Emerging Threat Vectors
Drones and Autonomous Systems in the Indian Defence Spectrum

Parikshit Bishnoi* and Rajan Bakshi**

This article examines the strategic implications of drones and autonomous systems within India's evolving defence and security environment. It argues that autonomy should not be assessed merely as a platform capability, but as a structural force that compresses decision cycles, complicates attribution and reshapes escalation control. Focusing on India's contested borders, grey-zone pressures, and proximity to technologically capable adversaries, the article analyses emerging threats from China and Pakistan, gaps in India's doctrine, training, C2 integration, cyber resilience and civil–military technology fusion. It recommends a decision-centric approach to threat assessment, supported by doctrinal reform, red teaming, indigenous autonomy stacks, and institutionalised operational learning.

Keywords: *Drones and Autonomous Systems; Indian Defence; Threat Assessment; Autonomous Warfare; Counter-UAS; Escalation Control*

Autonomy is not about removing humans; it is about empowering humans to operate at machine speeds.

– Dr Peter W. Singer, author of *Wired for War*

* Maj Parikshit Bishnoi is presently posted as a System Manager in Command Cyber Ops and Sp Wing (CCOSW), Northern Command.

** Col (Dr) Rajan Bakshi, a veteran Infantry Officer with 36 years of service in the Indian Army, is presently Director of the Amity Centre for Defence and Strategic Analysis (ACDSA) and an Associate Professor at the Amity Institute of Defence and Strategic Studies (AIDSS).

ISSN 0976-1004 (print); 2583-7567 (online)

Introduction

Drones and autonomous systems (DAS) have rapidly moved from niche applications to mainstream use in both civilian and military spheres, including India's defence sector. While these technologies offer clear operational advantages (from real-time surveillance to precision strikes), their proliferation also raises serious concerns from vulnerabilities in security and privacy to complex ethical and legal dilemmas in warfare. This assessment of DAS in the Indian context highlights their prospects as well as their limitations. The Indian Armed Forces operate in a challenging security environment, including cross-border tensions, insurgencies, terrorism and asymmetrical warfare. Autonomous Systems are weapon platforms that can operate autonomously to varying degrees. These systems can select, engage and neutralise targets without human involvement. Understanding their function and influence on India's threat assessment is critical for strategic decision-making. Drones have received considerable attention as Unmanned Aerial Vehicles (UAVs) because of their adaptability and operational capabilities. Effective threat assessment underpins military strategy; it must evolve as new technologies emerge and alter the battlefield. For India, this means reassessing how DAS affect threat perceptions and response protocols, rather than relying on traditional models.

Emerging technologies, such as autonomous weapons, cyber weapons, the weaponisation of space, and artificial intelligence (AI), alone or in combination with conventional modes of warfare, determine success or failure on modern battlefields, including conventional, sub-conventional and nuclear conflicts.[1] To paraphrase PM Narendra Modi, India needs to combine the third and fourth industrial revolutions in military capabilities.[2] These new technologies are simply part of India's military modernisation programme. Technology alone seldom wins battles; military strategies and tactics must include it.[3] The requirement of all military operations, whether offensive, defensive, or relating to low-intensity operations on land and sea, is fundamentally about the control of territory and populations, as the Indian Military's Joint Doctrine postulates.[4]

India aims to become a global drone hub by 2030 and a developed nation by 2047. Despite reforms since 2021, India still imports critical UAV components (e.g., semiconductors, sensors and GCS). The Ministry of Civil Aviation lacks an R&D leadership role, unlike the FAA (USA) or EASA (EU). Defence UAV programmes show mixed results: Nishant and Panchi closed, Rustom-1 stagnant, Tapas revived with 10 units ordered (IAF: 6, Navy: 4), and Archer-NG pending acceleration. India lacks civil–

military synergy, a nodal UAV ministry, and indigenous certification mechanisms.[5]

Accordingly, this article advances a context-specific analysis that treats drones and autonomous systems not as discrete platforms or force multipliers but as structural accelerants reshaping threat perception, decision-making and escalation control in India's immediate conflict environment. Their contribution lies in reframing the impact of autonomy on decision latency, attribution ambiguity and command authority, rather than cataloguing individual systems. Unlike Western expeditionary models characterised by permissive theatres and extended decision cycles, India's challenges are shaped by its geographic proximity to adversaries, compressed timelines, contested borders and persistent gray-zone activity. Against this backdrop, this study examines how evolving drone and autonomous capabilities in China and Pakistan translate into operational threats for India, evaluates the adequacy of existing doctrines and structures, and identifies practicable measures to reduce decision latency and escalation risk under autonomy-enabled conditions.

Autonomous Systems: Concepts and Capabilities

Empirical research on Autonomous Systems is difficult because they lack a universal definition or even a set of technical standards to determine whether a weapon system or platform is autonomous.[6] The US Department of Defense (DoD) unmanned systems roadmap outlines 'levels' or a 'spectrum' of autonomy, which can be understood through three distinct and independent dimensions: (i) *Task Type Autonomy*, which refers to the complexity and nature of tasks performed (e.g., navigation, targeting, engagement); (ii) *Human–Machine Interaction*, which ranges from human-in-the-loop (supervised), on-the-loop (semi-autonomous), to human-out-of-the-loop (fully autonomous); and (iii) *Cognitive Sophistication*, which refers to the machine's ability to perceive, reason and decide using artificial intelligence.[7] These dimensions define the extent of autonomy, and a system's classification as 'automatic', 'automated', or 'autonomous' depends on how far it advances along each axis. For instance, a drone may be fully autonomous in navigation but still require human confirmation for engagement, indicating partial autonomy.[8] In the Indian context, there is an urgent need to doctrinally define these levels of autonomy to standardise development, procurement and deployment across services. India's adoption must be calibrated and incremental, starting with supervised autonomy in Intelligence, Surveillance, Reconnaissance (ISR) roles, progressing to more complex applications such as target acquisition and electronic warfare.[9]

Autonomy and the Transformation of Threat Assessment

The introduction of drones and autonomous weapon systems (AWS) is transforming not only how military force is applied, but also how threats are perceived, assessed and managed. Traditional threat-assessment models within the Indian military have been largely platform-centric and ISR-driven, relying on linear intelligence cycles, human-led analysis and sequential decision-making. These models assume visible warning times, identifiable adversary intent, and relatively stable escalation ladders. Autonomy disrupts these assumptions by compressing operational timelines, redistributing decision authority between humans and machines, and altering how escalation is initiated, controlled and terminated, thereby reshaping threat assessment as a dynamic, time-sensitive process rather than a static evaluation of force structure.

Autonomous systems reshape threat assessment across three interlinked stages: *input*, *processing* and *output*. Table 1 outlines the progression from data generation to decision-making in contemporary operations, highlighting how sensor-driven inputs and automated processing compress the command timelines. In India's contested security environment, this dynamic significantly constrains deliberative escalation management in crises.

Table 1 Progression from data generation to decision-making in contemporary operations

Stage	Key Elements	Operational Effect
Input (Data Generation)	Multi-sensor inputs from UAVs Satellites Ground-based sensors Cyber sources	Continuous, high-volume data streams provide persistent situational awareness
Processing (Analysis & Assessment)	Automated analytics Machine-Assisted target recognition Prioritisation tools	Faster classification and ranking of threats than manual human processing
Output (Decision & Action)	Accelerated decision cycles Parallel response options	Compressed decision windows place increased pressure on command authority and escalation control

Source: Authors' own.

This shift exposes the limitations of legacy threat-assessment frameworks when applied to autonomy-enabled warfare. Western expeditionary models, developed for permissive or semi-permissive theatres, prioritise ISR dominance, air superiority, and extended decision cycles with a relatively low escalation risk. In contrast, India operates in an environment of continuous contact with peer and near-peer adversaries, where drone intrusions, loitering munition strikes, or swarm-based probing actions may unfold within minutes and below the threshold of declared hostilities. Under such conditions, threat attribution becomes algorithm-assisted rather than purely human-led, escalation control becomes simultaneous rather than sequential, and decision authority is increasingly stressed at the tactical and operational levels. Consequently, errors are more likely to emerge from data bias, algorithmic limitations, or adversarial manipulation than from human misjudgement alone, underscoring the need to reorient threat assessment frameworks around decision latency and escalation stability rather than platform capability. This shift can be analytically understood through an adaptation of existing threat-assessment constructs, recalibrated to reflect autonomy-enabled speed, attribution ambiguity, and escalation dynamics in India's operational context as shown in Table 2.

Table 2 Existing threat-assessment constructs

Analytical Dimension	**Legacy Threat Assessment**	**AWS-Enabled Threat Assessment**
Temporal Dimension	Linear, warning-based	Compressed, real-time
Attribution Logic	Human-led	Algorithm-assisted, multi-sensor attribution
Escalation Management	Sequential	Parallel and rapid escalation dynamics
Decision Authority	Hierarchical	Distributed and machine assisted decision authority
Primary Error Type	Cognitive bias and misperception	Data quality limitations and algorithmic bias

Source: Authors' own.

For India, this shift necessitates a recalibration of threat assessment doctrines away from *platform-centric evaluations* towards a *decision-centric approach*, where the primary variables are *decision latency, attribution ambiguity, and escalation stability*. Therefore, autonomous systems must be

assessed not only by their technical performance or lethality, but also by how they alter command-and-control rhythms, stress existing escalation control mechanisms, and reshape the balance between speed and control in crisis situations. Without such recalibration, the operational advantages offered by autonomy risk becoming strategic liabilities. Rather than proposing an entirely new framework, this article adapts and contextualises existing threat-assessment approaches to account for the operational effects of autonomy within the Indian conflict spectrum.

Drones in Military Operations

Beyond their conventional roles, the Indian Armed Forces are increasingly integrating advanced drone capabilities that reflect the emerging warfare paradigms. Swarm drones, comprising multiple UAVs coordinated by AI to function as a collective unit, are being developed to saturate enemy defences, conduct multi-directional reconnaissance, or serve as decoys. Indigenous efforts, such as the Defence Research and Development Organisation (DRDO) and Hindustan Aeronautics Limited (HAL) partnered project with Bengaluru-based Startup NewSpace Research and Technology (NSRT) Air Launched Flexible Asset–Swarm (ALFA-S) project, exemplify India's push in this domain. Loitering munitions, or kamikaze drones, combine ISR and strike capabilities on a single platform and are particularly effective in mobile warfare. These systems allow real-time threat identification and target neutralisation with minimal collateral damage, which is an ideal capability for border skirmishes and swift precision strikes. India has initiated the procurement and trials of systems such as SkyStriker and Nagastra-1, and private-sector innovations under iDEX are also advancing rapidly. Another transformative concept is Manned–Unmanned Teaming (MUM-T), which enables seamless cooperation between manned platforms, such as helicopters or tanks, and unmanned systems. For instance, rotary-wing aircraft can maintain safe standoff distances while UAVs conduct forward observations or engage targets, thereby enhancing survivability and mission effectiveness. Together, these evolving drone capabilities form the backbone of India's transition towards network-centric and multi-domain operations.

Threat Landscape Analysis

India's threat appraisal must account for shifting dynamics in drone warfare, especially as autonomous systems proliferate. One critical factor is the contrast

with Western employment of drones. Western militaries have mostly used UAVs in asymmetric scenarios (targeting distant terrorist networks with minimal direct engagement). In stark difference, the Indian Army faces immediate, high-intensity contact with two technologically capable adversaries along unresolved borders. This means lessons from Western experiences often against non-peer adversaries have limited applicability to India's context. The asymmetry in technology and the proximity of threats demand a uniquely Indian framework for assessing the value of lethal autonomous weapon systems (LAWS) in achieving national security objectives.[10]

India faces a rapidly evolving threat landscape driven by the proliferation and operational integration of DAS by both state and non-state actors. In the regional context, China has made significant advances in drone warfare by embedding swarming UAVs, stealth unmanned combat aerial vehicles (UCAVs), loitering munitions and manned–unmanned teaming (MUM-T) architectures into its military doctrine. Platforms such as stealth UCAVs, high-speed reconnaissance UAVs and swarm-deployment systems exemplify Beijing's transition towards 'intelligentised warfare', wherein AI enables distributed sensing, coordinated task execution, and autonomous decision support across multiple domains. Rather than representing isolated platform enhancements, these capabilities compress detection-to-response timelines, increase the likelihood of parallel and multi-axis engagements, and place sustained pressure on air defence saturation thresholds. For India, the operational challenge posed by Chinese UAV networks lies less in individual platform lethality and more in their capacity to overwhelm sensor grids, exploit decision latency, and complicate escalation control under contested electronic warfare conditions across the northern and eastern theatres Pakistan has steadily expanded its UAV inventory through indigenous development, strategic partnerships and external procurement, covering tactical ISR platforms, loitering munitions and limited swarm capabilities. The newly unveiled Shahpar-III by GIDS is a Medium-Altitude Long-Endurance (MALE) UAV with a 1,050 km range, 17-hour endurance and compatibility with strike munitions, such as the *Buraq* and *Al-Battar* LGB.[11] Tactical drones, such as the Uqab and Ranger, support ISR and surveillance roles for both the Army and Air Force. Pakistan's growing interest in loitering munitions is evident in systems such as Sarfirosh and the stealth-capable GM-500 Turah, which are reportedly used in coordinated swarm attacks. Pakistan has also collaborated with Turkey, notably fielding Bayraktar YIHA-III loitering munitions deployed during border skirmishes in May 2025.[12] Indigenous drone manufacturing is driven by state-owned entities, such as NESCOM

and GIDS, alongside collaborations with firms from Germany, Italy, and the Turkish private sector, pointing to a hybrid acquisition model that blends domestic capacity with foreign inputs.[13] Reports from May 2025 indicate the mass deployment of drones along the LoC, with over 50 Pakistani drones neutralised in a single night by Indian air defences, underscoring Islamabad's increasing reliance on UAV saturation tactics. Additionally, the increasing use of commercial drones by terrorist organisations and insurgents for surveillance, IED delivery and psychological impact, particularly in J&K, adds a complex sub-conventional threat dimension.

Pakistan's evolving UAV employment reflects an attrition-centric and escalation-managed approach designed to operate below the threshold of conventional conflict, particularly along the LoC. The increasing use of loitering munitions, swarm-enabled saturation tactics, and commercially adaptable platforms introduces significant attribution ambiguity and complicates India's escalation-management frameworks. These systems enable deniable, repetitive probing actions that strain brigade and division-level counter-UAS readiness and blur the distinction between sub-conventional and conventional triggers. Consequently, India's threat assessment must adapt to account for persistent UAV-enabled grey-zone pressure, prioritising rapid attribution, decentralised counter-swarm capabilities, and forward-deployed decision authority to prevent tactical drone incidents from escalating uncontrollably or, conversely, normalising persistent aerial violations. Taken together, China's autonomy-driven, multi-domain UAV integration and Pakistan's attrition-centric, grey-zone drone employment underscores the erosion of traditional threat-assessment models under conditions of compressed decision timelines, attribution ambiguity, and persistent autonomous pressure necessitating a shift towards decision-centric, autonomy-aware threat evaluation frameworks.

For India, this threat is not limited to physical platforms alone. Cyber vulnerabilities in command-and-control (C2) systems and satellite links can be exploited by adversaries through jamming, spoofing, or hacking, potentially rendering Indian assets inoperable or even turning them against friendly forces. Adversary counter-drone strategies, including radar-based detection, directed energy weapons, and electronic warfare suites, are being used to neutralise India's developing drone capabilities. As our adversaries evolve tactically and technologically, India must anticipate these shifts to remain operationally relevant. Furthermore, in multi-domain ops where air, land, cyber, and electromagnetic operations converge and interact with each other. Autonomous systems will increasingly operate in these fused

environments, necessitating joint services and the establishment of integrated drone warfare doctrine. Threat appreciation must also account for proxy use of drone swarms, the potential for AI-enabled decision loops, and the strategic ambiguity in attributing attacks conducted via autonomous platforms.

Autonomous drones and weapon systems complicate the application of International Humanitarian Law (IHL) by challenging core principles such as distinction, proportionality and accountability due to reduced human oversight in lethal decision-making. Traditional systems involve human judgement and clear chains of command to ensure legal compliance and responsibility. In contrast, autonomous systems operate based on algorithms and machine learning, lacking the contextual ethical reasoning required in complex battlefield conditions, particularly in hybrid or urban environments.[14] Furthermore, India must be cautious of how IHL and associated global norms are often selectively applied by major powers, who may circumvent these frameworks while advocating their enforcement upon others, thus creating geopolitical imbalances.[15] Without recognising this asymmetry, India's strict adherence to emerging AWS legal standards absent mutual reciprocity could become a self-imposed strategic constraint. Therefore, India must craft ethical and legal doctrines for AWS that are principled and pragmatically aligned with its national security and strategic autonomy.

Operational Considerations

The integration of AWS into the operational framework requires careful consideration of several factors. The Ghatak UCAV (Unmanned Combat Aerial Vehicle) is India's first indigenous stealth combat drone, being developed by DRDO's Aeronautical Development Establishment (ADE) and Aeronautical Development Agency (ADA), intended for autonomous deep-strike missions with internal weapon bays and low-observable features. Originally codenamed AURA, the programme has advanced through the Stealth Wing Flying Testbed (SWiFT) demonstrator, a 1-tonne scaled-down flying wing platform designed to validate critical technologies such as stealth aerodynamics, autonomous flight control and indigenous propulsion. SWiFT conducted its maiden flight on 1 July 2022 at Chitradurga and is undergoing upgrades, including a shift to the indigenous Manik small turbofan engine and a refined stealth airframe.[16] The full-scale 13-tonne Ghatak prototype and full-scale Ghatak UCAV programme continue to face propulsion and integration challenges, with indigenous engine (Kaveri) integration remaining

a longer-term objective rather than an assured near-term milestone. The Ghatak is envisioned to carry precision-guided munitions for high-risk missions.[17] Strategically, Ghatak aims to offer India a stealth UCAV capability at par with platforms such as China's GJ-11 and Russia's S-70, enhancing operational autonomy and survivability in contested airspaces.[18]

a. Despite notable progress in indigenous drone development, India's integration of DAS into military operations is constrained by several technological, policy and institutional limitations. A major capability gap exists in specialised training and human resource development; current programmes lack the scale and depth to meet the technical demands of AI-enabled systems. There is an urgent need to re-task and strengthen existing training nodes that focus on mission planning, data analysis, autonomous navigation and payload management.
b. Technologically, the command-and-control (C2) architecture remains fragmented, with limited interoperability between services and insufficient real-time data fusion capabilities. Akashteer is the Indian Army's mobile air defence command-and-control (C2) system developed by Bharat Electronics Limited (BEL), designed to integrate radars, communication units, and missile systems for real-time aerial surveillance and counter-drone operations, with full deployment targeted for 2027.[19] Complementing this, the Indian Air Force's Integrated Air Command and Control System (IACCS) functions as a centralised, automated tri-service C2 network that fuses inputs from radars, AWACS, missile batteries, and civilian air traffic systems to enable rapid threat detection and coordinated response.[20] India's emerging integrated counter-UAS network adopts a layered structure combining RF, EO/IR sensors, electronic warfare jammers, spoofers, and kinetic or laser-based hard-kill systems. These components form a broader C2 ecosystem with growing capabilities such as real-time situational awareness and inter-service synchronisation. However, critical gaps remain, particularly in seamless Akashteer–IACCS integration, detection of small and low-RCS drones, and field deployment of advanced directed-energy systems.[21]
c. On the policy front, India lacks a dedicated doctrine for DAS operations, including defined rules of combat engagement (ROE). The absence of legal and ethical frameworks tailored to AWS presents both strategic and humanitarian risks. Furthermore, India's defence cybersecurity posture is still adapting to drone-specific threats, and encryption, electronic hardening, and cyber-resilient communication protocols must be strengthened to safeguard drone operations.

d. Finally, challenges in human–machine interface (HMI) design, particularly under high cognitive loads in tactical environments, impede optimal operator performance. Addressing these issues demands a whole-of-government approach, involving defence R&D, industry collaboration under the 'Make in India' initiative, and doctrinal reforms driven by integrated theatre commands. Bridging these gaps is essential to realise the full potential of DAS in India's operational doctrine.
e. We can optimise the integration of DAS into its existing operational framework. Effective training, robust command and control mechanisms, logistical support, collaboration with other military components, adherence to legal and ethical standards, cybersecurity measures, and considerations for human–machine interaction for maximising the operational potential and effectiveness of DAS in military operations.

Strategic Implications and Policy Considerations

The integration of DAS into the operational framework has significant strategic implications and requires careful policy consideration. This section aims to analyse the key strategic implications and policy considerations associated with the deployment and use of DAS in Indian context.

a. *Norms, Ethics and Escalation Control*: The development of DAS poses significant challenges for arms control, ethics and international law, particularly given the selective application of regimes such as the Arms Trade Treaty and the Convention on Certain Conventional Weapons, including its Group of Governmental Experts on Lethal Autonomous Weapons Systems. (LAWS).[22] While these frameworks seek to uphold humanitarian norms, uneven compliance risks constraining states such as India more than technologically dominant nations. India must therefore adopt a norm-shaping approach that balances ethical responsibility with the policy space required for indigenous AI-enabled capability development.[23] Clear ethical and legal frameworks are required to govern the use of drones and autonomous systems, including defined levels of human control, proportionality, distinction and rules of engagement (ROEs) consistent with international humanitarian law.
b. *Capability and Doctrine Gaps*: India's integration of autonomous systems in military operations depends on critical technologies while platforms like SWiFT and ALFA-S show progress, especially in stealth and autonomous flight, gaps remain in full-spectrum stealth, indigenous AI chipsets, and doctrinal acceptance of tactical autonomy. Although

initiatives such as iDEX and IDDM have institutionalised industry engagement, civil–military R&D convergence remains fragmented due to weak joint governance structures, restricted data sharing, and short-term procurement models. Bridging these divides through integrated programmes, shared testbeds, and co-development pipelines is essential for India to achieve operational autonomy in drone warfare.[24] Private R&D investment remains below 5 per cent, far below the global average. While start-ups have shown innovation in swarm and loitering drones, they lack sustained domestic support.[25] India's defence drone ecosystem suffers from structural gaps, including the absence of a nodal authority for UAV R&D, certification and procurement, and lacks a Design-Linked Incentive (DLI) or IDDM certification under the DAP 2020. There are no dedicated UAV test corridors, certified laboratories, or robust defence–academia linkages. Training remains theoretical, and inconsistent service QRs limit indigenous participation.[26] Additionally, the doctrinal framework is underdeveloped, with no unified employment doctrine, unclear rules of engagement, limited support for experimentation and rapid prototyping, and weak civil–military integration.

c. By addressing these strategic implications and policy considerations, we can ensure the responsible and effective deployment of DAS. According to the Indian Ministry of Civil Aviation, India has the potential to become a global drone hub by 2030.[27] The Indian government is promoting the use of drones in many industries, and the entire approach towards their development has changed. The largest drone festival in India, Bharat Drone Mahotsav 2022, was recently held. In 2021, contracts worth over Rs 500 crores were negotiated by the Indian Army, Navy and Air Force.28 In August 2021, the Indian government announced the Drone Rules, which simplified the certification process, replaced the intricate clearance procedures required to fly drones, and promoted research and development.

Application of DAS in the Indian Context

The case studies and lessons learned from the experiences with DAS provide valuable insights into the challenges, successes and best practices associated with their deployment. This section aims to explore notable case studies and lessons learned from the use of Drones and Autonomous Systems.

a. *Border Surveillance and Counter-Terrorism Operations*: The employment of drones along the India–Pakistan and India–China borders has

enhanced persistent surveillance and reduced response timelines through real-time ISR feeds integrated into military command networks via LoS and BLoS links. Their integration into C4ISR architectures has improved target cueing and air defence coordination, as demonstrated during recent counter-UAS and air defence deployments. However, border surveillance and counter-terrorism operations continue to be constrained by interoperability gaps, uneven information sharing, training shortfalls, and coordination challenges across multiple agencies.[29]

b. *Humanitarian Assistance and Disaster Relief (HADR) Operations*: Drones have improved rapid damage assessment, search and rescue, and limited logistics support during disasters by enabling access to affected and inaccessible areas. Their employment by central agencies and through commercial partnerships has demonstrated utility in events such as major floods, cyclones and public health emergencies. However, HADR drone operations remain constrained by the absence of a standardised national framework, limited drone training among first responders, inadequate mission-specific payloads, fragmented airspace management, and the lack of centralised data processing, which collectively restrict scalability and timely decision-making.

c. *Reconnaissance and Target Acquisition*: The integration of DAS in counterinsurgency and counterterrorism operations has strengthened reconnaissance and target acquisition by enabling persistent surveillance and reducing exposure of personnel. Real-time transmission of high-resolution imagery has improved target cueing and decision-making, particularly when fused with satellite inputs and ground-based sensors. However, the full operational value of these capabilities remains dependent on structured training for imagery interpretation, data fusion and intelligence exploitation.

d. *Logistical Support and Resupply Operations*: Drones have enabled rapid delivery of critical supplies to remote and inaccessible areas by bypassing terrain constraints and reducing personnel exposure, particularly in disaster zones and forward military locations. While drone-based resupply remains cost-inefficient for bulk logistics and constrained by payload, range, environmental sensitivity and infrastructure dependence, it is operationally viable for time-sensitive, small-load missions. However, scalability is limited by vulnerabilities to weather and cyber threats, and the absence of supporting doctrine, hardened systems, and dedicated infrastructure continues to restrict sustained employment.

Evaluating the Efficiency of DAS

The assessment of the effectiveness and efficiency of DAS is crucial for India to evaluate the impact and value of these technologies in military operations.

a. *Operational Impact*: The operational impact of DAS is best assessed by their contribution to mission outcomes rather than platform performance. Key indicators include reductions in response and decision timelines, improvements in the accuracy of reconnaissance, surveillance, and target acquisition, enhanced situational awareness through timely intelligence collection and analysis, and the extent to which these systems reduce exposure and risk to personnel during hazardous operations.
b. *Cost and Resource Efficiency*: The cost and resource efficiency of DAS should be assessed in terms of their effect on operational expenditure and resource allocation. Key measures include cost substitution against manned platforms for surveillance, reconnaissance, and limited resupply missions, optimisation of manpower and logistics through reduced patrols, convoys and escort requirements. Long-term sustainability based on lifecycle costs, maintenance burden, modularity and local supportability. Efficiency gains are most evident in time-critical and small-payload missions, while scalability depends on effective lifecycle and data management.
c. *Mission Adaptability and Flexibility*: The adaptability and flexibility of DAS are best assessed by their ability to integrate with existing military systems, scale across mission scope and intensity, and operate reliably across varied terrains, weather conditions and threat environments.
d. *Training and Skill Requirements*: India's current training framework for DAS is limited to basic operator skills, with no structured modules for advanced roles, such as ISR, MUM-T, swarm operations, or loitering munitions. Technician training for maintenance and software adaptation is inadequate, leading to a dependence on OEMs. Key gaps include the absence of tiered training modules, simulation-based EW scenario training, joint-service UAV crew certification, and standardised human–machine interface (HMI) protocols. To address this, a dedicated DAS Training Centre is recommended, along with skill progression tracks, integration of AI and edge computing in training, standardised and intuitive HMIs, and the establishment of a tri-service UAV certification mechanism under the HQ IDS.
e. *Lessons Learned and Continuous Improvement*: Although we have expanded the use of DAS, a formal continuous improvement mechanism tailored

to these capabilities remains limited. After-action reviews largely focus on conventional operations and seldom capture DAS performance indicators such as ISR latency, behaviour under electronic warfare, or navigation resilience. Feedback from tactical users is informal and rarely translated into doctrine or training. Addressing this gap requires a structured framework that integrates formal feedback channels, systematic linkage with training institutions, and periodic technology assessment, enabling operational learning to inform doctrine, capability development and sustained employment.

Recommendations for Optimising AWS in Threat Assessment

In summary, India faces compressed decision times and attribution challenges from autonomy-enabled threats, yet current organisations and doctrines have not fully adapted to these pressures. Drones and AWS thus remain underutilised in threat assessment, due to identifiable gaps in training and simulation infrastructure, in legal/policy guidance for autonomous engagement, in coordination between industry research and military needs, and in inter-agency integration and risk preparedness. Accordingly, our recommendations emphasise better use of existing institutions rather than creating new ones. The aim is to improve decision-making, integration, and governance by re-tasking current organisations.

Immediate (0–1 Year)

a. *Inter-agency Collaboration*: At present, multiple agencies employ drones for ISR and disaster relief (HADR) with almost no cross-agency coordination. Each operates under its own procedures and approval chains. The result is fragmented tasking, inconsistent airspace management, delayed data sharing, and wasted aerial asset potential during joint operations. To address this, we propose a Unified National Drone Operations Protocol (UNDOP) under HQ IDS (in coordination with the Ministry of Defence and Ministry of Civil Aviation) to standardise interagency drone use. This protocol would harmonise airspace management and streamline tasking/clearances among the Armed Forces, NDRF and state agencies, ensuring faster response and efficient use of all available drones. Embedding military operators in civilian HADR planning exercises, and reciprocally integrating civilian agencies into military contingency planning, would further enhance coordination, reduce decision latency, and improve operational coherence.

b. *Red Teaming of Drone Command-and-Control (C2)*: DAS are increasingly targeted through cyber intrusion, navigation denial and electromagnetic interference, with adversaries focusing on disrupting command-and-control rather than destroying the platforms. The absence of hardened data links, resilient navigation fallbacks and routine adversarial testing across many systems creates vulnerabilities that can degrade situational awareness and decision integrity during operations. To address this, a mandatory Red Teaming and Cyber Risk Framework should be institutionalised for all operational AWS platforms, embedding encrypted and anti-jamming datalinks, back-up navigation systems such as inertial modes, electromagnetic hardening, and pre-deployment cyber-resilience testing within procurement and induction processes. Consequently, a national counter-UAS strategy should be pursued to ensure redundancy and operational continuity in drone-dependent missions.
c. *Strengthened Legal and Ethical Frameworks*: India lacks a dedicated military legal framework governing autonomous platforms. Ambiguity exists in the rules of engagement, accountability in semi-autonomous missions, and data privacy in civilian-involved HADR operations. A legal-ethical policy specific to military DAS should be developed under the HQ IDS and the Ministry of Defence, aligned with the Law of Armed Conflict and IHL. It must define thresholds for lethal autonomy, accountability, civilian protection during surveillance, and human-in-the-loop standards to ensure ethical use. Regular legal audits and the integration of lessons from other militaries (e.g., NATO and Israel) should guide policy refinement.

Mid-Term Measures (2–3 Years): Institutionalisation and Operational Integration

a. *Enhanced Training and Skill Development*: Training remains platform-specific, fragmented, and does not cover emerging domains such as AI-enabled C2, swarm dynamics, or manned–unmanned teaming. Operators lack access to simulation environments that replicate joint C2 drone operations in real time. India must strengthen and re-task existing mechanisms under a centralised Drone and AWS Training Node to standardise joint, multi-domain training. Modules must be developed for real-time ISR analysis, AI-aided threat assessment, cybersecurity and ethical compliance. Regular joint field exercises should simulate drone-C2 integration, especially for high-altitude logistics and MOOTW missions.

b. *Akashteer–IACCS Integration*: The effectiveness of counter-UAS and air defence operations depends on seamless inter-service command and control. Priority must be accorded to full operational integration between the Army's Akashteer system and the IAF's Integrated Air Command and Control System (IACCS). This integration is essential to enable real-time data fusion, automated cueing, and coordinated responses to saturation and swarm-based threats across services.
c. *Military Civil Technology Fusion Reforms*: India's civil military drone ecosystem is advancing towards an innovation and IP-led model but remains constrained by structural deficiencies. Despite DAP-2020, iDEX and post-2021 civil reforms, the defence UAV sector continues to face unrealistic Service QRs, weak design continuity, and dependence on imported propulsion and sensors. The absence of unified certification, credible Indigenous Content validation, and system-level testing necessitates an institutionalised inter-departmental mechanism within the Ministry of Defence to formalise Military Civil Technology Fusion through shared infrastructure, long-term funding and design-linked incentives.

Long-Term Measures (5–10 Years): Strategic Autonomy and Doctrinal Maturity

a. *Indigenous AI Chipsets and Autonomy Stack*: Long-term operational autonomy cannot be achieved without indigenous AI computing, edge-processing hardware and secure autonomous software stacks. Strategic investment in defence-grade AI chipsets and autonomy architectures is essential to reduce supply chain vulnerabilities and ensure resilience under contested cyber-electromagnetic conditions.
b. *Theatre-Level Autonomy Doctrine and Policy Review*: India must evolve a theatre-level doctrine for employing DAS within integrated theatre commands. This doctrine should explicitly address escalation control, decision authority, autonomy thresholds, and joint employment across the land, air, maritime, cyber and electromagnetic domains. To ensure adaptability, formalise an inter-departmental review mechanism under existing resources to monitor and steer Autonomous Systems Policy review within the Ministry of Defence, with representation from HQ IDS, ARTRAC, DRDO, and field formations. These should conduct six-monthly reviews based on operational feedback, international developments, and technology scans, institutionalising a continuous battlefield innovation loop.

c. *Industry–Research Partnerships*: India's defence innovation ecosystem continues to face translational bottlenecks. Start-ups face procurement and scaling challenges, whereas DRDO developed systems often suffer from limited battlefield adaptability. Civil military R&D collaboration remains fragmented, with few integrated test loops between users and developers. To address this, we should go beyond the current scope of the Army Design Bureau[30] and Strengthen R&D verticals within existing Army Design Bureau/HQ IDS structures to mirror models like China's PLA Research Academy of Military Science and the US Army Futures Command and Army Innovation Command. These entities embed long-term R&D, operational experimentation, and industry linkages directly into the military chain of command.[31]
d. To operationalise this in the Indian context, *Joint Technology Cells* should be formalised under existing mechanisms within key field formations, where developers, soldiers and academic partners co-design and test-deploy Decision Assistance Systems and emerging autonomous technologies. The iDEX framework must be expanded to support brigade-level innovation challenges, enabling bottom-up and use case-driven solutions. Furthermore, real-time user feedback should be institutionalised to ensure that private sector adaptations remain tactically relevant, agile and field-driven.

The analysis in this article underscores that the strategic challenge posed by DAS to India is not merely technological but fundamentally cognitive and organisational. As autonomy compresses decision cycles, blurs attribution, and enables persistent grey-zone pressure, traditional platform-centric approaches to threat assessment, force planning, and escalation management become increasingly inadequate. Therefore, Indian military must shift from viewing drones as supplementary assets to recognising autonomy as a structural force shaping command authority, escalation control and crisis stability across the conflict spectrum. In India's operational environment, defined by proximity to adversaries, contested borders and compressed timelines, the decisive vulnerability is not the absence of platforms but the persistence of decision latency. In future conflicts, autonomy will shape escalation control more profoundly than firepower.

Notes

1. Kartik Bommakanti, Yogesh Joshi, Shimona Mohan, Karthik Nachiappan and Antara Vats, 'Emerging Technologies and India's Defence Preparedness', Special Report No.

209, Observer Research Foundation, April 2023, available at https://www.orfonline.org/public/uploads/posts/pdf/20240510151332.pdf, accessed on 29 June 2023.
2. Ibid.
3. Ibid.
4. 'Joint Doctrine: Indian Armed Forces', Headquarters Integrated Defence Staff, Ministry of Defence, Government of India, 2017.
5. R.K. Narang, 'Military–Civil Technology Fusion (MCTF) for Making India Atmanirbhar Global Drone Hub@2030', Monograph No. 87, Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), 2024, available at https://idsa.in/publisher/monograph/military-civil-technology-fusion-mctf-for-making-india-atmanirbhar-global-drone-hub2030.
6. Austin Wyatt and Jai Gallipot, 'An Empirical Examination of the Impact of Cross-Cultural Perspectives on Value Sensitive Design for Autonomous Systems', MDPI, 17 December 2021, available at https://doi.org/10.3390/info12120527.
7. 'Unmanned Systems Integrated Roadmap FY2013–2038', Department of Defense, United States of America, 2013, available at https://apps.dtic.mil/sti/pdfs/ADA592015.pdf.
8. Paul Scherrer, *Army of None- Autonomous Weapons and Future of War*, W.W. Norton & Company, 2018, pp. 27–30.
9. R. Sundaram, 'India's Approach to Military AI and Autonomy: A Need for Doctrinal Clarity', Issue Brief, Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), 22 February 2022, available at https://idsa.in/issuebrief/ai-autonomy-military-doctrine-rsundar-220222.
10. Kartik Bommakanti, Yogesh Joshi, Shimona Mohan, Karthik Nachiappan and Antara Vats, 'Emerging Technologies and India's Defence Preparedness', n. 1.
11. 'Shahpar-III UAV Data Sheet', Global Industrial Defence Solutions (GIDS), November 2024, available at https://gids.com.pk/product/shahpar-iii.
12. Irfan Khan,'Bayraktar Loitering Munitions Used in Kashmir Standoff: Expert Insight', *Al Jazeera*, May 2025, available at https://www.aljazeera.com/news/2025/05/17.
13. Rahimullah Yusufzai, 'Pakistan's Drone Industry: Local and Foreign Partnerships Fuel Growth', *Dawn*, 12 December 2024, available at https://www.dawn.com/news/1729531.
14. Vincent Boulanin and Maaike Verbruggen, 'Mapping the Development of Autonomy in Weapon Systems', Stockholm International Peace Research Institute (SIPRI), November 2017, available at https://www.sipri.org/sites/default/files/2017-11/sipri-november-2017-autonomy-in-weapon-systems.pdf.
15. Angshuman Chakraborty, 'International Law and the Weaponisation of Norms: India's Strategic Choices', *Journal of Defence Studies*, Vol. 15, No. 4, 2021, pp. 25–46.
16. 'SWiFT Unmanned Aerial Vehicle Successfully Tested', Defence Research and Development Organisation (DRDO), 1 July 2022.
17. Rajeswari Rajagopalan, 'India's Ghatak UCAV and the Future of Stealth Warfare', Observer Research Foundation, December 2023.

18. Rahul Singh, 'Ghatak UCAV Project to be Fast-Tracked by DRDO', *Hindustan Times*, 7 January 2024.
19. 'Akashteer Project Overview', Bharat Electronics Limited (BEL), 2023.
20. 'Operation Sindoor and India's Drone Defence Matrix', Expert Speak, Observer Research Foundation (ORF), May 2024.
21. 'Indian Army Seeks to Strengthen Counter-UAS Capabilities', C-UAS Hub, 29 August 2024.
22. 'Background on the GGE on Lethal Autonomous Weapons Systems (LAWS)', United Nations Office for Disarmament Affairs (UNODA), 2022, available at https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws/.
23. Angshuman Chakraborty, 'International Law and the Weaponisation of Norms: India's Strategic Choices', n. 15.
24. Kartik Bommakanti, Yogesh Joshi, Shimona Mohan, Karthik Nachiappan and Antara Vats, 'Emerging Technologies and India's Defence Preparedness', n. 1.
25. R.K. Narang, 'Military–Civil Technology Fusion (MCTF) for Making India Atmanirbhar Global Drone Hub@2030', n. 5.
26. Ibid.
27. 'Union Minister Jyotiraditya Scindia Launches NITI Aayog's Experience Studio on Drones', Press Information Bureau, NITI Aayog, 10 May 2022, available at https://pib.gov.in/PressReleasePage.aspx?PRID=1824140.
28. Jyoti Yadav, 'Growing Importance of Drone in India', The United Service Institution of India, June 2022, available at https://usiofindia.org/publication/cs3-strategic-perspectives/growing-importance-of-drone-in-india.
29. 'Akashteer Shifts Battlefield Balance: India's Indigenous Air Defence System Proves Decisive in Operation Sindoor', *The Economic Times*, 23 May 2025, available at https://economictimes.indiatimes.com/news/defence/akashteer-shifts-battlefield-balance-indias-indigenous-air-defence-proves-decisive-in-operation-sindoor/articleshow/121357278.cms.
30. Nitin A. Gokhale, 'India's Army Design Bureau Needs an Upgrade', *BharatShakti.in*, October 2022.
31. 'R&D in India's Defence Ecosystem: Time for Structural Reform', Issue Brief, Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), February 2022, available at https://www.idsa.in/issuebrief/rnd-indian-defence-ecosystem.