



Battlefield of the future

How AI is transforming warfare



October 2026

kpmg.com/in

KPMG. Make the Difference.

Foreword

India stands at an inflection point in its national development journey. The vision of Agrabharat is not only about economic growth, technological leadership, and global influence, but also about building the capabilities required to safeguard and sustain that progress in an increasingly uncertain world. As geopolitical competition intensifies and technologies evolve at an unprecedented pace, national security and technological self-reliance have become deeply interconnected.

Artificial Intelligence (AI) has emerged as one of the defining technologies of this era. Its significance extends far beyond automation or efficiency improvement. AI is reshaping how nations generate, process, and act upon information, transforming decision-making across military, economic, and governance domains. In warfare, AI is accelerating operational tempo, enhancing situational awareness, enabling autonomous systems, and creating new pathways to achieve decision advantage. As data becomes a strategic resource, the ability to harness AI effectively is expected to increasingly influence national power and military effectiveness.

The implications for India are particularly significant. The country's strength lies in its vibrant digital ecosystem, world-class talent base, expanding innovation landscape, and growing defence industrial capabilities. These strengths create a unique opportunity to build indigenous capabilities that support both national development and defence modernisation. The technologies that power military AI, including advanced computing, data platforms, sensors, communications networks, robotics, and analytics, are often developed within broader commercial and civilian ecosystems. Consequently, the future of defence innovation will depend not only on investments within the defence sector, but also on the strength of collaboration across government, industry, academia, start-ups, and research institutions.

Globally, nations leading in military AI have demonstrated the importance of strong civil-military technology partnerships. Innovation increasingly occurs at the intersection of public and private sectors, where commercial technological advances

can be adapted to national security applications, and defence requirements can stimulate wider industrial and technological development. For India, fostering such collaboration can serve as a force multiplier, accelerating capability development while strengthening domestic innovation and technological sovereignty.

This report explores the evolution of military AI, its applications across contemporary military functions, emerging risks and governance considerations, and the foundational capabilities required to realise its full potential. Importantly, it highlights that successful adoption of military AI is not solely a question of technology. It requires robust data ecosystems, digital infrastructure, interoperable architecture, trusted governance frameworks, skilled human capital, and institutions capable of integrating technological innovation into operational practice.

As India advances towards the vision of an Agrabharat, the convergence of national security, technology, and innovation presents a unique opportunity. By leveraging its strengths in digital transformation, deep technology, and entrepreneurship, while fostering greater collaboration between civilian and defence ecosystems, India can strengthen its preparedness for the evolving character of warfare and contribute to a more secure, resilient, and technologically empowered future.

I hope this report provides useful insights for policymakers, defence leaders, industry stakeholders, and the wider strategic community as they navigate the opportunities and challenges presented by the age of AI-enabled warfare.

Nilachal Mishra

Partner and Head, Government & Public Services
KPMG in India

Foreword

India stands at a defining moment in its journey towards becoming an Aatmanirbhar and Agrasar Bharat; a nation that is not only economically and technologically self-reliant, but also capable of shaping the future of security and strategic affairs. In this vision, defence modernisation is no longer solely about acquiring advanced platforms and weapon systems. It is increasingly about building the digital foundations, industrial capabilities and innovation ecosystems that will determine military effectiveness in the decades ahead. Today, AI and Machine Learning (ML) represent the next major inflection point. Their significance lies not merely in enabling smarter platforms, but in transforming how military organisations observe, orient, decide, and act.

Recent conflicts have underscored that military advantage is increasingly determined by the ability to process information faster, integrate data across domains, deploy autonomous systems at scale and generate superior decisions under conditions of uncertainty. The future battlefield will be shaped by the convergence of data, algorithms, sensors, networks, autonomous systems, and human judgement. In this environment, decision superiority may prove to be as decisive as traditional measures of combat power.

One trend that I have increasingly observed across the defence, and technology ecosystem is the convergence of Artificial Intelligence, unmanned systems and space capabilities. These technologies are no longer evolving in isolation. AI is becoming the intelligence layer that enables autonomous decision-making, UAVs are emerging as distributed sensors and effectors across the battlespace and space-based assets provide the communications, navigation, intelligence and connectivity that tie these capabilities together. Their convergence is creating entirely new possibilities for military effectiveness, national security, and strategic advantage.

What makes this moment particularly significant is

that this domain remains at an early stage of evolution. No nation has yet established an undisputed leadership position. This presents a rare opportunity for India not merely to adopt emerging technologies, but to help shape the trajectory of their development. With its deep technology talent, vibrant start-up ecosystem, growing defence industrial base and expanding space ambitions, India possesses many of the ingredients required to emerge as a global leader in next generation defence technologies.

In many ways, this opportunity resembles India's transformation in the mobile technology sector. While we did not lead the landline era, we successfully leveraged a technological inflection point to become one of the world's largest and most dynamic mobile ecosystems. The convergence of AI, autonomy, space and advanced manufacturing presents a similar opportunity. If seized with ambition and purpose, it can help India leapfrog traditional models of defence capability development and emerge as a leader in shaping the future battlefield. It is time to translate innovation into mission ready capability.

We are pleased to present this report and hope it contributes meaningfully to the ongoing dialogue among policymakers, defence leaders, industry stakeholders, academia and innovators who are collectively shaping the future of an Aatmanirbhar, secure, and Agrasar Bharat.

Gaurav Mehndiratta

Partner and National Head
Aerospace, Defence and Space
KPMG in India



Contents

Executive summary	06
1. The evolution of warfare	08
1.1 From mass to precision	10
1.2 The unmanned turn	10
1.3 The intelligentised turn	11
1.4 A decade of AI at war: timeline	11
2. AI transforming warfare and the OODA loop	14
2.1 The military AI stack	15
2.2 Three ways AI changes the character of war	17
2.3 Approach of global players for military AI	18
2.4 AI's impact on OODA loop	22
2.5 AI at strategic and operational level of warfare - A framework	26
3. AI at the strategic level of warfare	28
3.1 Manufacturing and sustainment	29
3.2 Cyber: AI on both sides of the keyboard	31
3.3 Protecting national assets: energy, ports, nuclear, health, fuel and dams	33
3.4 Compute, space and the cognitive domain	34
4. AI at the operational level of warfare	36
4.1 Joint Command and Control (C2)	37
4.2 Targeting and kill-chain compression	38
4.3 Air and missile defence	38
4.4 Planning, wargaming and logistics	40
4.5 AI at tactical edge	42
4.5.1 Terminal autonomy	42
4.5.2 Swarms and collaborative autonomy	44
4.5.3 Counter-drone at machine speed	47
5. Risks and responsibility in military AI	51
6. Key imperatives for India	57
List of abbreviations	61

Executive Summary

AI is emerging as one of the most consequential military technologies of the twenty-first century. Much as mechanisation transformed mobility, air power transformed reach, and precision weapons transformed targeting, AI is transforming the speed and quality of military decision-making. Its significance lies not in a single weapon system or platform, but in its ability to connect sensors, networks, commanders, and weapons into an increasingly intelligent and responsive system of systems. As warfare becomes more data-intensive, military advantage is increasingly determined by the ability to convert information into decisions and decisions into action faster than an adversary. This report examines how AI is reshaping warfare across the strategic, operational, and tactical levels, and what these developments mean for India's journey towards an Aatmanirbhar and Agrasar Bharat.

The character of warfare has evolved through successive eras of mechanisation, precision strike, networked operations, and unmanned systems. The emerging era of intelligentised warfare builds upon these foundations by augmenting human cognition itself. AI enables military organisations to process vast volumes of data, generate situational awareness, identify patterns, recommend courses of action, and support increasingly autonomous operations. As a result, the focus of military competition is shifting from platform superiority and force mass towards decision superiority, where the ability to sense, understand, and respond faster becomes a decisive advantage.

At the heart of this transformation lies the Observe-Orient-Decide-Act (OODA) loop. AI enhances every stage of the cycle by automating observation, accelerating orientation through data fusion, supporting decision-making through analytics and recommendations, and enabling faster execution through autonomous and semi-autonomous systems. While these capabilities compress decision timelines and increase operational tempo, they also create new vulnerabilities, including automation bias, adversarial

deception, data poisoning, model dependence, and machine-speed escalation. The challenge for military organisations is therefore not merely to deploy AI, but to deploy it responsibly, preserving meaningful human judgement and accountability in increasingly automated environments.

The report identifies three fundamental ways in which AI is altering the character of warfare. First, data is emerging as a strategic military asset, with advantage increasingly derived from the quality, accessibility, and exploitation of operational data. Second, autonomous systems are changing the economics of warfare by enabling affordable mass, allowing large numbers of relatively inexpensive platforms to impose disproportionate costs on defenders. Third, AI is shifting the human role from information processing towards supervision, judgement, and mission command, making governance, doctrine, training, and human-machine teaming central to future military effectiveness.

AI's impact extends well beyond the battlefield. At the strategic level, it is transforming defence manufacturing, sustainment, logistics, cyber operations, critical infrastructure protection, intelligence processing, space-based Intelligence, Surveillance and Reconnaissance (ISR), and the cognitive domain. At the operational level, AI enables joint Command and Control (C2), targeting, air and missile defence, campaign planning, and logistics optimisation by integrating information across services and domains. At the tactical edge, AI allows platforms and units to operate effectively even in contested, degraded, or denied environments, supporting terminal autonomy, collaborative swarms, and machine-speed counter-drone operations. Together, these applications signal the emergence of a more distributed, resilient, and adaptive model of warfare.

Global experience demonstrates that success in military AI depends on more than technological innovation alone. Leading powers are investing in sovereign data ecosystems, digital infrastructure, interoperable architecture, AI-enabled command systems, and new models of civil-military collaboration. The most effective programmes combine operational users, industry, academia, and government institutions within a common innovation ecosystem capable of translating emerging technologies into deployable military capability.

For India, the implications are profound. Future military effectiveness will depend not only on acquiring AI-enabled platforms but on building the foundations of intelligent warfare: trusted data architecture, resilient digital infrastructure, sovereign AI capabilities, secure software ecosystems, interoperable command networks, and adaptive institutional frameworks. The opportunity extends beyond defence modernisation. Military AI can act as a catalyst for domestic innovation, advanced

manufacturing, deep-tech entrepreneurship, and civil-military technology collaboration, reinforcing the broader national vision of Agradar Bharat.

The report concludes that AI is not changing the fundamental nature of war, which remains a contest of political will, strategy, and human judgement. It is, however, profoundly changing the character of warfare by compressing decision cycles, expanding autonomy, and elevating the importance of data and digital infrastructure as instruments of national power. In this environment, enduring strategic advantage will belong to those nations that can most effectively combine technology, institutions, industrial capacity, and human judgement into an integrated system capable of delivering decision superiority across the spectrum of conflict.



01

The Evolution of warfare



Successive technological eras have compressed the sensor-to-shooter kill chain, shifting battlefield awareness from individual soldiers and field formations toward algorithm-enabled strategic decision-making.

Warfare has continuously evolved in response to advances in technology, organisation, and the methods through which military forces generate and exploit information. From an era where battlefield awareness was limited to individual commanders and local formations, warfare progressed through mechanisation, precision strike capabilities, and networked operations that expanded the scale and speed of military action. Across these successive eras, the common trend has been the compression of the sensor-to-shooter cycle through improvements in sensing, communication, processing, and weapon systems. Today, the growing volume and complexity of battlefield data have created a new challenge: the ability to interpret and act upon information faster than an adversary. AI represents the latest stage in this evolution, enabling military organisations to transform vast streams of data into actionable insights, accelerate decision-making, and support increasingly autonomous operations. Understanding this historical progression provides the foundation for assessing how AI is reshaping the character of warfare and redefining military advantage in the twenty-first century.

The evolution of warfare can be viewed as a progression in how militaries collect information, make decisions, and translate those decisions into battlefield effects. In the earliest era, commanders relied on limited local observations and slow communications, resulting in sequential decision-making cycles. Mechanisation, radio communications, and aerial reconnaissance subsequently expanded situational awareness, enabling coordination across larger formations. The emergence of satellites, radar, and precision-guided weapons further accelerated the sensor-to-shooter chain, making information a critical source of combat power. The next phase saw the development of networked forces, where real-time data sharing enabled coordinated operations across multiple domains. Exhibit 1 presents the same.

Exhibit 1: Five eras of warfare and the shifting unit of decision

Era	Battlefield awareness	Decision model	Dominant decision unit	Character of the decision cycle
Localised Awareness and Commander-Led Warfare	Information derived primarily from direct observation, scouts, messengers and reports from nearby formations	Decisions based on incomplete, delayed and locally held information	Individual commander and field formation	Sequential and slow: observe locally, relay information, decide centrally and issue orders
Connected Command and Mechanised Warfare	Radio, aerial reconnaissance and mobile headquarters extend awareness beyond line of sight	Commanders coordinate manoeuvre using periodically updated reports from multiple formations	Division, corps or fleet headquarters	Connected but hierarchical: faster communication improves coordination, but information remains fragmented
Sensor-Enabled Precision Warfare	Satellites, airborne surveillance, radar and electronic intelligence create a broader operational picture	Specialists analyse sensor information and commanders match identified targets with precision weapons	Joint or theatre-level command	Sensor-to-shooter integration: detection and targeting accelerate, although analysis and approvals remain manpower-intensive
Networked and Distributed Warfare	Data from multiple platforms and services is shared through common operational networks	Decisions are distributed across connected headquarters, platforms and tactical units	Networked joint force	Near-real-time collaboration: shared awareness enables coordinated action across domains and shorter kill chains
Algorithm-Assisted and Autonomous Warfare	AI continuously fuses sensor, intelligence and open-source data, identifies patterns and prioritises threats	Machines support orientation and course-of-action development; humans supervise, authorise or set decision boundaries	Human-machine decision system	

Today, warfare is entering an era of algorithm-assisted and autonomous operations, where AI systems continuously process vast volumes of data, support course-of action development, and enable human-machine teaming. Across all these eras, the consistent trend has been the expansion of battlefield awareness, the acceleration of decision cycles, and the increasing importance of information processing as a determinant of military advantage

1.1 From mass to precision

For much of the industrial era, battlefield success depended on the ability to mobilise and sustain mass: large armies, concentrated firepower and deep stocks of arms and ammunition. Forces sought to overwhelm and saturate enemy defences, absorb acceptable losses and create breakthroughs through weight of numbers. Over time, however, the objectives and constraints of warfare expanded beyond the capture and holding of territory. Advances in intelligence, surveillance, communications, navigation and precision-guided weapons shifted the basis of effectiveness from mass alone to the selective application of force. Commanders acquired a wider range of options to achieve military and political objectives with greater nuance striking specific targets, tailoring the scale and timing of effects, limiting collateral damage and conserving scarce personnel and materiel. Information superiority therefore became a form of combat power in its own right, enabling forces to replace indiscriminate concentration with precise, proportionate and increasingly networked action.

1.2 The unmanned turn

UAVs first demonstrated their distinctive operational value in counterterrorism and counter-insurgency campaigns, particularly in Afghanistan and Iraq. Their endurance enabled persistent surveillance over areas of interest, while armed variants could rapidly engage identified targets with precision, limiting collateral damage and removing aircrew—and, in some cases, ground forces from immediate danger. Their role subsequently expanded from asymmetric campaigns to conventional conflict. During the 2020 Nagorno-Karabakh war¹, Azerbaijan employed UAVs and loitering munitions effectively against Armenian forces, using persistent sensing and precision attack to locate, expose and strike air-defence systems, armour and other battlefield assets. A key enabler in both contexts was technological asymmetry: UAVs were most effective where the adversary lacked layered air-defences, electronic-warfare capabilities and suitable counter-UAV measures. The rise of UAVs therefore represented more than the introduction of an unmanned platform; it underscored the growing importance of collecting persistent sensor data, processing it rapidly into actionable intelligence, and transmitting it reliably across the sensor-to-shooter chain.

Recent conflicts, most notably the Russia-Ukraine war² and India's Operation Sindoor³ in May 2025, have underscored the emergence of drones as the principal instruments of attrition on the modern battlefield. These conflicts demonstrated the ability of unmanned systems to deliver persistent surveillance, precision strike, and massed combat effects at relatively low cost and risk. Operation Sindoor was widely characterised in India as the country's first largely non-contact conflict, where drones, loitering munitions, and long-range missiles substituted for the large-scale employment of conventional troop formations⁴. The result is a growing shift towards standoff, technology-driven warfare in which the contest increasingly revolves around sensors, networks, algorithms, and autonomous platforms rather than the massing of forces.

1. CSIS. The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense. December 2020.

2. How Are Drones Changing War? The Future of the Battlefield, Center for European Policy Analysis (CEPA), Michael Newton, November 2025

3. Operation SINDOOR: The Rise of Aatmanirbhar Innovation in National Security, Press Information Bureau, Santosh Kumar, Ritu Kataria and Kritika Rane, May 2025

4. The Tribune. Operation Sindoor accelerated indigenous drone development and counter-measures. 9 May 2026.

1.3 The intelligentised turn

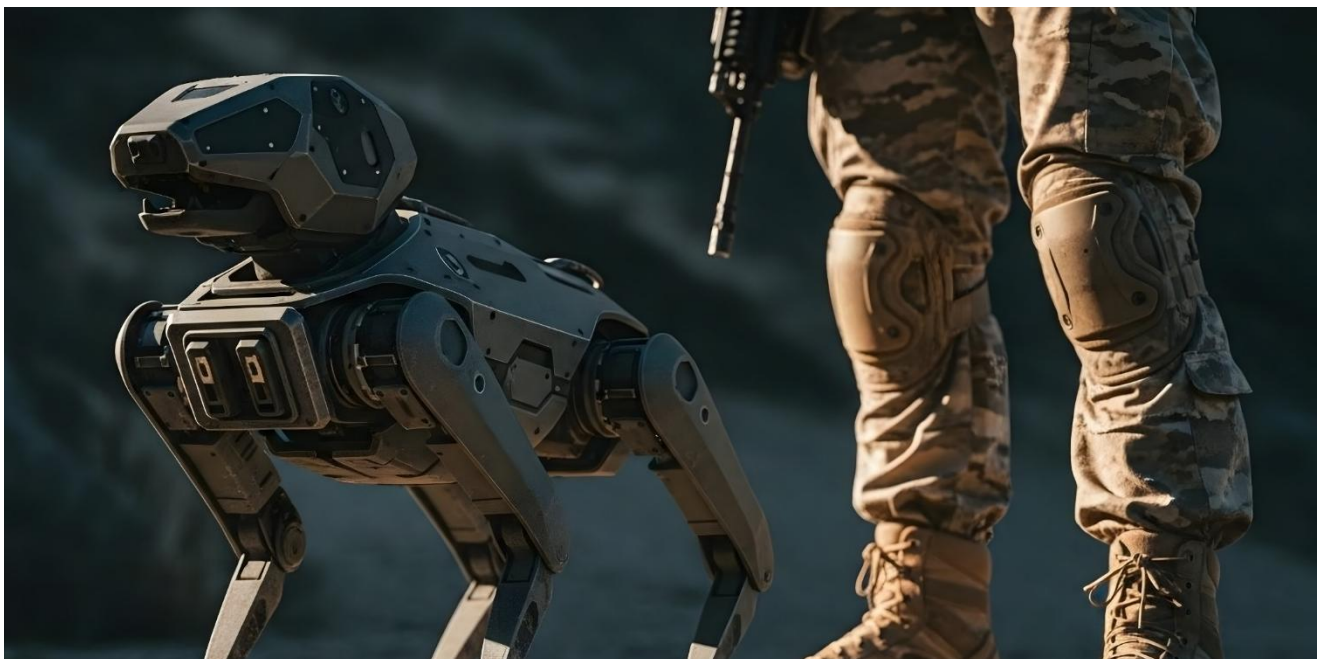
The current era can be characterised as one of intelligent warfare. While previous military revolutions enhanced battlefield sensors, communication networks, and precision weapons, AI transforms the critical layer between them: decision-making and data processing. AI enables military organisations to convert vast volumes of information into actionable insights at a speed and scale that far exceeds human capabilities.

The magnitude of this challenge is illustrated by commercial satellite imagery. According to a leading geospatial intelligence company's Chief Technology Officer, a single analyst would require approximately 85 years to review just one day's worth of imagery generated by the company's satellites⁵. ML algorithms can sift through the same data in seconds, automatically identifying anomalies, prioritizing targets, and presenting operators with a concise set of actionable observations. As a result, competitive advantage increasingly stems not from the ability to collect data, but from the ability to process, interpret, and act on it faster than an adversary.

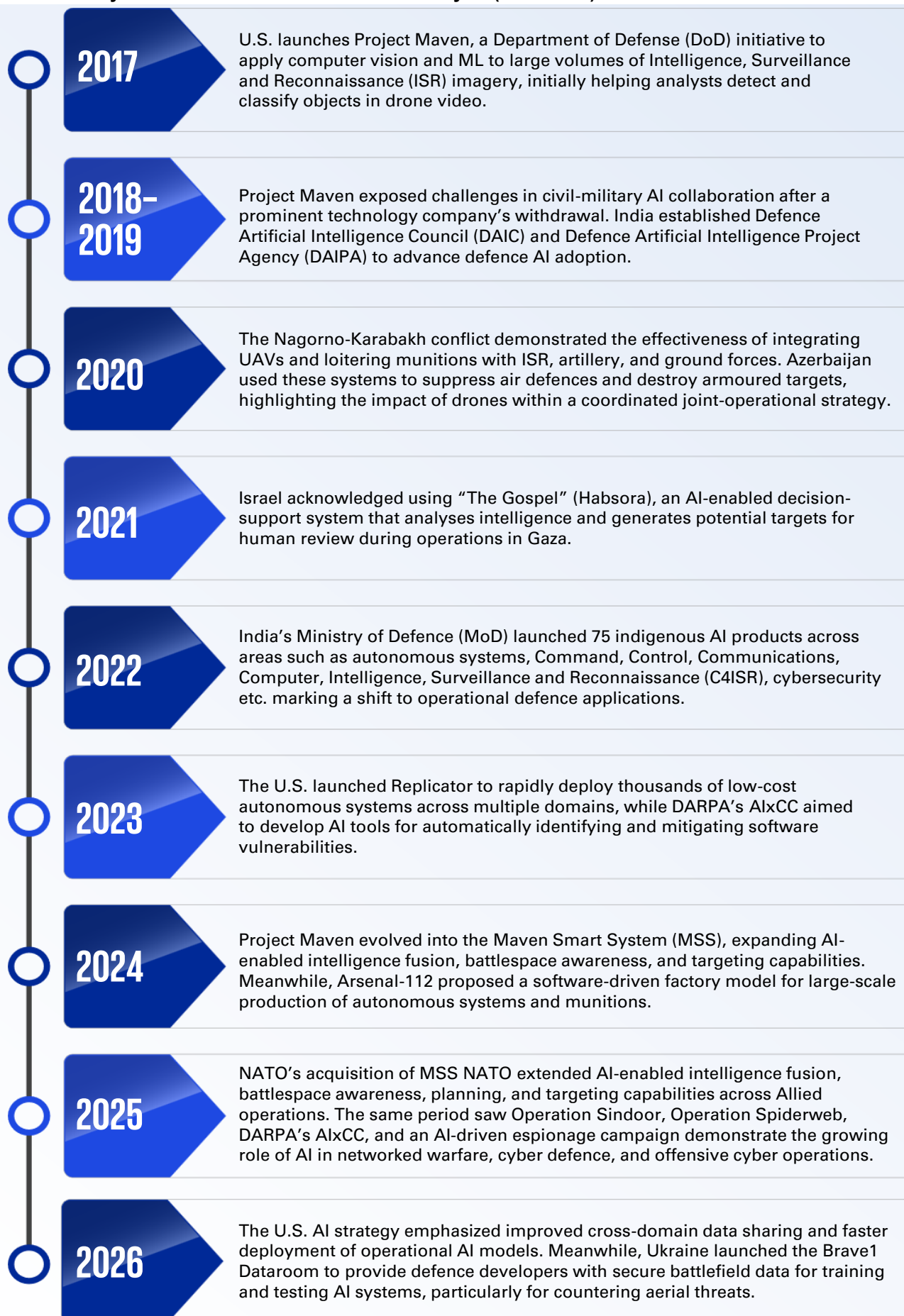
1.4 A decade of AI at war: timeline

Military AI has evolved from a niche analytical capability into a core enabler of combat operations, defence industrial production, cyber warfare, and military decision-making. The last decade has witnessed a series of important milestones that have transformed AI from an experimental analytical tool into a core military capability. Beginning with the application of ML to intelligence analysis, the evolution has expanded to AI-enabled targeting, autonomous systems, cyber operations, defence manufacturing, and enterprise-wide decision-support platforms. Collectively, these developments demonstrate a clear shift towards data-driven warfare, where military advantage increasingly depends on the ability to collect, process, and act upon information faster than an adversary.

The timeline below highlights some of the most significant global milestones that have shaped the emergence of AI-enabled warfare between 2017 and 2026. The milestones collectively highlight a broader shift from using AI to support analysis towards using AI to shape operational outcomes across the battlefield and defence enterprises.



5. M. Mande and G. C. Allen, CSIS. What Is Maven Smart System, and What Does It Do?. 2 Jun 2026

Exhibit 2: Key milestones in the evolution of military AI (2017-2026)^{6,7,8,9,10,11,12,13,14,15,16,17}

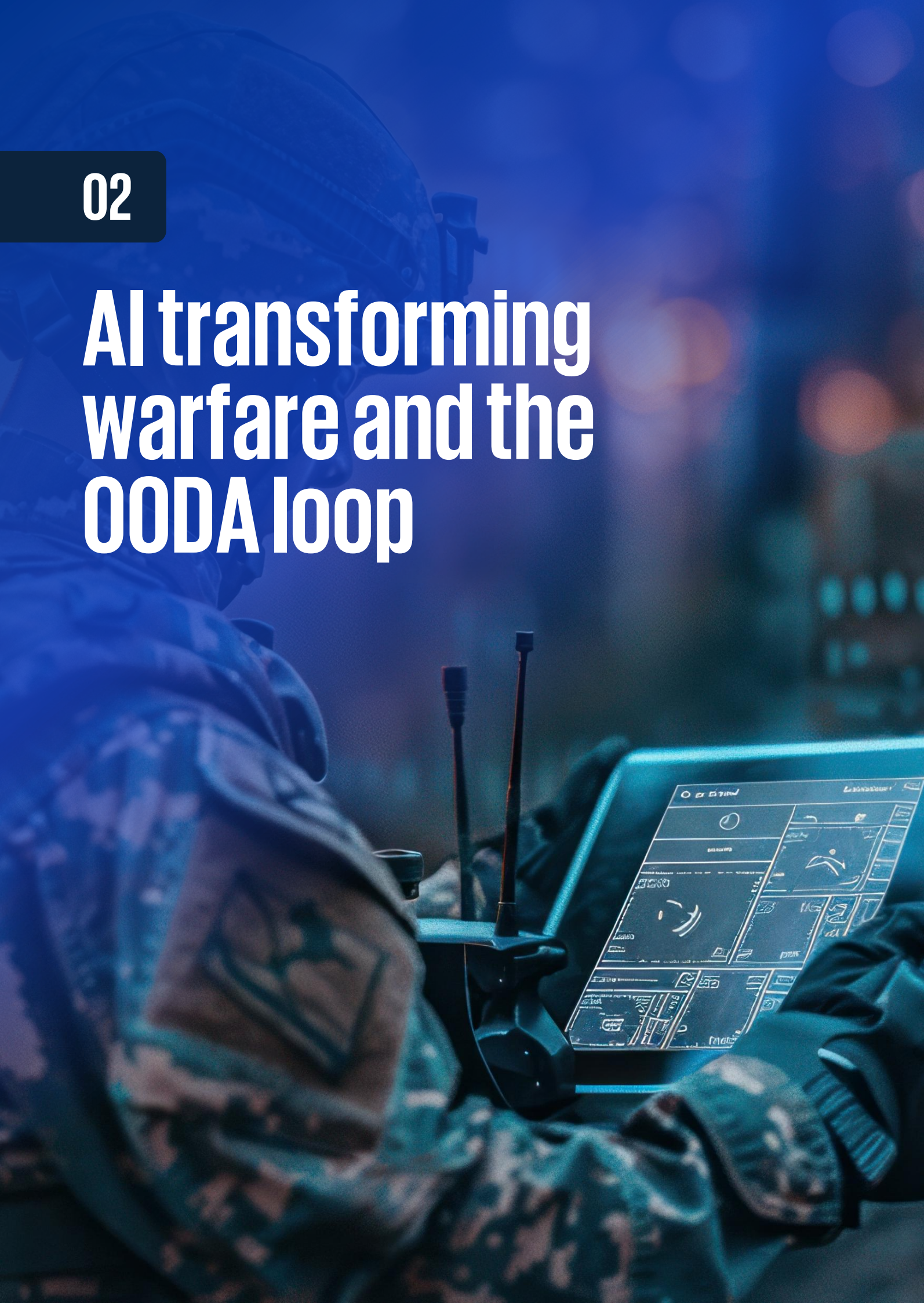
Over the past decade, military AI has progressed from experimental tools for analysing ISR data to operational systems supporting targeting, platform autonomy, cyber operations and battlefield decision-making. The decisive shift is now from proving individual applications to scaling trusted, interoperable capabilities across forces supported by operational data, secure digital infrastructure, agile procurement and human oversight.



6. Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven), U.S. Department of Defense, Deputy Secretary of Defense, April 2017
7. Google and Project Maven (A): Big Tech, Government and the AI Arms Race, INSEAD, Gianpiero Petriglieri and Jaimie Stettin, May 2018
8. Task Force for Implementation of AI, Press Information Bureau, March 2022
9. Lessons from the Nagorno-Karabakh 2020 Conflict, Center for Army Lessons Learned, Phillip Andrews, August 2021
10. Technology and Human Decision-Making in IDF Operations: The IDF's Use of Data Technologies in Intelligence Processing, Israel Defense Forces (IDF), June 2024
11. Raksha Mantri Launches 75 Artificial Intelligence Products/Technologies During First-Ever 'AI in Defence' Symposium and Exhibition in New Delhi, Press Information Bureau, July 2022
12. Implementing the Department of Defense Replicator Initiative to Accelerate All-Domain Attributable Autonomous Systems to Warfighters at Speed and Scale, Defense Innovation Unit (DIU), November 2023
13. Contracting Personnel Use AI, Maven Smart System Simulation During Warfighter Exercise, United States Army, Tish Williamson and Mission and Installation Contracting Command Public Affairs, March 2025
14. Anduril Building Arsenal-1 Hyperscale Manufacturing Facility in Ohio, Anduril Industries, January 2025
15. NATO Acquires AI-Enabled Warfighting System, Supreme Headquarters Allied Powers Europe (SHAPE), April 2025
16. Artificial Intelligence Strategy for the Department of War, United States Department of War, Pete Hegseth, January 2026
17. Ministry of Defence Launches Brave1 Dataroom, a Secure Environment for Training Military AI Solutions, Ministry of Defence of Ukraine, January 2026

02

AI transforming warfare and the OODA loop



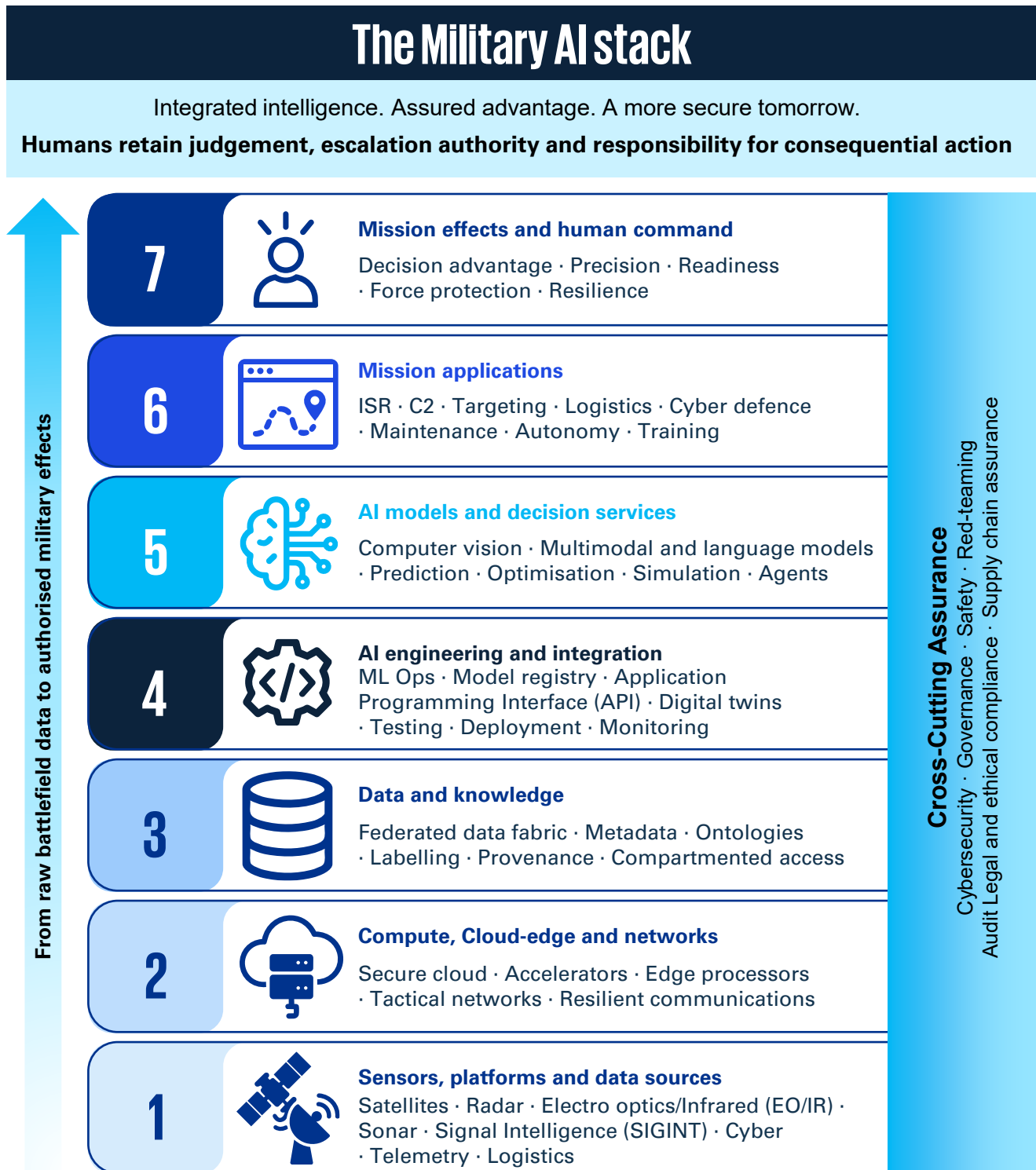
AI does not transform warfare through a single weapon or platform; it transforms the entire kill chain. By automating target detection, data fusion, prioritisation, decision support and targeting. AI compresses every stage of the OODA loop, shifting military competition from platform superiority toward decision superiority, where the quality, accessibility, and exploitation of data become decisive advantages.

2.1 The military AI stack

The military AI stack provides a useful framework for understanding how AI-enabled military capability is created and translated into operational outcomes. The stack begins with sensors, platforms, and data sources that generate information from across battlespace, supported by computing infrastructure, communications networks, and data-management capabilities that enable its collection, processing, and dissemination. AI models, decision-support services, and mission applications then transform this information into actionable insights, recommendations, and operational effects across functions such as intelligence, C2, targeting, logistics, cyber operations, and autonomous systems. The ultimate outcome is the generation of decision advantage, operational effectiveness, force protection, and mission resilience. The framework also highlights two principles that underpin successful military AI adoption: human judgement remains central to consequential decisions, and assurance mechanisms such as cybersecurity, testing, validation, governance, and legal oversight must extend across every layer of the stack.



Exhibit 3: The Military AI capability stack



The sections that follow examine this AI ecosystem from multiple perspectives. The report first explores the three ways in which AI is changing warfare, namely by making data a strategic asset, compressing decision cycles, and enabling greater autonomy across military operations. It then analyses how leading military powers are approaching AI adoption, including the institutional, technological, and industrial foundations they are building to operationalise these capabilities at scale.

2.2 Three ways AI changes the character of war

AI changes the character of war in three fundamental ways: it transforms data into a source of combat power, enables affordable mass through autonomous systems, and shifts human effort from processing information to exercising judgement. Collectively, these changes move military competition from platform superiority towards decision superiority.

1. It turns data into a weapon system

In AI-enabled warfare, data is evolving from a supporting asset into a core element of combat power. Like ammunition or fuel, data must be continuously collected, processed, distributed and refreshed to generate operational advantage. Modern military platforms including satellites, UAVs, radars, electronic intelligence systems and frontline sensors generate vast volumes of information on adversary movements, targets, signatures and vulnerabilities, while simultaneously providing visibility into the status, readiness and disposition of friendly forces.

AI creates value by fusing these disparate data streams into a Common Operational Picture (COP), enabling commanders to improve situational awareness, prioritise threats, allocate resources more effectively and accelerate the transition from detection to action. Consequently, military advantage is increasingly determined not by the volume of data collected, but by the quality, accessibility, timeliness and interoperability of that data. High-quality datasets enable more accurate models, faster decisions and greater operational precision, whereas fragmented or outdated data can undermine even the most advanced AI-enabled systems.

Recent initiatives highlight the growing strategic importance of data ecosystems. Ukraine's Brave1 Dataroom provides vetted developers access to structured battlefield datasets for training and validating defence AI models¹⁸, while U.S.'s AI strategy emphasizes cross-domain data sharing and the rapid deployment of operational models^{19 20}. Together, these developments underscore a fundamental shift in modern warfare: control over trusted, high-quality operational data is increasingly becoming a prerequisite for decision superiority and sustained military advantage.

2. It changes the economics of mass

AI-enabled autonomy is changing the economics of mass by allowing relatively inexpensive unmanned systems to be deployed in numbers large enough to saturate conventional defences. The resulting asymmetry is not only operational but also economic: a defender may be compelled to expend scarce, high-cost interceptors, maintain continuous surveillance and deploy specialised countermeasures against threats that are individually cheap and expendable. Even when most incoming systems are neutralised, their volume can exhaust magazines, overload sensors and command networks, expose defensive positions and create openings for more capable weapons. UAVs, loitering munitions and unmanned surface or underwater vehicles are central to this model because they can distribute sensing and strike functions across many attritable platforms. Autonomous navigation and terminal guidance further strengthen the advantage by reducing dependence on continuous communications and making some systems more resilient to jamming²¹. Recent drone-swarm attacks and the use of unmanned sea vehicles against higher-value naval assets demonstrate how low-cost autonomous mass can impose economically disproportionate defensive requirements and shift the cost-exchange balance in favour of the attacker.

18. Ministry of Defence of Ukraine (Zbroiya.gov.ua). Ukrainian companies train AI at scale in Brave1 Dataroom. 11 Jun 2026.
19. U.S. Department of War. Artificial Intelligence Strategy for the Department of War. 9 Jan 2026.

20. 20. GovCIO Media & Research. Hegseth Unveils 'Wartime Footing' for Military AI in Strategy Document. 23 Jan 2026.
21. Kyiv Post. 'Fire and Forget': Ukraine Rolls Out FPV Drones With Autonomous Terminal Guidance. 15 Sep 2025.

3. It relocates the human role

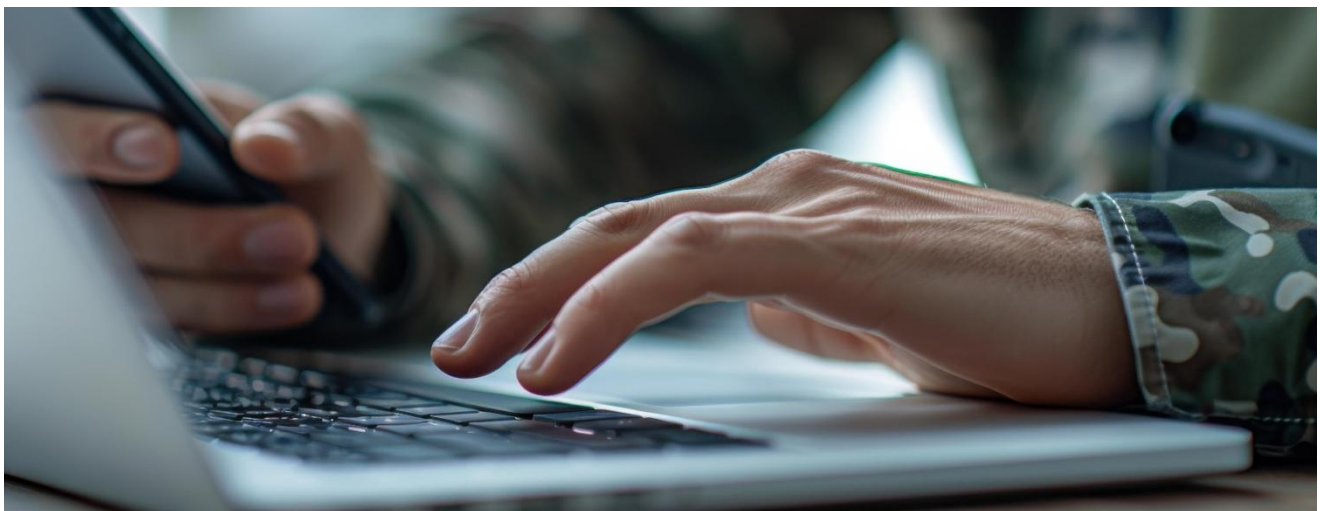
AI is relocating the human role further along the decision chain. Earlier digital tools primarily helped analysts collect, organise and visualise information; contemporary AI systems can increasingly fuse multiple data streams, identify patterns, assess their operational significance and present outputs in a decision-ready format. They may also generate, compare and prioritise courses of action, leaving commanders and analysts to validate assumptions, weigh trade-offs, apply contextual judgement and authorise the response. The shift is therefore not simply from manual data assembly to faster analysis, but from human-led analysis towards machine-assisted decision preparation.

As AI assumes more of both the assembly and analytical workload, the distinctive human contribution increasingly lies in deciding whether, when and how to act. This makes doctrine, training, accountability and meaningful human oversight as important as the underlying software.

2.3 Approach of global players for military AI

Data point-innovation capital is becoming as significant as experimentation programs in the adoption of military AI. Governments are now investing in the broader innovation system needed to transition cutting edge technologies into operational military capability, on top of just funding individual AI solutions. For example, 23 NATO Allies agreed on establishing a EUR 1 billion Innovation Fund to support dual-use deep technologies. This is, while NATO's Defence Innovation Accelerator for the North (DIANA) network expansion took place. In 2024, it expanded from 90 to 182 test centres and from 11 to 23 accelerators²². These numbers signal that successful military AI adoption depends on a combination of test infrastructure, industry engagement, and the deployment pathways rather than algorithm building alone. Collectively, they give a useful indicator of the capital which is being mobilised across the broader military deep-tech ecosystem.

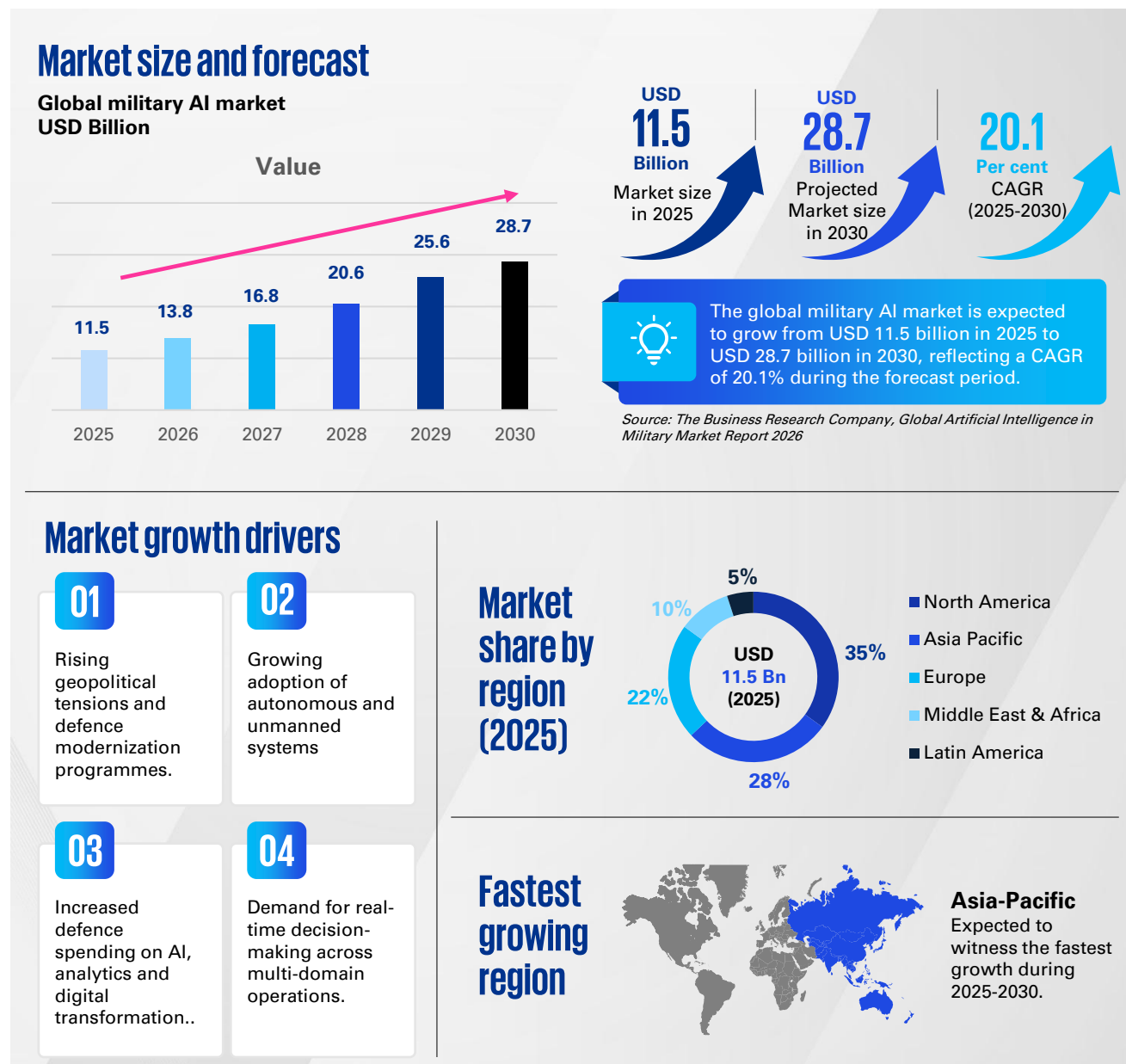
Global defence spending provides a broader investment backdrop for military AI. Military expenditure reached approximately USD 2.9 trillion in 2025, a 2.9 per cent real term increase over the previous year and around 40 per cent above 2016 levels²³. While AI-enabled systems still account for a relatively small share of this expenditure, market forecasts point to sustained growth. Leading estimates value the global military AI market at approximately USD 9–15 billion in the mid-2020s and project it to reach USD 19–29 billion by 2030, implying annual growth of about 13–20 per cent^{24 25}. Growth spans autonomous platforms, intelligence and surveillance, cybersecurity, C2, logistics, training and decision support. These figures remain indicative, however, because market definitions differ and no globally accepted methodology consistently separates military AI expenditure from wider spending on digital systems, platforms and dual-use technologies.



22. DIANA, NATO's Innovation Accelerator, Doubles the Size of its Transatlantic Network, North Atlantic Treaty Organization (NATO), 14 March 2024
23. Trends in World Military Expenditure, 2025, Stockholm International Peace Research Institute (SIPRI), Xiao Liang, Nan Tian, Diego Lopes da Silva, Lorenzo Scarazzato, Zubaida A. Karim

- and Jade Guiberteau Ricard, April 2026
24. Artificial Intelligence in Military Market Size, Share & Trends Analysis Report, 2025–2030, Grand View Research, December 2024
25. Artificial Intelligence in Military Market Report 2026: Global Outlook, The Business Research Company, September 2026

Exhibit 4 – Potential global military AI market size

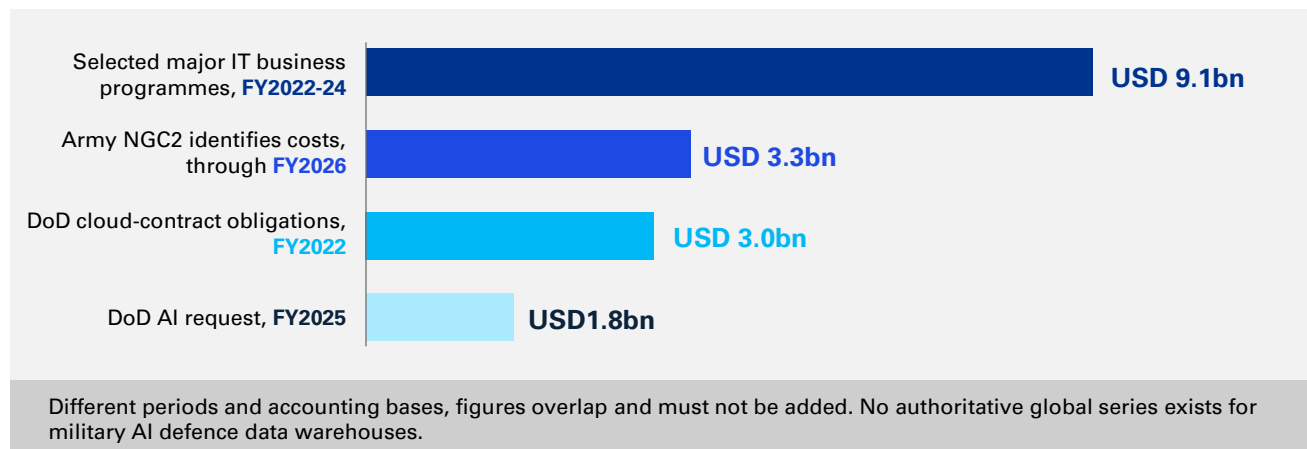


As AI is increasingly becoming a significant factor of military effectiveness, countries are adopting different strategies to build and operationalise these capabilities. While national objectives vary, from speeding up the decision-making and improving the autonomous systems to building cyber resilience and military industrial competitiveness, a common trend is emerging: AI is being integrated into core functions of military rather than being treated as a standalone initiative. Governments are therefore investing in digital infrastructure and defence databases, establishing dedicated AI institutions, and integrating AI across C2 chain, logistics and operational planning functions.

The experience of global military players illustrates the shift from testing to scaled capability deployment. While some defence institutions have given priority to enterprise-wide decision support platforms, others have given more importance to autonomous and unmanned systems or on developing sovereign data ecosystems to support future AI applications.

Some AI initiatives taken by the U.S. that are playing an important role in shaping the futuristic warfare are shown in exhibit 5

Exhibit 5: Publicly disclosed U.S. defence digital-investment proxies



Source: U.S. Government Accountability Office (GAO)

Exhibit 6: Initiatives adopted by major defence powers for military AI

Actor	Initiatives	Documented programmes and capabilities
United States	U.S. DoD established the Algorithmic Warfare Cross-Functional Team (AWCFT) in April 2017 to accelerate the integration of big data and machine learning and convert defence data into actionable intelligence ²⁶ .	Project Maven: Its first task was to augment or automate processing, exploitation and dissemination of tactical Unmanned Aerial Systems (UAS) and mid-altitude full-motion video for the Defeat-ISIS campaign. Initial capabilities covered computer-vision-based object detection, classification and alerts, with integration planned in 90-day sprints ²⁷ .
China	The U.S. DoD's 2024 report to Congress describes the PLA's modernisation objectives and its development of AI and other advanced technologies as part of future force development, including objectives associated with 2027.	The report addresses PLA strategy, current capabilities, military-technological development, operational concepts and resources for force modernisation. It identifies AI among the technologies relevant to the PLA's longer-term development ²⁸ .
NATO	NATO acquired an AI-enabled common data and warfighting capability for Allied Command Operations to support military operations and the adoption of additional AI models developed across the Alliance.	Maven Smart System NATO: NATO Communications and Information Agency (NCIA) states that the system supports intelligence fusion and targeting, battlespace awareness, planning and accelerated decision-making, and includes applications ranging from large language models to generative AI and machine learning. The acquisition took six months from requirement definition to contract ²⁹ .

26. Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven), U.S. Department of Defense, Robert O. Work, April 2017

27. U.S. Department of Defense, Deputy Secretary of Defense memorandum, "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," 26 April 2017.

28. Military and Security Developments Involving the People's Republic of China 2024, U.S. Department of Defense, December 2024.

29. NATO Acquires AI-Enabled Warfighting System, NATO Communications and Information Agency, April 2025

Actor	Initiatives	Documented programmes and capabilities
Ukraine	Ukraine's Ministry of Defence is providing vetted defence developers with controlled access to structured combat datasets for training, testing and validating military AI models.	Brave1 Data room: launched in January 2026 with visual and thermal datasets of aerial targets. The initial focus is detection, classification and autonomous interception of enemy drones. By June 2026, the Ministry reported that more than 100 Ukrainian companies had obtained access ³⁰ .
Israel	The Israel Defense Forces (IDF) states that it uses big-data processing tools to help intelligence analysts cross-reference existing intelligence sources and focus on information relevant to their research.	Gospel and Lavender: The IDF describes them as data-analysis tools that support intelligence processing. It states that they do not autonomously select or generate targets, cannot be the sole basis for identifying a target, and do not replace the analyst or operational commander ³¹ .
India	Following a multi-stakeholder task force, the Indian MoD created the Defence AI Council (DAIC) and Defence AI Project Agency (DAIPA) in February 2019 to provide policy guidance, structural support and an operating framework for defence AI adoption.	Official releases record Service-level AI subcommittees and a tri-Service joint working group, Service data policies and data-management officers, projects through iDEX and academia, and AI roadmaps for defence public-sector undertakings ³² . In August 2022, the government reported 70 identified DPSU AI projects, of which 40 had been completed ³³ .
Russia	The Russian Federation adopted the National Strategy for the Development of AI up to 2030 in 2019. The strategic document directs government bodies to support AI adoption across priority sectors including defence ³⁴ .	Uran-9 robotic combat system: The platform incorporates autonomous navigation system, target tracking and remote-control capabilities and obstacle avoidance ³⁵ .

Industrial players of military AI

The military AI sector is experiencing both rapid growth and diversity, translating it into one of the most dynamic segments of defence industry. As governments accelerate the integration of AI capabilities, the market has attracted a broad spectrum of private players. The list ranges from legacy defence primes to emerging companies. This has led to a notable evolution of the industrial landscape with the new players reshaping competitive dynamics and traditional value chains. Consequently, defence contractors are expanding their AI portfolios through a combination of strategic partnerships, in-house innovation, and acquisition of niche AI start-ups.

As per SIPRI report on-"Mapping the military AI industry" the companies involved in the provision of military AI have been categorized based on their business models³⁶ as following:

30. Ministry of Defence Launches Brave1 Dataroom, a Secure Environment for Training Military AI Solutions, Ministry of Defence of Ukraine, January 2026.
31. Technology and Human Decision-Making in IDF Operations: The IDF's Use of Data Technologies in Intelligence Processing, Israel Defense Forces, June 2024.
32. Task Force for Implementation of AI, Press Information Bureau, Ministry of Defence, March 2022
33. Enhancement of Capabilities of AI Technology, Press Information

- Bureau, Ministry of Defence, August 2022
34. Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation, Center for Security and Emerging Technology, October 2019
35. Uran-9 Unmanned Ground Combat Vehicle, Army Technology, Praveen Duddu, November 2016
36. Mapping the Military AI Industry, Stockholm International Peace Research Institute (SIPRI), Alexander Blanchard, Vincent Boulanin and Laura Bruun, April 2026

Exhibit 7: Initiatives adopted by major defence powers for military AI

Defence primes 	Neoprimes and startups 	Big tech 	Foundational model providers 
• Legacy defence contractors with long-term government relationships • Serve as lead integrators for major defence programmes • Applications across weapon integration, logistics, maintenance, surveillance and target acquisition • Ex: autonomous loitering munition, automated weapon systems.	• Relatively new players • Primary focus on data analytics, autonomy, AI intelligence, and digital platforms • Deliver highly niche capabilities; could be dual-use • Capabilities include autonomous systems, AI-powered intelligence tools, Battle Management Systems (BMS) and counter-UAV solutions.	• Major global technology companies that operate across both markets-commercial and military • Leverage their capital, scale and dominance over critical digital infrastructure like data centres, cloud platforms, communication networks.	• Build and maintain large-scale AI models, contribute as foundational technologies • Applications include analytics, intelligence functions, autonomy and decision support • Backed by a combination of strategic funding and venture capital from big tech.

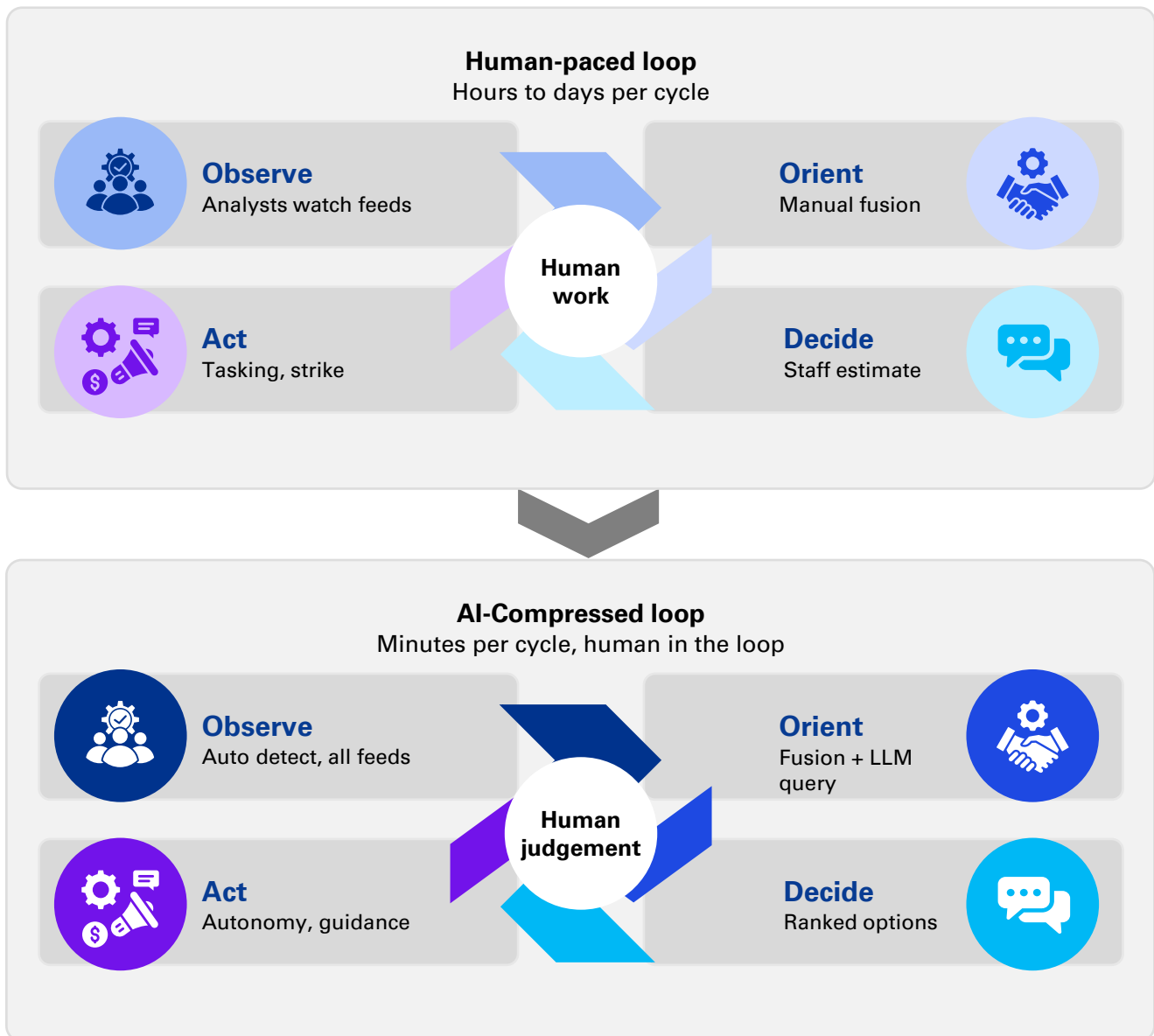
2.4 AI's impact on OODA loop

Colonel John Boyd was a U.S. Air Force fighter pilot and military strategist whose work on air combat, decision-making and organisational adaptation influenced modern military thought. He expressed conflict as a recurring cycle of Observe, Orient, Decide and Act the OODA loop. The central proposition was not simply that the side completing the cycle fastest would prevail, but that it could repeatedly create, and exploit change faster than an opponent could understand and respond to it³⁷.

Orientation is the pivotal phase because it gives meaning to what has been observed. It is where raw information is filtered through experience, doctrine, training, cultural assumptions, prior knowledge and the unfolding operational context to form a working picture of the situation. Decisions and actions are only as sound as this interpretation: rapid observation followed by a flawed orientation can produce a confidently wrong response. Orientation also shapes the rest of the loop continuously by determining what commanders look for next, which developments they consider significant and which options appear feasible. An actor that adapts its mental model more accurately than its opponent can therefore disrupt the opponent's understanding and initiative even without possessing uniformly superior platforms or information.

AI changes the OODA loop by increasing the volume and speed of observation, fusing diverse inputs into a COP, identifying patterns and supporting the comparison of possible responses. Its most consequential effect is on Orientation, where algorithms increasingly help determine what the data means and what deserves attention. AI can consequently compress the overall cycle and support action at greater tempo, but it can also propagate stale data, hidden bias or adversarial deception more quickly. The stage-by-stage effects and associated vulnerabilities are set out below.

37. CULTURAL KSAs: Skill Development Using the OODA Loop, Air University, Patricia Fogarty, March 2019

Exhibit 8: The OODA loop before and after AI³⁸

Boyd's model: The side that cycles faster and orients better wins

As AI becomes embedded across command-and-control systems, it is compressing the time required to move from detection to action while improving the scale and quality of information available to commanders. However, these gains are accompanied by new risks, including automation bias, data manipulation, adversarial deception, and machine-speed escalation. The exhibit below illustrates how AI is transforming each stage of the OODA loop, highlighting both the operational advantages and the emerging vulnerabilities that military organisations must manage in an increasingly AI-enabled battlespace

38. Speeding Up the OODA Loop with AI: A Helpful or Limiting Framework?, Joint Air Power Competence Centre, Owen Daniels, May 2021

Exhibit 9: How AI changes each stage of the OODA loop

Stage	Before AI	With AI/ML	New vulnerability
Observe	- Analysts manually reviewed video, imagery, radar and sensor feeds - Sensors outgrew the workforce, so subtle or short-lived indicators were often missed.	- Computer vision and signal processing models scan feeds from satellites, UAVs, radars and ground sensors - They flag objects, movements and anomalies so analysts can focus on what matters.	- Camouflage, decoys and spoofing can evade detection - Poisoned, outdated or unrepresentative training data can cause missed threats or false alerts.
Orient	- Intelligence, operations and logistics reports were reconciled through spreadsheets, maps and voice updates - Slow process, with headquarters often working from different versions of the situation.	- Data fusion tools build a shared, map based operational picture - Models correlate tracks and spot patterns, and language models summarise relevant reports.	- A clean display can make uncertain information look settled - Bias, wrong correlations or stale inputs can mislead commanders, especially when presented with confidence.
Decide	- Staff manually matched forces, weapons, timing and rules of engagement - Recommendations passed through several systems and approval levels before authorization.	- Decision support systems compare courses of action and match targets to effectors in one interface - The commander still tests assumptions and approves, modifies or rejects.	- Users may defer to machine recommendations that look precise or when tempo leaves no time to challenge them - Poorly framed objectives can make a system optimise the wrong outcome.
Act	- Orders went by voice, message or separate systems, with operators controlling platforms to the end - Preserved human control but was slower and relied on reliable communications.	- Approved tasks go directly from a common command interface - Autonomous systems can keep navigating or guiding when links degrade, within human set rules.	- Faulty software, lost links or changed conditions can lead systems to act on outdated instructions - Faster execution leaves less time to stop unintended actions or manage escalation.

Enablers of an effective accelerated loop

Battlefield advantage depends on combining decision speed with decision quality. AI can accelerate the decision cycle and strengthen situational awareness by helping commanders process more information within operational timelines. As an associate director of a security research centre has noted, the value of faster processing is greatest when it is supported by sound interpretation, contextual understanding and informed human judgement³⁹.

The following enablers can help military organisations realise these benefits:

- **Strong institutional and technical foundations enable faster decision cycles:** In April 2025, the U.S. GAO highlighted the value of a comprehensive framework for the DoD's joint C2 effort, including coordinated implementation across the Services and appropriate data access⁴⁰. Enterprise-wide architecture, common standards and clear governance allow the speed of individual tools to translate into integrated decision-making across the force.
- **Resilient orientation strengthens operational understanding:** Because orientation determines how information is interpreted, forces can strengthen this stage through diverse data sources, model validation, authentication and regular testing against deception techniques. During the 2020 Nagorno-Karabakh conflict, Azerbaijan's reported use of decoy aircraft against Armenian air defences illustrated the operational importance of corroborating sensor inputs before they are incorporated into the COP⁴¹.
- **Human authority supports controlled operations at machine speed:** When opposing AI-assisted systems operate at high tempo, clearly defined decision rights, escalation thresholds and human approval points help ensure that automated recommendations remain aligned with command intent. These arrangements allow military organisations to benefit from speed while maintaining informed oversight of consequential decisions.

The case study below demonstrates how AI-enabled systems can accelerate operational processes and how current, reliable data supports effective performance.

Case study 1 | Decision advantage of Maven Smart System | U.S./NATO

Maven Smart System (MSS)

U.S. Department of War's flagship AI-enabled battle-management and targeting platform, built as prime integrator on top of Project Maven. It is a classic example of use of AI to create decision advantage.

**USD
2.3 Bn**

FY2027 budget request for MSS and the Joint Fires Network



Multi Sensor data fusion increases accuracy

The gain came from integrating multiple systems into one, not from a single intelligent model

**USD
1.3 Bn**

MSS contract ceiling through 2029; raised by ~66 per cent in May 2025



Decision advantage

AI-enabled diversified sourcing gives the battlefield management systems better decision advantage

179

Distinct data sources used in CENTCOM's deployment of MSS in 2024



Faster targeting cycles

As AI analyses more data significantly faster than humans, sensing to targeting cycle reduces significantly

Sources: U.S. Army TRADOC G-2, January 2023. DefenseScoop, Brandi Vincent, 23 May 2025. Center for Strategic and International Studies (CSIS), Matt Mande and Gregory C. Allen, June 2026

39. Stuck between Real and Ideal: The OODA Loop and Military AI, LUFTLED, Owen J. Daniels, April 2024

40. Defense Command and Control: Further Progress Hinges on Establishing a Comprehensive Framework, U.S. Government

Accountability Office, April 2025

41. Lessons from the Nagorno-Karabakh 2020 Conflict, Center for Army Lessons Learned, Phillip Andrews, August 2021

Maven Smart System (MSS)

MSS is the U.S. Department of War's flagship AI-enabled battle-management and targeting platform, built as prime integrator on top of Project Maven, which commenced in 2017. It ingests satellite, UAV, radar and signal feeds; uses LLM to supply natural-language querying and analysis runs computer-vision models to detect objects, and lets users select a detected target, compare available strike assets and order the strike through a unified operational interface. It is a classic example of AI at decision advantage. The following enablers can help military organisations realise these benefits:

Scale and adoption

- In May 2025, the Pentagon raised the MSS contract ceiling by USD 795 million, from USD 480 million to nearly USD 1.3 billion through 2029. The FY2027 budget request includes USD 2.3 billion for MSS and the Joint Fires Network, and the Deputy Secretary of Defence directed that MSS become a programme of record⁴².
- As per a report cited by a strategic research centre, 179 distinct data sources were used in CENTCOM's deployment of MSS in 2024⁴³.
- On 25th March 2025, NATO finalized the procurement of a version of MSS, called MSS NATO for Allied Command Operations.

Key takeaway

- Data fusion speeds up the process. The gain came from integrating multiple systems into one, not from a single intelligent model.
- AI-enabled diversified sourcing gives the battle management systems a decision advantage.

2.5 AI at strategic and operational level of warfare – A framework

AI creates military value across all levels of warfare, but its role and operating model differ across the strategic, operational, and tactical edge. While strategic and operational applications derive value from integrating data, systems, and decision-making across the defence enterprise, tactical AI must deliver effectiveness under contested conditions where connectivity cannot be assumed. As modern battlefields become increasingly contested in the electromagnetic spectrum, military forces are recognising the need for AI capabilities that can operate both as part of a networked force and independently at the tactical edge when communications are degraded or denied.

At the strategic level, AI contributes to force generation, national resilience, and military preparedness through applications in defence manufacturing, logistics, intelligence analysis, cyber operations, infrastructure protection, and long-term capability development. At the operational level, AI enhances theatre-level planning, joint C2, targeting, battlespace awareness, and force coordination through multi-sensor data fusion and decision support. These applications derive much of their value from access to large volumes of information across multiple domains and organisations.

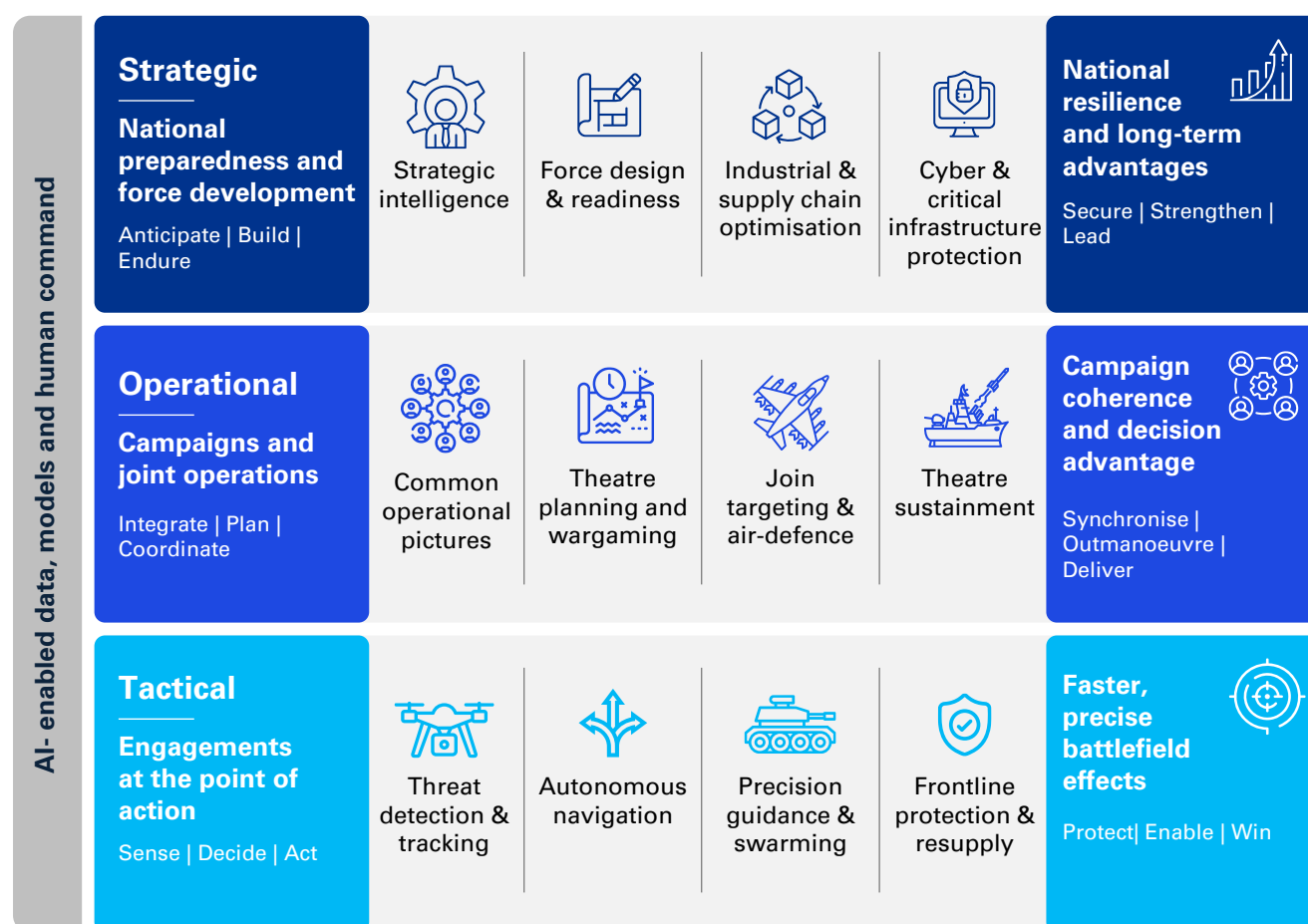
At the tactical level, however, AI serves a distinct purpose. Beyond improving target recognition, autonomous navigation, swarm coordination, and frontline situational awareness, AI enables platforms and weapon systems to continue operating effectively when disconnected from higher headquarters or wider communication networks. In contested environments where jamming, cyber-attacks, or bandwidth constraints may disrupt connectivity, AI-equipped platforms can maintain local situational awareness, adapt to changing conditions, execute mission objectives, and support decision-making with a greater degree of autonomy. This allows military operations to remain effective even when access to centralised C2 systems is temporarily denied.

42. Growing Demand" Sparks DOD to Raise Palantir's Maven Contract to More Than \$1B, DefenseScoop, Brandi Vincent, 23 May 2025

43. What Is Maven Smart System, and What Does It Do?, Center for Strategic and International Studies (CSIS), Matt Mande and Gregory C. Allen, June 2026

The framework therefore highlights the dual role for military AI. At the strategic and operational levels, AI functions primarily as a force integrator, connecting data, sensors, platforms, and decision-makers to improve the speed and quality of military decisions. At the tactical edge, AI acts as a force multiplier, enabling distributed platforms and units to sense, decide, and act with greater autonomy when operating in contested, degraded, intermittent, or disconnected environments. Together, these capabilities create a more resilient military architecture that can exploit the advantages of networked warfare while retaining effectiveness when networks are disrupted.

Exhibit 10: AI across the strategic, operational and tactical levels



The succeeding sections examine in detail the role of AI at the strategic and operational levels of warfare, where its primary contribution lies in enhancing national preparedness, force generation, joint-force coordination, decision support, and campaign execution. However, the increasing prevalence of contested, degraded, and communication-denied battlespaces has elevated the importance of AI at the tactical edge. The following sections also focus on this dimension, examining how capabilities such as terminal autonomy, autonomous swarms, and counter-drone systems can enable platforms and frontline units to sense, decide, and act with greater independence, sustaining operational effectiveness even when disconnected from wider C2 networks.

03

AI at the strategic level of warfare



At the strategic level AI continuously aids what a country is building, defending and sustaining, always – peacetime, grey-zone as well as during wartime.^{44 45}

While strategic AI is less visible than a tactical strike, it decides the course of the conflict and the preparedness of the systems to protect and sustain themselves. Unlike the operational and tactical levels which are dominated by active conflicts, the strategic work is constant throughout the peacetime, grey-zone competition as well as during wartime. It comprises national assets like an industrial base, which is built during peacetime, cyber defences that are regularly tested by intrusions that stop short of war. It also includes the protection of critical infrastructure which can be targeted during any phase. The assets can be broadly divided at strategic level into four arenas: the industrial base that manufactures and maintains equipment; the cyber domain; the critical national infrastructure- both civilian and military; and the extensive information space.^{46 47}

3.1 Manufacturing and sustainment

AI assists the military industrial base at four stages of design and simulation, production, supply chain and sustainment.^{48 49} During design and simulation, the digital models are tested in AI-enabled software before the physical procedure begins. AI assists in automated inspection, scheduling, and robotic support in the production phase. For supply-chain management, demands can be forecasted, and shortages can be spotted using an AI model. To sustain the industrial base, AI helps in planning maintenance and predicting failures. The readiness for war is built in peacetime, years before the engagement begins, and continues through it.

Exhibit 11: AI for manufacturing and sustainment

Stage	AI assistance	Contemporary example	Initiatives by India
 Design and simulation	Shortens design cycle by testing it in AI-enabled software before building	Modular design behind Arsenal- 1	Spiral development under draft DAP 2026
 Production	Automates production inspection, schedule management and AI-powered robotics	U.S. based defence technology's planned Ohio plant	Scaling up of drones and munition production across PSUs and private players
 Supply chain	Forecasts equipment demand, flags shortages and identifies single-vendor risks.	Commercial supply chains used for autonomous systems	Indigenisation lists and import substitution
 Sustainment	Predicts failure, keeps the inventory update and schedules maintenance	F-35 ODIN	Data rights on imported systems and platforms

44. Artificial Intelligence Strategy for the Department of War, U.S. Department of War, Pete Hegseth, January 2026

45. 2025 Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, U.S. Department of Defense, 23 December 2025.

46. How AI Protects Critical Infrastructure from Emerging Global Threats, World Economic Forum, Ricardo Villadiego, 13 May 2026

47. Pentagon Report Warns That China May Wield AI to Enhance 'Cognitive Domain Operations', DefenseScoop, Jon Harper, 30 November 2022

48. Anduril Announces New Facility to Streamline Autonomous Systems, Weapons Production, DefenseScoop, Mikayla Easley, 8 August 2024

49. F-35 JPO Finishes First Phase in Overhauling Logistics System, Air & Space Forces Magazine, Greg Hadley, February 2022

Case study 2 | F-35 ODIN and Arsenal: Sustainment and production | U.S.

F-35 ODIN and Arsenal – 1

Autonomic Logistics Information System (ALIS), the original logistics backbone of the global F-35 fleet faced usability issues and was afflicted by false alarms. In 2020, it was replaced by a cloud-native system called Operational Data Integrated Network (ODIN).

**USD
1.5 Bn**

Initial funding for Arsenal -1 to hyper scale production of autonomous systems in “tens of thousands”

**50
per cent**

Lower processing times than fielded ALIS servers

05

Months taken to move from solicitation to awarding of contract through the Replicator program



Multi Sensor data fusion increases accuracy

The gain came from integrating multiple systems into one, not from a single intelligent model



Decision advantage

AI-enabled diversified sourcing gives the battlefield management systems better decision advantage



Faster targeting cycles

As AI analyses more data significantly faster than humans, sensing to targeting cycle reduces significantly

Sources: Air and Space Forces Magazine 2020, 2022. Military & Aerospace Electronics, Feb 2026. DefenseScoop, Aug 2024

F-35: from ALIS to ODIN

ALIS, the original logistics backbone of the global F-35 fleet, was used to track spare parts and schedule and predict maintenance. It faced usability issues and was afflicted by false alarms. So, in 2020, it was replaced by a cloud-native system called ODIN. To keep control under military users, the government-written software was run on government-controlled hardware. The first hardware kits integrated with ODIN started getting installed at bases in 2022. As per the Joint Programme office, ODIN is designed to be more secure, enable predictive maintenance and generate fewer errors.^{50 51 52}

Arsenal-1: Software-defined production

In August 2024, a U.S. based defence technology company announced its plans of establishing a facility meant to “hyperscale” the production of munitions and autonomous systems in “tens of thousands” by incorporating its Lattice software, modular designs, and commercial supply chains. This was named Arsenal-1 and it was backed by a USD 1.5 billion funding round.⁵³

50. F-35 JPO Finishes First Phase in Overhauling Logistics System, Air & Space Forces Magazine, February 2022

51. F-35 Program Dumps ALIS for ODIN, Air & Space Forces Magazine, January 2020

52. Lockheed Martin to Provide 29 ODIN Maintenance and Software Kits to Help F-35 Crews Keep Combat Jets Flying, Military & Aerospace Electronics, January 2022

53. Anduril Announces New Facility to Streamline Autonomous Systems, Weapons Production, DefenseScoop, August 2024

Replicator: Government demand at speed

In August 2023, U.S. Defense Innovation Unit (DIU) announced its Replicator initiative. This was intended to field thousands of attritable autonomous systems in 24 months across various domains. In 2024, this initiative turned to counter-UAV systems. In August, the following year, DIU reported that it was on track for its planned quantities, but independent assessment of the claim remains unverified. In 2024, DIU was looking for proposals from private players for two software lines: resilient C2 structure and collaborative autonomy for swarms of a large number of uncrewed assets. Within five months, the solicitation moved to the awarding of contract.^{54 55}

Key takeaways

- Readiness depends on the control of software and data⁵⁶. While ALIS had experienced the risk of infected data, ODIN's infrastructure allows the operator to control the code.⁵⁷
- Mass is enabled by incorporating commercial supply chain and modular design. To achieve the results faster, design has to be modified and the AI models, sourced from multiple vendors.
- Clear demand signals drive innovation. The success of Replicator underscores the importance of a well-defined operational requirement and strong leadership commitment. Start-ups are more likely to engage when the procurement priorities are explicit, and there's a credible pathway to adoption.

3.2 Cyber: AI on both sides of the keyboard

Cyber operations are among the domains most susceptible to AI disruption because their core inputs, data, software, network traffic, and code, are inherently digital. Unlike physical battlefields, where information must first be collected and transmitted, cyber environments already generate the structured data required to train, deploy, and continuously improve AI systems. As a result, AI is accelerating both offence and defence, creating a dynamic competition in which each side seeks to outpace the other through automation, scale, and speed.

On the offensive side, AI enhances reconnaissance, vulnerability discovery, exploit development, phishing, and intrusion operations by automating tasks that previously required significant human expertise and time. Threat actors can use AI to analyse target networks, identify weaknesses, generate exploitation code, and conduct operations at a scale that would be difficult to achieve manually. On the defensive side, AI strengthens cyber resilience through continuous network monitoring, anomaly detection, automated threat hunting, vulnerability remediation, and machine-speed incident response. Consequently, the contest increasingly revolves around which side can detect, analyse, and respond faster.

Much of this competition unfolds below the threshold of conventional warfare, making cyber operations one of the most prominent instruments of grey-zone competition. Unlike kinetic attacks, cyber operations can disrupt critical infrastructure, steal sensitive information, undermine public confidence, or impose economic costs while avoiding direct military confrontation and often obscuring attribution. AI further amplifies these characteristics by lowering the barriers to conducting sophisticated cyber operations and reducing the time between vulnerability discovery and exploitation.

Recent developments illustrate both sides of this technological race. AI-enabled cyber campaigns have demonstrated the ability to automate large portions of offensive operations, while initiatives such as U.S.'s AI Cyber Challenge (AIxCC) have showcased how AI can be harnessed to identify and remediate software vulnerabilities before they are exploited⁵⁸. Together, these trends suggest that future cyber advantage will increasingly depend on the ability to operate at machine speed, secure software supply chains, and maintain trust in AI-enabled systems.

54. DOD Replicator Initiative: Background and Issues for Congress (IF12611), Congressional Research Service, January 2026

55. Defense Innovation Unit. Replicator. accessed Sep 2026

56. F-35 JPO Finishes First Phase in Overhauling Logistics System, Air & Space Forces Magazine, February 2022

57. Lockheed Martin to Provide 29 ODIN Maintenance and Software Kits to Help F-35 Crews Keep Combat Jets Flying, Military & Aerospace Electronics, January 2022

58. DARPA AI Cyber Challenge Aims to Secure Nation's Most Critical Software, Defense Advanced Research Projects Agency (DARPA), August 2023

Case study 3 | Cyber Dome | Israel

Cyber Dome: building an AI powered national cyber shield

Cyber Dome is a national cyber defence architecture modelled on the Iron Dome air defence system. It uses big data and AI to detect anomalies, separate genuine threats from large volumes of threat intelligence.

2022

Year the INCD announced Cyber Dome as a national, AI driven proactive defence



From organisational to national defence

Cyber defence is shifting from protecting single organisations to one nationwide shield that constantly monitors critical assets

3x

Rise in the intensity of cyberattacks on Israel since the start of the Gaza conflict



Civil military collaboration drives superiority

Combining military intelligence expertise with civilian cyber agencies creates visibility no single body could achieve alone

700

Cyberattacks thwarted by Israel's Shin Bet in 2024, as attacks rose fivefold after October 7



AI is critical at scale

Threat volume and speed now exceed human capacity, so AI is needed to identify, rank and respond to threats in real time

Sources: Israel National Cyber Directorate, via JNS, 28 June 2022. Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), Rohit Kumar Sharma, 3 July 2024. Tazpit Press Service (TPS), Pesach Benson, 31 December 2024

Israel's Cyber Dome is one of the most ambitious attempts at creating an AI-enabled cyber defence architecture at a national scale. This architecture can detect, analyse and mitigate cyber threats in real time. Cyber Dome aims to provide a digital equivalent of Israel's missile-defence system- Iron Dome. Its key role is to protect Israel's national cyber parameter infrastructure against cyber campaigns, espionage, ransomware and disruptive attacks^{59 60}.

Unlike legacy cybersecurity systems that operate at the organisational level, this architecture intends to generate country-wide cyber-defence ecosystem. It integrates expertise from multiple security stakeholders.

It leverages big-data analytics to process volumes of cyber telemetry, AI-powered anomaly detection and threat identification, real-time intelligence sharing across government, military, and civilian organisations. Cyber Dome also automates threat correlation across sectors to provide national-level cyber situational awareness and coordinate an incident response. Cyber Dome can be integrated with Israel's military cyber and intelligence ecosystem, specifically capabilities developed by Unit 8200. Architecture derives its advantage from a fusion of military-grade intelligence and analytics and civilian cyber protection infrastructure.

59. We Are Promoting a National Cyber-Dome, Israel National Cyber Directorate, Gaby Portnoy, June 2022

60. Israel National Cyber Directorate, Government of Israel, accessed October 2026

Key takeaways

- Cyber defence is evolving toward national integrated air-defence models: This architecture demonstrates how cyber defence is moving from organisation-level protection toward a centralized, nation-wide defensive architecture that constantly monitors and defends critical national assets⁶¹. Cyber Dome aggregates data from state agencies, telecommunication providers, critical infrastructure operators and security organisations into a COP. This enables cross-sector visibility which is difficult to achieve independently⁶².
- Information superiority requires civil-military collaboration: Cyber Dome's effectiveness stems from the combination of military operational expertise and civilian cyber-defence agencies.
- AI is becoming critical for defensive operations at scale: The scale, velocity and sophistication of current day cyber threats exceed human analytical capacity. Cyber Dome demonstrates how AI enables real-time identification, ranking and response across the national cyber-defence ecosystem.

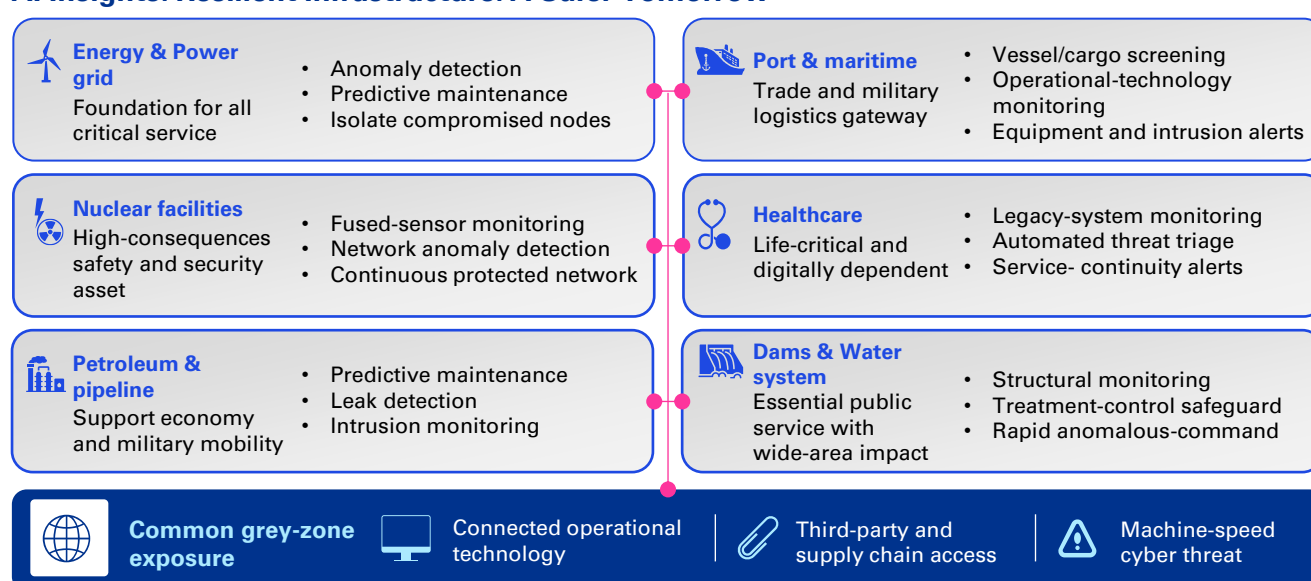
3.3 Protecting national assets: energy, ports, nuclear, health, fuel and dams

Critical national infrastructure remains a high-value target across all three phases. During peacetime, it can be probed, vulnerabilities can be mapped and system interdependencies can be noted; In the grey-zone environment, infrastructure may be subjected to disruption just enough to signal intent, cause economic or political damage, without inviting a military response; once a war has begun, these assets become direct targets, as dismantling them can generate cascading effects across the society, economy and the military. The same convergence of information technology (IT) and operational technology (OT) that makes this infrastructure more resilient, makes them vulnerable.^{63 64 65}

Assets such as energy infrastructure, ports, nuclear facilities, healthcare, fuel networks and water systems are essential to national resilience, economic stability and military operations. AI is increasingly being used to strengthen the resilience of these assets through real-time anomaly detection, automated monitoring of OT environment, predictive maintenance and faster incident response.

Exhibit 12: AI-enabled protection of critical infrastructure

AI Insights. Resilient Infrastructure. A Safer Tomorrow



61. As Iranian Hackers Grow More Skilled, Israel Builds 'Cyber Dome' to Protect Itself, The Times of Israel, Agence France-Presse (AFP) and Times of Israel Staff, May 2024

62. We Are Promoting a National Cyber-Dome, Israel National Cyber Directorate, Gaby Portnoy, June 2022

63. AI Can Protect Critical Infrastructure from Emerging Threats,

World Economic Forum, May 2026

64. NCIIIC Explained: Safeguarding India's Critical Infrastructure, UpGuard, 2026

65. Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign, Anthropic, November 2025

Civilian and military users are increasingly relying on the same strategic infrastructure; hence, resilience largely depends as much on integration as on protection. India's dual-use assets like satellite constellations, compute infrastructure, ports and other logistics corridor, support both military and economic objectives. These are supported by initiatives such as PM Gati Shakti, National Logistics Policy and the Defence Space Agency⁶⁶. In this context, AI-enabled cyber defence capabilities can be used as a common layer across shared assets to provide unified threat visibility, quicker response time and better operational efficiency. A siloed approach for civilian and military security architectures may arise the concern of blind spots and duplicative investments.

3.4 Compute, space and the cognitive domain

The military implications of AI extend well beyond autonomous platforms and decision-support systems. Increasingly, strategic competition is shifting towards the underlying digital infrastructure, data ecosystems, and information environments that enable AI-enabled military operations.⁶³ As a result, the future battlespace will encompass not only physical domains, but also the computational, informational, and cognitive foundations of military power.

Compute Infrastructure and data centres

AI capabilities are fundamentally dependent on access to computing power, data storage, connectivity, and reliable energy infrastructure. These assets form the backbone of modern military AI systems, enabling model training, data processing, and real-time operational support. Consequently, digital infrastructure is emerging as both a strategic enabler and a high-value target. Recent conflicts have demonstrated that attacks on data centres, communications infrastructure, and energy networks can disrupt military operations as effectively as attacks on conventional military assets. In the AI era, compute capacity became a critical element of national security and military preparedness.

Space based ISR

The rapid expansion of satellites, unmanned systems, and networked sensors has created an unprecedented volume of operational data. However, collecting information alone no longer guarantees advantage. Military effectiveness increasingly depends on the ability to process, triage, analyse, and distribute intelligence at speed. AI plays a central role in this process by automating imagery analysis, identifying anomalies, prioritising targets, and converting raw sensor feeds into actionable intelligence. As the volume of ISR data continues to grow, AI-powered analytics will become indispensable for maintaining situational awareness and decision superiority.

The cognitive domain

Beyond physical and digital infrastructure, AI is increasingly shaping the cognitive dimension of warfare, the contest to influence perceptions, decision-making, public opinion, and strategic narratives. Advances in generative AI, LLMs, and synthetic media have significantly lowered the cost and increased the scale of information operations. These capabilities can be used to create persuasive content, amplify narratives, target specific audiences, and conduct influence campaigns with unprecedented speed and precision. As a result, AI is expanding the scope of grey-zone competition by enabling states and non-state actors to pursue strategic objectives below the threshold of conventional conflict. In this environment, the ability to defend information integrity and build societal resilience may become as important as traditional military capabilities.

66. Need for India to Pursue a Civil-Military Fusion, Raksha Anirveda, A. Mirza, 2026



04

AI at the operational level of warfare



While the previous section examined AI's role in peacetime preparedness, industrial mobilisation, and grey-zone competition, this section focuses on its application during active military operations. Modern campaigns are executed simultaneously across land, air, maritime, cyber, and space domains, creating an unprecedented volume of information for commanders to process.

Historically, operational effectiveness was constrained by the time required to collect intelligence, develop plans, coordinate forces, and sustain logistics. As the number of sensors, platforms, and operational actors increased, decision-making became increasingly complex. AI addresses this challenge by fusing large volumes of data from diverse sources, transforming them into a coherent COP, and generating decision support for commanders.

At the operational level, AI's most significant contribution is therefore not autonomous action, but decision advantage. By accelerating the flow from sensor to commander, AI helps military organisations understand the battlespace faster, evaluate options more effectively, and coordinate actions across multiple domains.

4.1 Joint Command and Control (C2)

Modern military operations are increasingly conducted across multiple domains, involving a large number of sensors, platforms, headquarters, and service components operating simultaneously. Satellites, airborne early warning systems, drones, radars, electronic intelligence assets, naval platforms, and ground-based sensors collectively generate vast volumes of information. While the availability of data has increased dramatically, the ability of commanders to process, correlate, and act upon it has become the principal challenge.

AI addresses this challenge by transforming data into actionable understanding. It can automatically fuse inputs from disparate sensors, identify patterns, remove duplicate tracks, resolve conflicting reports, and generate a coherent COP. Rather than requiring staff officers to manually collate information from multiple systems, AI enables commanders to access a near real-time view of the operational environment, highlighting the most relevant developments and potential threats.

Beyond situational awareness, AI improves the quality and speed of decision-making. It can correlate intelligence from multiple sources, identify emerging trends, assess likely adversary intentions, and present decision-makers with prioritised courses of action. This helps commanders focus their attention on critical decisions rather than routine information processing, compressing the observe-orient-decide-act (OODA) loop.

AI-enabled C2 is particularly valuable in joint and integrated operations. By providing a shared operational picture across land, air, maritime, cyber, and space domains, it improves coordination between services and reduces the risk of fragmented decision-making. The result is greater synchronisation of operations, faster allocation of resources, and more effective employment of combat power across the theatre.

Ultimately, AI's contribution to Joint C2 is not to replace commanders, but to reduce the cognitive burden of managing complex multi-domain operations. Its value lies in converting large volumes of fragmented data into shared understanding and timely decisions, thereby creating a decisive advantage in operational tempo and coordination.

4.2 Targeting and kill-chain compression

The effectiveness of military operations increasingly depends on how rapidly forces can move from detecting a target to engaging it. Traditionally, this process, often referred to as the sensor-to-shooter chain or kill chain, involved multiple sequential stages: detecting a target, validating its identity, assessing its priority, assigning a suitable weapon, obtaining command approval, executing the strike, and evaluating the outcome. Each stage required human intervention, introducing delays that could allow targets to relocate, disperse, conceal themselves, or conduct their mission before engagement.

AI compresses this decision cycle by automating many of the data-processing and analytical tasks that sit between sensing and action. It can process large volumes of imagery, video feeds, signals intelligence, and sensor data simultaneously, identifying objects of interest and alerting operators in near real time. Rather than requiring analysts to manually review vast quantities of information, AI enables rapid target detection, classification, and tracking across multiple domains.

Beyond detection, AI contributes to target prioritisation and weapon-target matching. By analysing factors such as target value, threat level, location, weapon availability, collateral damage considerations, and likelihood of success, AI can recommend optimal engagement options for commanders. This allows scarce strike assets to be allocated more effectively and reduces the time required to develop and approve engagement plans.

AI also enhances the ability to maintain persistent target tracks. Modern battlefields are characterised by highly mobile and time-sensitive targets, including missile launchers, command posts, air-defence systems, and logistics nodes. AI-enabled tracking systems can correlate observations from multiple sensors, predict movement patterns, and maintain track continuity even when targets temporarily disappear. This improves the probability of successful engagement while reducing the burden on human operators.

A further contribution comes after the strike. AI-assisted battle damage assessment (BDA) can rapidly analyse post-strike imagery and sensor data to determine whether the intended effects have been achieved, enabling commanders to decide whether re-engagement is required and redirect resources accordingly.

The cumulative effect is a significant compression of the kill chain. AI enables forces to detect, decide, and engage faster than traditional command processes, increasing operational tempo and reducing the adversary's opportunity to react. At the operational level, the advantage lies not simply in finding more targets, but in converting information into effects more quickly than the opponent can adapt. In modern warfare, the side that can shorten the sensor-to-shooter cycle often gains a decisive advantage in both initiative and operational effectiveness.

4.3 Air and missile defence

Air and missile defence are one of the most time-sensitive military missions, requiring operators to identify and respond to multiple threats within seconds. Modern air-defence networks must track aircraft, missiles, drones, and loitering munitions simultaneously, often during large-scale saturation attacks.

AI enhances these systems by fusing inputs from multiple sensors into a unified air picture, improving situational awareness and reducing decision time. It can automatically detect, classify, and prioritise threats based on their trajectory, speed, likely target, and level of danger, enabling operators to focus on the most critical engagements.

AI also supports engagement management and weapon-target matching, helping commanders allocate the most appropriate interceptor or defence system to each threat. This is particularly valuable during saturation attacks, where manual decision-making can become overwhelmed by the volume and speed of incoming targets.

In addition, AI enables more effective layered air defence by coordinating sensors and effectors across the network. This allows lower-cost systems to engage routine threats, preserving high-value interceptors for more dangerous targets and improving the overall cost-effectiveness of the defence.

India's Akashteer programme reflects this transition towards increasingly integrated and automated air-defence networks. By connecting sensors, command nodes, and weapon systems into a COP, such systems seek to accelerate decision-making and strengthen the effectiveness of air and missile defence.

At the operational level, AI's primary contribution is to shorten the timeline between detection and engagement, enabling forces to respond to threats faster, at greater scale, and with improved coordination.

Case study 4 | Decision advantage of integrated air defence system | India

Operation Sindoor: Akashteer and SANJAY, India's own fusion layer under fire

Akashteer, an automated air defence control and reporting system, fuses radar and sensor feeds into a COP. SANJAY combines ground and aerial sensor inputs and uses edge processing, hence analysis continues when networks are jammed.

300 to 400

Pakistani drones launched in a single night against Indian military and civilian sites

36

Locations from Leh to Sir Creek targeted in that attack

06

Akashteer nodes deployed on the western front



The network delivered the result

Many sensors combined into one air picture, passed down to the units that fire, mattered more than any single radar or launcher



Two Services, one air picture

Linking Akashteer with the Air Force's command system let the Army and the Air Force engage against the same tracks at the same moment



Analysis continued when links failed

Edge processing kept the surveillance picture working even when networks were jammed or cut

Sources: Ministry of External Affairs (MEA) special briefing, 9 May 2025. Deccan Herald, Kalyan Ray, 14 May 2025. Press Information Bureau (PIB), 16 May 2025

Operation Sindoor: Akashteer and SANJAY

India has demonstrated that it can build and operate its own fusion layer under fire. Akashteer and SANJAY carried an air defence that neutralised hundreds of Pakistani drones and missiles over several nights from 7 May 2025⁶⁷.

Akashteer is an automated air-defence control and reporting system, built by jointly developed by multiple Indian defence research and manufacturing units⁶⁸. It fuses radar and sensor feeds into a single air picture, distributes that picture to the lowest Army air-defence units, and connects to the Air Force's Integrated Air Command and Control System so that the two Services work from one track⁶⁹. It was used at six nodes on the western front, and in the coordinated aerial attack of 9–10 May 2025 it intercepted and neutralised every inbound projectile⁷⁰. The advantage came from the network rather than from any single radar or launcher.

67. Operation Sindoor Accelerated Indigenous Drone Development and Counter-Measures, The Tribune, Vijay Mohan and Tribune News Service, May 2026

68. Operation Sindoor: How AI-Powered Air Defence System Akashteer Shielded India, Inc42, Tapanjana Rudra, May 2025

69. Operation Sindoor: Indian Army's Home-Grown Akashteer Air

Defence Systems Block Pakistan's Air Adventure, Deccan Herald, May 2025

70. Akashteer: The Unseen Force Behind India's New War Capability, Press Information Bureau, Ministry of Information and Broadcasting, Government of India, Santosh Kumar, Ritu Kataria and Kritika Rane, May 2025

SANJAY addresses surveillance, it fuses ground and aerial sensor input into a COP and feeds the Army's Decision Support System. It can be linked with the Army's Trinetra system and uses edge processing, so that analysis continues when networks are jammed or cut⁷¹. A counter-drone exercise held in border areas on 26–28 April 2025 had rehearsed the saturation tactic that followed, and radars were operated intermittently during the attacks so that positions were not disclosed⁷².

Key takeaways

- The network delivered the result: No single radar or launcher stopped the attack. Readings from many sensors were combined into one picture of the air situation, and that picture was passed down to the units that actually fire. The advantage came from joining the parts together rather than from the performance of any one of them.
- Two services, one air picture: Akashteer was connected to the Air Force's C2 system, so the Army and the Air Force saw the same tracks at the same moment. That removed the need to reconcile two separate accounts of what was in the air and allowed both services to engage against a single shared picture.
- Analysis continued when links failed: SANJAY processes sensor data on the equipment itself rather than sending everything back to a central computer. When networks were jammed or cut, the surveillance picture kept working. That matters because degrading an opponent's communications is among the first things any adversary will attempt.

4.4 Planning, wargaming and logistics

Operational success depends as much on sustaining forces as on employing them in combat. AI supports operational planning by evaluating multiple courses of action, modelling potential outcomes, and identifying risks before decisions are made. This enables commanders to compare alternatives and select the most effective approach.

In logistics, AI can forecast requirements for fuel, ammunition, spare parts, and maintenance support, helping identify shortages and bottlenecks before they affect operations. It can also enable predictive maintenance, improve equipment availability and reduce downtime.

By improving planning, resource allocation, and sustainment, AI helps commanders maintain operational tempo and generate combat power over prolonged campaigns.

Taken together, these applications demonstrate that AI's primary value at the operational level is to enhance their understanding of complex environments, shorten decision cycles, and improve the coordination of multi-domain operations.



71. India's Use of Artificial Intelligence During the Indo-Pak Four-Day Crisis, The Diplomat, Usman Haider and Komal Khan, October 2025

72. "We Anticipated This": Did a Counter-Drone Exercise to Tackle Attacks at Army Chief's Behest, Says Top Army Air Defence Officer, The Tribune, Asian News International (ANI), May 2025

Case study 5 | DELTA and Avengers | Ukraine

Ukraine's DELTA and Avengers AI: A bottom-up Battle Management System

Delta, Ukraine's situational awareness and battle-management platform is employed across command levels from frontline units to operational commands.

70% Of observed enemy vehicles and equipment identified and classified within seconds



COP is a force multiplier

Deploying a single system across tactical and operational echelons improves coordination and decision making

66% Reduction in time taken from detection of target to engagement



User-led development drives adoption

Software written and iteratively refined tends to evolve faster and align better with operational demands as compared to top-down designs

12000 Units of enemy vehicles/equipment detected weekly by Avengers AI through video analysis



Data is a strategic asset

Battlefield data when turned into a controlled national asset and shared with the industry can give a competitive advantage

Sources: U.S. Army TRADOC G-2, January 2023. | DefenseScoop, Brandi Vincent, 23 May 2025. | Center for Strategic and International Studies (CSIS), Matt Mande and Gregory C. Allen, June 2026

Ukraine's DELTA and Avengers AI: a bottom-up battle-management system

DELTA, Ukraine's situational awareness and battle-management platform is employed across command levels from frontline units to operational command. By integrating drone feeds, sensor data and intelligence inputs into a real-time COP, accessible via tablets and smart phones including offline devices, Delta has significantly accelerated decision making. Reportedly, the time taken from detection of the target to its engagement has been reduced from 20-30 minutes to three to ten.

The AI layer

Key enabler of Delta's effectiveness is the computer-vision module, Avengers. It automates the target detection and classification of drone and surveillance imagery. According to Ukraine's digital ministry, the system identifies and classifies about 70 per cent of the observed enemy vehicles and equipment within seconds. It leverages a dataset, which it claims to be world's largest manually labelled dataset of enemy hardware⁷³.

To further strengthen its edge, Ukraine launched the Brave1 Dataroom in January, this year. It is a state-controlled platform which gives defence companies access to real visuals and thermal battlefield data to train and develop their AI models.

Key takeaways

- COP is a force multiplier. Deploying a single system across tactical and operational echelons improves coordination and decision-making.
- User-led development drives adoption. Software written and iteratively refined tends to evolve faster and align better with operational demands as compared to top-down designs.
- Data is strategic asset. Ukraine's experience underlines that proprietary battlefield data when turned into a controlled national asset and shared with the industry can give a competitive advantage.

73. Enemy Equipment Detected in 2 Seconds: The Ministry of Defence Showcased DELTA and Avengers Systems at the London Defence Conference, Ministry of Defence of Ukraine, May 2025

4.5 AI at tactical edge

At the tactical edge, AI enables low-cost platforms to independently sense, process, and engage targets in contested environments, while allowing defenders to detect, assess, and respond to threats at comparable speed and scale.

The tactical level is where AI's impact on the economics of warfare becomes most apparent. Historically, neutralizing a radar system or an armoured vehicle at stand-off range required precision-guided munitions costing hundreds of thousands of dollars.

Today, low-cost uncrewed systems costing only a few hundred dollars can achieve similar battlefield effects with sufficient reliability to alter force planning assumptions, and the software that lets it finish the attack unaided adds only a 10th fraction to its price.⁷⁴ As a result, the combination of inexpensive mass and intelligent autonomy has fundamentally shifted cost-exchange dynamics in favour of the attacker. In such an environment, defenders may successfully intercept waves of low-cost UAVs, but relying on high-cost interceptors against cheap, mass-produced threats can create an unfavourable exchange ratio that becomes increasingly difficult to sustain over time.

Evidence from Ukraine shows both the opportunity and its limits. Tactical uncrewed aircraft account for 60–70 per cent of damaged and destroyed Russian systems. Yet 60 to 80 per cent of such drones never reach their targets, and electronic warfare is the main cause.⁷⁵ The challenge lies in closing the gap between the aggregate effects these systems can generate and the reliability of each individual sortie.

4.5.1 Terminal autonomy

At the tactical edge, autonomy is increasingly a response to electronic warfare rather than a substitute for human operators. The critical weakness of many low-cost drones is the control link connecting them to the operator. By enabling onboard target recognition and terminal guidance, AI removes this vulnerability from the final phase of engagement, allowing the platform to complete its mission despite jamming or signal loss. Because the task is computationally narrow, requiring recognition of specific target classes rather than comprehensive battlefield understanding, the capability can be delivered on low-cost hardware. Commercial advances in computer vision have further reduced barriers to adoption, making autonomous terminal guidance one of the most economically attractive applications of military AI.

A Ukrainian system now classifies roughly 70 per cent of enemy vehicles in video in as little as 2.2 seconds.⁷⁶ Terminal autonomy does not eliminate vulnerability; it changes its location. As communications links become less critical to mission success, electronic jamming yields diminishing returns and the contest shifts to the AI model itself. Adversaries can exploit this dependency through camouflage, decoys, signature manipulation, and other forms of deception that are often cheaper and more scalable than electronic attack. Consequently, battlefield advantage increasingly depends on assets that cannot be rapidly acquired in crisis: extensive labelled datasets of adversary targets and a robust test-and-evaluation framework capable of proving model performance under realistic and adversarial conditions. In the age of autonomous warfare, data quality and model assurance become as important as the platforms that carry them.

74. 'Fire and Forget': Ukraine Rolls Out FPV Drones With Autonomous Terminal Guidance, Kyiv Post, September 2025

75. Tactical Developments During the Third Year of the Russo-Ukrainian War, Royal United Services Institute (RUSI), Jack Watling and Nick Reynolds, February 2025

76. 2 Seconds and the Target Is Identified: How the Digital Ecosystem of the Armed Forces Works, Ministry of Digital Transformation of Ukraine, September 2025

4.5.2 Swarms and collaborative autonomy

Mass and collaboration are often conflated, but they represent distinct capabilities. Mass involves deploying large numbers of uncrewed systems against a common objective, whereas collaborative autonomy enables platforms to share information, allocate tasks, and adapt collectively as losses occur. While both can produce similar battlefield effects, their constraints differ significantly.

Mass is primarily limited by industrial and organisational factors such as production capacity, logistics, launch infrastructure, and operator availability. Collaboration, by contrast, depends on resilient communication, onboard processing, and autonomous decision-making. A swarm reliant on continuous control links remains vulnerable to electronic warfare; effective swarming therefore requires platforms to operate independently when disconnected.

As a result, terminal autonomy is a prerequisite for collaborative autonomy rather than an alternative to it. Coordination software can enhance effectiveness, but meaningful swarm capability ultimately depends on fielding autonomous systems at scale.

For defenders, however, the distinction is less important than the economics of engagement. Whether enabled by software coordination or sheer numbers, mass overwhelms defences through saturation. The critical metrics are therefore cost-exchange ratios and defensive endurance, not simply interception success rates. A defence that defeats every incoming threat may still be lost if it exhausts resources faster than the attacker.



Case study 6 | Operation Spiderweb | Ukraine

Operation Spiderweb: Mass and low cost without much AI

On 1 June 2025, FPV drones launched from trucks parked near five Russian airbases struck strategic bombers and other aircraft, after about 18 months of preparation. Each drone had its own pilot, and the control arrangement combined autonomous algorithms with manual intervention.

117 FPV drones launched from trucks parked near five Russian airbases



Human control caps the numbers

Each drone in this attack had its own pilot, so the size of the raid was set by how many trained people could be put behind controllers

40 Adversary aircraft struck as per the Ukrainian officials



Autonomy protected aircraft, not the group

Drones that lost signal flew to a pre-planned target and detonated on contact. Autonomy safeguarded each aircraft individually. It did not let the group re-target, reallocate aim points or compensate when members were lost

18 Months of planning before the operation was executed



Coordinated swarms remain unfielded

What exists today is many drones flown by many people to a common plan, which is an achievement of production, logistics and training rather than of autonomy

Sources: Janes, June 2025 | Euronews, June 2025.

Operation Spiderweb: mass and low cost without much AI

Numbers can break a defended target, but a force assembled out of individually piloted aircraft is slow to build and limited once it is committed. On 1 June 2025, 117 FPV drones launched from trucks parked near five Russian airbases struck strategic bombers and other aircraft, after about 18 months of preparation⁷⁷. Each drone had its own pilot, and the control arrangement combined autonomous algorithms with manual intervention: drones that lost their signal continued along a pre-planned route to a designated target and detonated on contact⁷⁸. Autonomy was therefore present, but only inside each aircraft. Nothing coordinated the group.

The operation shows what numbers achieve against a defence configured for something else. Moving the launch point to within a few kilometres of the targets reduced warning time to seconds and rendered range, interceptors and early-warning radar largely irrelevant. Saturation did the rest. A defence able to engage a handful of targets at a time cannot answer dozens arriving together, whatever the quality of each individual interception. Ukrainian officials put the number of aircraft struck at 40⁷⁹.

77. Operation Spiderweb: Covert Drone Strike Inside Russia, Janes, June 2025

78. Kyiv Releases New Drone Footage of Operation Spiderweb as More Details Emerge, Euronews, June 2025

79. How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare, Center for Strategic and International Studies (CSIS), Kateryna Bondar, June 2025

It shows what assembling mass this way costs. One pilot per aircraft meant the size of the raid was bound by the number of trained people who could be put behind controllers, and concealing and moving the launch vehicles consumed some eighteen months. The autonomy that was present served as a fallback for a single drone that had lost contact, not as a means of dividing work between drones. Collaborative autonomy is the next increment: aircraft that share a target set, allocate aim points among themselves and redistribute tasks as members are lost would require neither one operator each nor a continuous connection. No force has yet fielded that capability at scale, which is why operations of this kind still rest on people and planning.

Key takeaways

- Human control caps the numbers: Each drone in this attack had its own pilot, so the size of the raid was set by how many trained people could be put behind controllers. Software that lets a group divide an attack among its own members is what lifts that ceiling, and that is a different capability from flying one aircraft well.
- Autonomy protected aircraft, not the group: Drones that lost their signal flew on to a pre-planned target and detonated on contact, so the attack did not depend entirely on a continuous connection. That autonomy safeguarded each aircraft individually. It did not let the group re-target, reallocate aim points or compensate when members were lost.
- Coordinated swarms remain un-fielded: No force has yet shown large numbers of aircraft genuinely organising themselves in combat. What exists today is many drones flown by many people to a common plan, which is an achievement of production, logistics and training rather than of autonomy.

Case study 7 | Swarms drone | India

India's emerging AI-enabled swarm drone capability

At the January 2021 Army Day parade, Indian Army showcased around 75 drones flying coordinated mock missions.

75

Drones flown in a coordinated swarm demonstration at Army Day 2021



From platforms to networks

Swarms draw their strength from autonomy, software and collaborative decision making, not from any single drone.

USD
15 Mn

Contract for 100 swarm UAVs under the A-SADS programme



Cost effective saturation

Large numbers of low-cost drones can overwhelm air defences, shifting the cost balance in the attacker's favour.

50 km

Operational radius, with 3 hours endurance and a 20,000 ft service ceiling suited to high altitude borders



Human machine teaming is the next edge

Concepts such as manned unmanned teaming will link combat aircraft with drone swarms to compress the decision cycle.

Sources: *The Week*, 15 January 2021 | *Janes*, Akhil Kadidal, 6 March 2023 | *ThePrint*, Snehash Alex Philip, 13 February 2023

India's emerging AI-enabled swarm drone capability

In January 2021, India demonstrated its swarm-drone capability during the Indian Army Day Parade. 75 autonomous drones coordinated and brought out simulated reconnaissance and strike mission by integrating AI-enabled swarming algorithms along with automated target recognition. The demonstration represented one of the earliest military swarm-drone showcased by Indian armed forces⁸⁰.

Following these trials, in September a USD 15 million contract was awarded by the Indian Army to an Indian firm to supply 100 AI-enabled swarm drones. This contract was given under emergency procurement procedure that was introduced post the India-China border conflict. This system was designated as Autonomous Surveillance and Armed Drone Swarm (A-SADS). The swarm combines heterogeneous UAVs capable of autonomously collaborating for ISR purposes, communications relay and carrying out precision kinetic missions. The AI-powered coordination algorithm allows the swarm to divide tasks among the individual drones, share information and carry out missions even if individual platforms disconnect from the swarm.

As per the firm, the A-SADS system provides an operational radius of 50 km and up to three hours of endurance. It is designed to suit India's high altitude border environments, hence can operate at altitudes up to 20,000 feet. Apart from being able to support both surveillance and strike operations, the swarm can enable future concepts like Manned-Unmanned Teaming (MUM-T)⁸¹.

India's premier aerospace and defence public sector and the same firm are jointly developing air-launched swarm concept through the Combat Air Teaming System (CATS) programme. CATS has Air Launched Flexible Asset-Swarm (ALFA-S) system to deploy multiple autonomous drones from a host aircraft. This can overwhelm adversary air-defence networks and collaboratively strike high-value targets⁸².

Key takeaways

- AI is shifting India's focus from platform-centric to network-centric warfare: Drone swarms derive their efficacy from autonomy, software and collaborative decision making rather than individual system performance.
- Swarms offer a cost-effective way to saturate adversary defences: Unlike conventional attack aircraft or missile systems, swarm drones can overwhelm air-defence networks through distributed and scaled attacks, shaping favourable economic outcomes for the attacker.
- Future battlefield edge will depend on human-machine teaming: Concepts such as MUM-T which focus on the collaboration of combat aircraft and integrated drone network will shape the future battlefield landscape. They create AI-enabled kill chain that compress the decision cycle thereby improving battlefield responsiveness^{83 84}.

4.5.3 Counter-drone at machine speed

Counter-drone defence is fundamentally an economics problem as a defender can intercept every incoming drone and still lose if each engagement costs more than the threat it defeats. The objective is therefore to minimise cost per interception through a layered defence architecture, reserving expensive effectors for high-value threats while relying on lower-cost systems for routine engagements.

Speed is critical as under saturation attacks, detection, identification, decision, and engagement must occur within seconds and often across multiple targets simultaneously. This requires significant automation, with human operators increasingly supervising the process rather than directing every engagement. In practice, rules of engagement and system design become the primary mechanisms of control.

80. Drone Swarm Technology: India's Autonomous UAV Swarms, India Defence Wire, IDW Bureau, accessed October 2026

81. Indian Army Receives 'Swarming' UAVs, Janes, Akhil Kadidal, 6 March 2023

82. Drone Swarm Technology, India Defence Wire, IDW Bureau, accessed October 2026

83. Army Orders 100 Swarm Drones from Indian Startup, Livelist, Team Livelist, September 2021

84. Drone Swarm Technology, India Defence Wire, IDW Bureau, accessed October 2026

Further, survivability depends on distributed sensing since active sensors reveal their position and become targets themselves, resilient air defence networks rely on multiple sensors contributing to a common operating picture. This improves both situational awareness and platform survivability by reducing dependence on any single emitter.

Finally, counter-drone defence must be adaptable and integrated. Rapidly evolving threats favour software-defined systems that can be updated quickly, while the widespread nature of the drone threat requires protection down to the lowest tactical echelons. The greatest risk is fragmentation: isolated purchases may create local coverage, but without a shared operational picture, they remain vulnerable to saturation and coordinated attacks.

Case study 8 | Nagorno-Karabakh 2020 | Armenia And Azerbaijan

Nagorno-Karabakh 2020: Drones defeat a conventional air defence

Over 44 days in 2020, Azerbaijan used Turkish Bayraktar TB2 drones and Israeli loitering munitions to destroy Armenian radars, launchers, artillery and armour. Remotely flown An-2 biplanes acted as decoys, drawing Armenian radars to switch on and reveal their positions. With no dedicated counter-drone layer, Armenia's air defence could not stop the attack

44

Days of war in which drones dismantled Armenia's air defence and ground forces



Dedicated interceptors keep defence affordable

Firing costly missiles at cheap drones wins the engagement but loses the campaign

34

Armenian surface-to-air missile systems visually confirmed destroyed



Human speed cannot match saturation

When targets arrive in numbers, parts of the kill chain must be automated, with operators supervising

146

Armenian tanks destroyed



Networked sensors stay alive

Linking many sensors into one picture lets radars stay silent and avoid giving away their position

Sources: Center for Strategic and International Studies (CSIS), Shaan Shaikh and Wes Rumbaugh, 8 December 2020 | Oryx, Jakub Janovsky et al., September 2020 EVN Report, Davit Khachatryan, 27 March 2024

An air defence built for the wrong threat can be taken apart by inexpensive aircraft in a matter of weeks. Over 44 days in 2020, Azerbaijan used Turkish Bayraktar TB2 armed drones and Israeli loitering munitions to destroy Armenian radars, launchers, artillery and armour, and the Armenian air-defence network could not prevent it⁸⁵. The campaign is one of the clearest demonstrations available of why a dedicated counter-drone layer, and the automation required to operate it, are not optional additions to an air-defence system.

The attack opened with deception. Soviet-era An-2 biplanes, stripped of crews and flown by remote control, crossed at low level as decoys. Armenian radars switched on to engage them and disclosed their positions, after which the TB2s and loitering munitions destroyed the radars and launchers that had fired⁸⁶. Once the air-defence belt was suppressed, drones operated over artillery, armour and supply columns with little opposition.

85. The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense, Center for Strategic and International Studies (CSIS), Shaan Shaikh and Wes Rumbaugh, December 2020

86. Lessons from the Nagorno-Karabakh 2020 Conflict, U.S. Army Center for Army Lessons Learned (CALL), Phillip Andrews, August 2021

Each failure points to a capability that was absent. The radars had been built to find manned aircraft at altitude and performed poorly against targets that are small, slow and close to the ground. Nothing in the inventory was dedicated to engaging drones, so every interception had to be attempted with a missile designed and priced for a different target. Detection, identification and engagement were conducted at the speed of crews working one target at a time, against an attack that arrived in numbers. And because the sensors were few and separately operated, each had to transmit in order to see, which is what exposed them. A layered, automated and networked counter-drone capability answers all four shortfalls, and this campaign shows what follows in its absence⁸⁷.

Key takeaways

- Dedicated interceptors keep defence affordable: Armenian crews had to answer cheap drones with missiles designed for aircraft. Firing a costly interceptor at an inexpensive target wins the engagement and loses the campaign, so a counter-drone layer needs effectors priced for the threat it is actually meant to meet.
- Human speed cannot match saturation: Detection, identification and engagement were carried out at the pace of crews handling one target at a time, while the attack arrived in numbers. When many targets appear at once, parts of that sequence have to be automated, with operators supervising the system rather than approving every individual engagement.
- Lone radars give themselves away: A radar that transmits in order to see discloses its position, and a munition that steers itself towards that signal will find it. Linking many sensors into one shared picture allows individual radars to stay silent for long periods while the track is still held, which is what keeps them alive.

87. Beyond the Drone Hype: Unpacking Nagorno-Karabakh's Real Lessons, EVN Report, Davit Khachatryan, March 2024



05

Risks and responsibility in military AI



Characteristics that make AI militarily valuable, namely speed, scale, and operational opacity, also create its principal risks. Experience from operational deployments shows that a relatively small set of failure modes recur across military AI applications. These failures are not unique to specific algorithms or platforms; they stem from fundamental system-design challenges such as data quality, model reliability, human oversight, and performance under unforeseen conditions.

As a result, these risks should be treated as engineering and operational requirements from the outset of a programme rather than as ethical considerations addressed after deployment. Effective military AI depends not only on capability, but also on robust testing, validation, assurance, and governance mechanisms that ensure systems perform predictably in contested and rapidly changing environments.

Exhibit 13: Principal risks of military AI and suggested mitigations

Risk	What it looks like	Evidence	Mitigation
 Automation bias and stale data	Operators trust machine output; underlying data is out of date	Minab school strike: over-reliance on MSS and imagery seven years old ⁸⁸ .	Data-freshness checks; mandatory human review with recorded reasoning; independent red-team
 Vendor and model dependence	One supplier controls the models, data or contract terms	US dispute over terms of use; Pentagon now seeks multiple vendors. ⁸⁹	Multi-vendor architecture; sovereign models; source-code and data rights
 Adversarial attack	Decoys, spoofing or poisoned data mislead models	Decoy aircraft used to trigger air defences in 2020. ⁹⁰	Adversarial testing; multi-sensor cross-checks
 Legal and accountability gaps	Unclear responsibility for AI-assisted targeting	Gospel and Lavender debate; ⁹¹ unclear accountability in the 2026 Iran war. ⁹²	Legal review; audit trails; commander accountability
 Escalation at machine speed	Compressed decision time reduces room for de-escalation	Recorded Concerns ⁹³	Human authority over escalation; crisis communication; testing under stress

Many risks associated with military AI ultimately stem from the location and quality of human judgement within the decision process. The commonly used phrase “human in the loop” often obscures more than it clarifies, as it encompasses a wide spectrum of operational arrangements. In practice, meaningful oversight depends not on whether a human is present, but on when and how that human intervenes.

A more useful framework distinguishes three modes of human involvement: human-in-the-loop, human-on-the-loop, and human-out-of-the-loop. In the first, a human authorises each action before execution; in the second, the system acts autonomously under human supervision with the option for intervention; and in the third, the system completes the entire process without real-time human input. Each model offers different trade-offs between speed, scalability, and control, and each requires a distinct set of safeguards, assurance mechanisms, and accountability structures.

88. 84. US Strike on School in Iran’s Minab Was Result of Over-Reliance on AI, Outdated SAT Images—Bloomberg, ThePrint, Archishman Ganguly, September 2026

89. 85. M. Mande and G. C. Allen, CSIS. What Is Maven Smart System, and What Does It Do?. 2 Jun 2026

90. 86. U.S. Army TRADOC G-2. Nagorno-Karabakh 2020 Conflict: catalogue of weapons and tactics (Aug 2021, public release). 31

Jan 2023

91. 87. Lieber Institute, West Point. The Gospel, Lavender, and the Law of Armed Conflict. 6 Sep 2024

92. 88. The Soufan Center. AI Integration in Operation Epic Fury and Cascading Effects (IntelBrief). 3 Mar 2026

93. 89. O. J. Daniels, CSET Georgetown. Stuck between Real and Ideal: The OODA Loop and Military AI. 2024

Understanding these distinctions is essential because the primary risks of military AI arise not from autonomy itself, but from mismatches between system behaviour, human oversight, and operational requirements. Consequently, effective governance depends on aligning safeguards to the specific mode of human involvement rather than applying a single oversight model across all AI-enabled capabilities.

Exhibit 14: Modes of human control and safeguards

Risk	Meaning	Key safeguard
In the loop	A human approves each engagement	Depth and time of review; audit trail
On the loop	The system acts; human supervises and can stop it	Override authority; limits set in rules of engagement
Bounded autonomy	A weapon completes its mission after launch within set limits	Restrictions on target type, area and time; test standards

One of the greatest risks often lies in the ‘human-on-the-loop’ model, where oversight exists in principle but may be ineffective in practice. A supervisor who can formally intervene in an engagement but has only seconds to react provides a legal safeguard more than an operational one. As attack tempos accelerate and saturation becomes commonplace, the opportunity for meaningful human intervention diminishes rapidly.

For systems operating under supervisory control, risk mitigation must therefore be designed into the system before the engagement begins. This includes clearly defined rules of engagement, restrictions on target classes and operating areas, and predefined responses for degraded scenarios such as jamming, deception, or model failure. In such environments, effective control depends less on real-time operator actions and more on the constraints, permissions, and safeguards embedded within the system.

The critical design question is not whether a human can intervene, but whether that intervention remains practical under operational conditions. For military organisations, this requires explicitly defining the intended level of human oversight and documenting the corresponding assurance measures. While the details need not be public, clarity on the supervisory model is essential for ensuring both operational effectiveness and accountability.

These design considerations operate within a legal framework whose core principles are already well established. The law of armed conflict applies irrespective of the technology employed, requiring military operations to distinguish between combatants and civilians, remain proportionate, and incorporate feasible precautions. The introduction of AI does not alter these obligations; it changes how they must be implemented and assured.

Accordingly, the legal review of AI-enabled systems must extend beyond the platform itself to encompass the concept of operations, human oversight arrangements, and intended modes of employment. Compliance depends not only on what a system can do, but also on how and under what conditions it is used. Equally important is maintaining a clear record of decision-making, including who authorised deployment and under what authority.

Discussion of autonomous weapons continues in United Nations (UN) forums, and voluntary norms are being developed through the Responsible AI in the Military Domain process. One position would prohibit autonomous weapons whose effects cannot be understood or predicted, along with those designed to apply force against people. It would restrict the remainder by target type, duration, area and scale, under effective human supervision⁹⁴. Another position accepts autonomy but regulates it procedurally. It requires senior approval before development and again before fielding, rigorous verification and validation, realistic operational testing, and a design that lets commanders exercise judgement over the use of force⁹⁵. India holds that the Convention on Certain Conventional Weapons is the proper forum, that international humanitarian law is technology-neutral and sufficient, and that a binding instrument is premature while definitions remain unsettled⁹⁶. The position is coherent and has been held consistently.

Accountability should remain vested in a clearly identified commander rather than being diffused across committees, developers, or suppliers. This requires robust audit mechanisms that record system recommendations, human interventions, and operational outcomes. Combined with post-engagement reviews that feed errors and lessons learned back into training, testing, and validation processes, such measures help ensure that military AI remains both operationally effective and accountable under existing legal obligations.

An audit trail records what was approved; it does not show whether the approval involved any real scrutiny. Unintended harm enters AI-enabled targeting at that point, through a recommendation accepted because the operator has little time, limited visibility into how it was produced, and no practical basis on which to dispute it. What holds this in check is procedural rather than technical: time to review, visibility into the basis of a recommendation, and a higher threshold of authorisation where the output concerns a person. Recent use of AI-enabled targeting in Gaza shows how quickly each of these comes under strain in a campaign conducted at speed and at scale.

Case study 9 | Gospel and Lavender | Israel

Israel's Gospel and Lavender: AI decision support under scrutiny

The reported use of Gospel and Lavender during the Gaza conflict became a defining case of the promise and risks of AI-enabled targeting.

100

Targets per day reportedly generated by Gospel, compared with about 50 per year earlier



Human oversight must be verifiable

Clear rules on who approves, how, and how it is recorded must sit behind every AI recommendation

37,000

Palestinians reportedly flagged by Lavender as suspected militants



Scoring people raises higher risk

Score based targeting of individuals brings sharper ethical, legal and precision concerns than targeting structures

~10%

Reported error rate of Lavender's classifications, with about 20 seconds of human review per target



Governance over performance claims

With claims unverifiable, the lasting lesson is about legal accountability, not system metrics

Sources: The Guardian, Harry Davies, Bethan McKernan and Dan Sabbagh, 1 December 2023 | +972 Magazine, Yuval Abraham, 3 April 2024
Fortune, David Meyer, 4 April 2024

94. ICRC Position on Autonomous Weapon Systems, International Committee of the Red Cross, May 2021

95. Pentagon Updates Guidance for Development, Fielding and Employment of Autonomous Weapon Systems, DefenseScoop,

January 2023

96. India's Normative Stance on Lethal Autonomous Weapons Systems, Carnegie India, T. Bharadwaj and C. Bhatt, February 2024

The reported use of the Israeli systems- Gospel and Lavender during Gaza conflict became a significant case of the prospects and challenges associated with AI-enabled targeting. According to media reports, Gospel was designed to assist in identifying structures and facilities, while Lavender assessed the risk associated with individuals based on its intelligence indicators. The reports sparked controversy over the extent of human oversight, the dependability on AI-generated classification and the role of automation in targeting.

Contested

The details remain contested, as the claims were rejected by IDF. They have stated that such systems are decision-support tools and are not being deployed as autonomous targeting systems. Many of the reported claims could not be verified without access to the system. As a result, the significance of this example lies more in the governance and legal concerns it raises for military adoption of AI than the disputed performance metrics.

Key takeaways

- Human oversight must be clearly defined and verifiable: Organisations require robust framework that specifies human oversight, an authorised approver and documentation process.
- Score based targeting of humans introduce higher risks: It raises more complex ethical, legal and precision concerns
- Transparency underpins legitimacy. Public confidence in AI-embedded military systems depends on the clarity of the legal framework.





06

Key imperatives for India



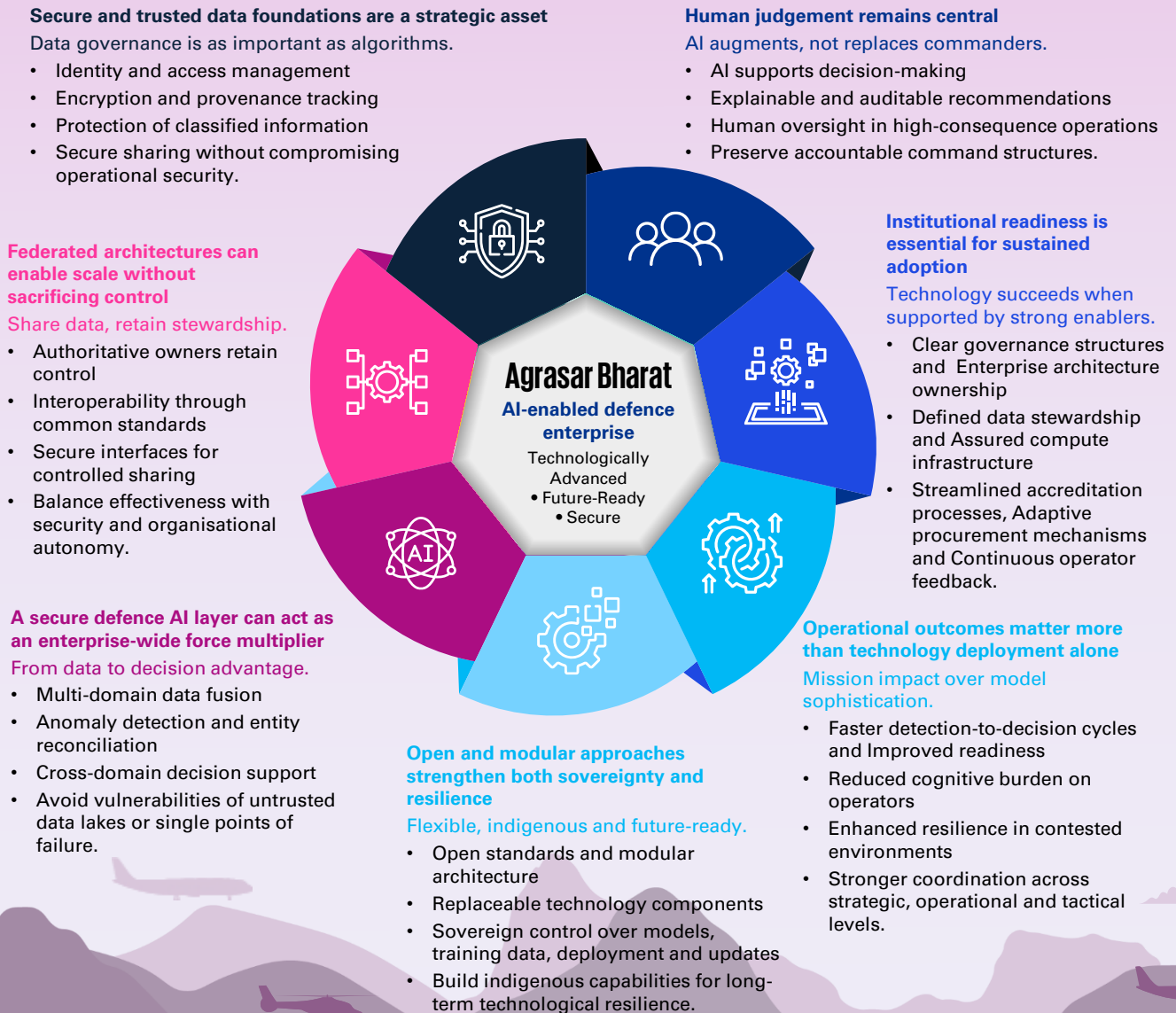
- The next phase of military AI adoption will be shaped not by the proliferation of isolated applications, but by the ability to embed AI across the defence enterprise through trusted data, interoperable systems, robust governance, and operational integration. For India, this aligns closely with the broader vision of Agrabharat - a technologically advanced, self-reliant, and future-ready nation capable of securing its interests in an increasingly contested and data-driven security environment.
- Human judgement remains central to military decision-making: Experience across leading military AI programmes suggests that the most effective systems augment rather than replace commanders. Particularly in high-consequence military operations, trust is strengthened when AI recommendations remain explainable, auditable, and subject to human oversight. This reinforces the importance of preserving accountable command structures while leveraging AI to enhance decision quality and speed.
- Secure and trusted data foundations are a strategic asset: Defence organisations worldwide increasingly recognise that data governance is as important as algorithms themselves. Effective AI adoption has been underpinned by strong mechanisms for protecting classified information through identity management, encryption, provenance tracking, and role-based access controls, ensuring that sensitive data can be used securely without compromising operational security.



Exhibit 14: Key imperatives for India in military AI

Defence AI lessons for India

Advancing Agrasar Bharat through a trusted, sovereign and operationally integrated AI ecosystem



- **Federated architectures can enable scale without sacrificing control:** Rather than consolidating information into centralised repositories, many defence institutions are adopting federated approaches that allow authoritative owners to retain stewardship of their data while enabling controlled sharing through common standards and secure interfaces. Such models balance operational effectiveness with security, accountability, and organisational autonomy.
- **A secure defence AI layer can act as an enterprise-wide force multiplier:** A recurring characteristic of advanced military AI ecosystems is the emergence of secure AI platforms capable of drawing insights from authorised data sets across multiple domains. These platforms support data fusion, anomaly detection, entity reconciliation, and decision support while avoiding the vulnerabilities associated with unrestricted data leaks or single points of failure.
- **Open and modular approaches strengthen both sovereignty and resilience:** Global experience indicates that adaptable AI ecosystems benefit from open standards, modular architectures, and replaceable technology components. At the same time, retaining sovereign control over models, training data, deployment environments, and updating mechanisms is becoming increasingly important for strategic autonomy. For India, this reflects the broader Agradar Bharat aspiration of coupling indigenous capability development with long-term technological resilience.
- **Operational outcomes matter more than technology deployment alone:** The most successful AI initiatives are measured by their impact on mission effectiveness rather than by model sophistication. International programmes have increasingly focused on outcomes such as faster detection-to-decision cycles, improved readiness, reduced cognitive burden on operators, enhanced resilience in contested environments, and stronger coordination across strategic, operational, and tactical levels.
- **Institutional readiness is essential for sustained adoption:** Military AI programmes that have achieved scale have typically been supported by clear governance structures, enterprise architecture ownership, defined data stewardship, assured computing infrastructure, streamlined accreditation processes, adaptive procurement mechanisms, and continuous operator feedback. These enablers often prove as important as the underlying technology itself.

Taken together, these lessons suggest that the pursuit of defence AI is ultimately an enterprise-transformation challenge rather than a technology-adoption exercise. For India, the opportunity lies in leveraging AI to advance the vision of Agradar Bharat by building a sovereign, trusted, and interoperable defence AI ecosystem that combines indigenous innovation, secure digital foundations, and human-centred decision-making. Such an approach can help translate AI investments into enduring military capability, greater strategic autonomy, and sustained decision advantage across the full spectrum of national security operations.



List of abbreviations

Acronym	Full Form
AI	Artificial Intelligence
AIxCC	AI Cyber Challenge
ALIS	Autonomic Logistics Information System
API	Application Programming Interface
A-SADS	Autonomous Surveillance and Armed Drone Swarm
AWCFT	Algorithmic Warfare Cross-Functional Team
BDA	Battle damage assessment
C2	Joint Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CATS	Combat Air Teaming System
CCCW	Convention on Certain Conventional Weapons
CERT-IL	Computer Emergency Response Team Israel
CENTCOM	United States Central Command
COP	Common Operating Picture
CSET	Center for Security and Emerging Technology
CSIS	Center for Strategic and International Studies
DAIC	Defence Artificial Intelligence Council
DAIPA	Defence Artificial Intelligence Project Agency
DAP	Defence Acquisition Procedure
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
DEF CON	Defence Condition
DIANA	Defence Innovation Accelerator for the North Atlantic
DIU	Defense Innovation Unit
DPSU	Defence Public Sector Undertaking
DRDO	Defence Research and Development Organisation
EO/IR	Electro Optic/Infrared
EUR	Euro
EW	Electronic Warfare
FPV	First Person View
FY	Financial Year
GAO	Government Accountability Office
GPS	Global Positioning System
iDEX	Innovations for Defence Excellence
IDF	Israel Defense Forces
ISIS	Islamic State of Iraq and Syria
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
LLM	Large Language Model
ML	Machine Learning
MSS	Maven Smart System
NATO	North Atlantic Treaty Organization
NCIA	NATO Communications and Information Agency
ODIN	Operational Data Integrated Network
OODA	Observe-Orient-Decide-Act
OT	Operational Technology
PLA	People's Liberation Army
PM	Prime Minister
SIGINT	Signal Intelligence
SIPRI	Stockholm International Peace Research Institute
UAE	United Arab Emirates
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
U.K.	United Kingdom
U.S.	United States
USD	United States Dollar



Acknowledgements

Manan Asri

Niharikka Puri

Mukunda Murthi Rao

Aparna Srivastava

Megha Saravanan

Yudhisther Ranawat

Garima Pandey

Design and compliance

Prajakta Talpade

Venkatesh R

Samiksha Madke

Amishka Aryendra

Nisha Fernandes

KPMG in India contacts:

Akhilesh Tuteja

Head – Clients & Markets

P: +91 1242549191

E: Atuteja@kpmg.com

Himanshu Suryavanshi

Associate Partner – Aerospace,

Defence and Space

E: himanshus9@kpmg.com

Nilachal Mishra

Partner and Head – Government
& Public Services (G&PS)

E: nilachalmishra@kpmg.com

Cdr. Jaikumar Raghunathan

Director

Aerospace, Defence and Space

E: rjaikumar@kpmg.com

Gaurav Mehndiratta

Partner and National Head –
Aerospace, Defence and Space

E: gmehndiratta@kpmg.com

kpmg.com/in



Access our latest insights
on KPMG Insights Edge

Follow us on:

kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the quoted third parties and do not necessarily represent the views and opinions of KPMG in India.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai – 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Some images in this report have been created using artificial intelligence technology.

This document is for e-communication only. (TL_1026_VR_PT_SM_AA)