection, classification, prioritisation, and response are connected through shared decision logic rather than operated independently. Specifically, radar detection, RF sensing, EO/IR tracking, and jamming response systems should be linked through a common threat-management layer that: (1) automatically correlates inputs from multiple sensors to generate composite tracks of airborne threats; (2) classifies threats by type, trajectory, and assessed intent using AI models trained on Indian operational environment-data generated in the short-term foundational dataset phase; (3) dynamically prioritises threats based on collective behaviour, identifying swarm dynamics and coordinated attack patterns, rather than treating each platform as an isolated contact; and (4) recommends and, within defined parameters, initiates electronic warfare responses — jamming, spoofing, command-link disruption — while alerting operators to engagements in progress. The Indian Army's *Akashteer* and the Air Force's IACCS should serve as the command-and-control backbone for this integration, with AI-assisted threat-management layers added progressively rather than requiring wholesale replacement of existing systems. Engagements that exceed defined parameters, such as large swarm-volumes, threats to critical national infrastructure, or scenarios requiring kinetic response, should automatically escalate to human decision authority.

80. **Distributed Machine-Assisted Command and Control** *Progressively shifting command workflows toward distributed, machine-assisted decision-making in defined operational sectors, reducing the centralisation-induced latency that disadvantages Indian forces in high-tempo engagements.* India's centralised command structures introduce decision latency that becomes operationally critical as engagement timelines compress. The medium-term objective is not to replace centralised command but to selectively distribute decision authority to lower echelons in specific, well-defined operational contexts where AI-assisted decision support can be validated and trusted. This should begin in two bounded domains. The first is in terms of counter-UAS engagements in forward areas, where the threat parameters are relatively well-defined and the consequences of autonomous or semi-autonomous response can be bounded by clear rules of engagement. The second concerns maritime situational/ domain awareness responses, where the IMAC's AI-assisted watchlist can be extended to recommend and, within defined parameters, initiate surveillance and tracking responses without requiring centralised authorisation for each contact. In both cases, the AI system should operate within a defined decision envelope — a set of pre-authorised response options that commanders have approved in advance — with automatic escalation outside that envelope. This approach preserves command authority while eliminating the latency introduced by routeing routine decisions through centralised structures. As confidence in AI-assisted outputs grows through operational experience, the decision envelope can be progressively expanded, moving toward the distributed, machine-assisted command architecture that modern high-tempo operations require.[69]

Long-Term Priorities: Structural and Doctrinal Transformation

81. *The long-term phase represents the culmination of the dual-track strategy, which is the point at which localised short-term deployments and the integrated medium-term architectures converge into a unified, continuously learning operational ecosystem. The objective is not the adoption of individual AI capabilities but the structural transformation of how India's defence forces sense, decide, and act. This phase is as much institutional and doctrinal as it is technological. The systems built in earlier phases will deliver their full potential only if the organisations, processes, and frameworks that govern their use are transformed in parallel.*

[69] Joint Chiefs of Staff, "Joint All-Domain Command and Control Strategy, 2022".

82. **Unified Defence Data Architecture**. *Establishing a tri-service data backbone that enables real-time, standards-compliant sharing of operational data across all domains and commands - the foundational infrastructure upon which all AI-enabled operations depend.* The unified defence data architecture is the most critical and most demanding requirement of the long-term phase. It is the layer that transforms the individual pipelines and integrated architectures built in earlier phases from a collection of connected systems into a genuinely unified operational ecosystem. Specifically, it should comprise four components. The first is a tri-service data backbone — a secure, high-bandwidth network layer enabling real-time data exchange across Army, Navy, and Air Force systems, theatre commands, and national intelligence agencies, built on common protocols and interoperability standards, which are compatible with India's key defence partners. The second is a common data ontology — a shared vocabulary and taxonomy for operational data, defining how entities, events, locations, and relationships are labelled and described consistently across all contributing systems, so that AI models trained on data from one service can operate effectively on data from another. The third is a federated data lake architecture — centralised enough to enable cross-domain fusion and AI model training, but sufficiently distributed to preserve operational security, redundancy, and resilience against single points of failure or cyber-attack. The fourth and final one is a continuous data quality assurance mechanism — automated tools that monitor incoming data streams for completeness, accuracy, consistency, and timeliness, flagging degraded inputs before they propagate errors into AI model outputs. HQ Integrated Defence Staff should own the architecture standard, with each defence force responsible for compliance within its own systems and the Defence Cyber Agency responsible for security architecture and resilience.

83. **Fully Integrated Operational Ecosystem**. *Connecting ISR, targeting, air defence, electronic warfare, cyber, and maritime systems into a common operational framework capable of supporting multi-domain operations at machine speed.* The fully integrated operational ecosystem is the operational expression of the unified data architecture — the point at which the individual capabilities developed in earlier phases function as components of a single, coherent system rather than as separate programmes. Specifically, this requires the integration of six functional domains into a common framework: (1) ISR and targeting pipelines feeding a continuously updated common operational picture; (2) AI-assisted TERA modules linked to all service command systems; (3) counter-UAS and electronic warfare architectures operating within shared threat-management logic; (4) cyber operations integrated as a response option within the TERA framework alongside kinetic and electronic warfare options; (5) maritime domain awareness connected to both the ISR pipeline and naval command systems; and (6) space-based ISR and positioning assets integrated as primary inputs rather than supplementary feeds. Integration should be achieved progressively, connecting existing systems through common interfaces rather than replacing them, with HQ IDS maintaining architectural oversight and each theatre command responsible for operational integration within its area of responsibility.[70] The system should be designed from the outset for scalability, so that new platforms, sensors, and AI models can be added without requiring architectural redesign.

84. **Scalable, Continuously Learning AI Systems**. *Developing AI models that improve through operational experience, incorporating feedback from real engagements to progressively enhance performance in Indian operational conditions.* The AI systems deployed in earlier phases will, at the point of initial deployment, be trained on historical data and validated in simulation. Their long-term operational value depends on their ability to learn continuously from real operational experience, updating their models as new threat signatures, environmental conditions, and adversary behaviours emerge. This requires three specific capabilities. First, a federated learning architecture that allows AI models to be updated from operational data generated across multiple

[70] U.S. Department of Defense, "Summary of the Joint All-Domain Command and Control Strategy".

commands and platforms without requiring that data to leave its originating system, preserving operational security while enabling model improvement. Second, a structured operational feedback loop in which operator decisions — approvals, rejections, and modifications of AI recommendations — are automatically captured, labelled, and fed back into model retraining cycles, so that the system learns from human judgment rather than operating independently of it.[71] Third, a Red Team and adversarial testing programme that continuously probes deployed AI systems for vulnerabilities, including data poisoning, adversarial inputs, and model exploitation, and incorporates the findings into model updates. DRDO's CAIR, working with private sector AI partners, should maintain primary responsibility for model development and retraining, with the AIICs established in the short-term phase providing the operational feedback interface.

85. **Data Governance, AI Testing and Certification Framework**. *Establishing enduring institutional structures to govern data quality, validate AI system performance, and certify systems for operational use - ensuring that AI is integrated responsibly and accountably.* As AI becomes embedded in operational decision-making, the institutions governing its development and use become as important as the technology itself. Three enduring structures are required. First, a Defence Data Governance Authority - a tri-service body with statutory authority to set and enforce data standards, resolve interoperability disputes between services, and oversee data quality across the unified architecture, publishing binding standards and conducting regular compliance audits. Second, an AI Testing and Certification Centre - a dedicated facility ideally co-located with an existing DRDO establishment, responsible for the independent testing, validation, and certification of all AI systems before operational deployment, maintaining standard test datasets, simulation environments, and red team capability, and issuing formal operational clearances specifying the conditions under which a given system is certified for use. No AI system should be operationally deployed without such clearance.[72] Third, a Standing Committee on AI in Warfare - a joint body comprising operational commanders, legal officers, technical specialists, and where appropriate external academic and civil society expertise - responsible for continuous doctrinal adaptation, reviewing rules of engagement governing AI-assisted systems, and advising the Chief of Defence Staff on emerging risks and required policy responses.[73]

86. **Doctrinal Transformation and Human Oversight Framework**. *Ensuring that India's military doctrine, rules of engagement, and accountability frameworks keep pace with the capabilities being deployed - preserving meaningful human control as AI becomes progressively embedded in operational decision-making.* Doctrinal transformation is the dimension most frequently acknowledged and least specifically addressed in AI and warfare discourse. For India, it requires three concrete actions. First, the existing joint doctrine on command and control, targeting, and rules of engagement must be comprehensively reviewed and rewritten to reflect the specific characteristics of AI-assisted operations - defining precisely what constitutes meaningful human oversight at each stage of the targeting process, what decision authorities can be delegated to AI-assisted systems under what conditions, and what accountability mechanisms apply when AI-assisted decisions result in unintended outcomes.[74] This review should be led by the Headquarters Integrated Defence Staff in consultation with the JAG branch and should result in binding doctrinal publications within a defined timeframe. Second, professional military education at all levels - from the Defence Services Staff College to the National Defence College - must be updated to develop commanders who understand AI capabilities and limitations, can critically evaluate AI-generated recommendations, and are equipped to exercise meaningful oversight rather than

---

[71] Probasco et al., "AI for Military Decision-Making".
[72] NATO, "Summary of NATO's Revised Artificial Intelligence Strategy, 2024".
[73] International Committee of the Red Cross, "Autonomous Weapon Systems and International Humanitarian Law: Selected Issues", October 2025. https://www.icrc.org/sites/default/files/media_file/2025-10/ICRC-Position_Paper-Autonomous_Weapon_Systems_and_IHL-Selected_issues_Oct2025.pdf
[74] U.S. Department of Defense, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy".

defaulting to automation. This is not a technical education requirement but a command education requirement: the goal is commanders who can ask the right questions of AI systems, not commanders who can build them. Third, India should actively engage in the development of international norms and frameworks governing autonomous weapons and AI-assisted targeting - both to shape emerging standards in ways consistent with its strategic interests and to ensure that its own developing capabilities are designed with those standards in mind from the outset, rather than requiring costly retrofitting later.[75]

Conclusion

87. India's challenge in the emerging battlespace is not the absence of platforms, sensors, or isolated technological capabilities. It is the inability, at present, to integrate these into a coherent system that can sense, interpret, decide, and act at the speed demanded by modern conflict. This paper has argued that this inability is not primarily technological in origin - it is structural, rooted in an incomplete transition to network-centric warfare, a platform-centric institutional culture that has consistently prioritised individual capability over integrated architecture, and the absence of the governance frameworks required to deploy AI responsibly at scale. India is not one step behind in the transition to algorithmic warfare. In meaningful respects, it is two steps behind - and the distance between its current architecture and the data-centric operational model that its adversaries are already implementing is correspondingly greater than it may appear.

88. The risks arising from this gap are not theoretical. They are already visible in the asymmetric decision cycles that characterise India's primary threat environments - a People's Liberation Army that has moved beyond experimentation into the operational integration of intelligentised warfare, and a Pakistan that increasingly draws on Chinese AI-assisted platforms and architectures that exceed its organic capability. In such an environment, delay is not inconsequential. It compounds disadvantage at precisely the rate at which adversaries accelerate. Every month India does not move is a month China and Pakistan do.

89. India's response must be both immediate and sustained - and these imperatives are not in contradiction with each other but mutually reinforcing. Operationally bounded AI deployments must proceed now, designed from the outset as the first components of the larger integrated architecture that medium and long-term transformation requires. The objective is not to match individual technologies but to build a coherent operational system in which sensing, understanding, deciding, and acting are connected at machine speed across all domains.

90. Ultimately, the question is not whether India will adopt artificial intelligence in warfare - that question has already been answered by the character of the battlespace it faces. The question is whether it can do so with the structural coherence, institutional urgency, and governing frameworks that effective and responsible AI-enabled warfare demands. In a competition defined by speed, integration, and data, that ability is not one advantage among many. It is the decisive one.

---

[75] UN General Assembly Resolution 79/62, "Lethal Autonomous Weapons Systems", 2 December 2024. https://digitallibrary.un.org/record/4068497