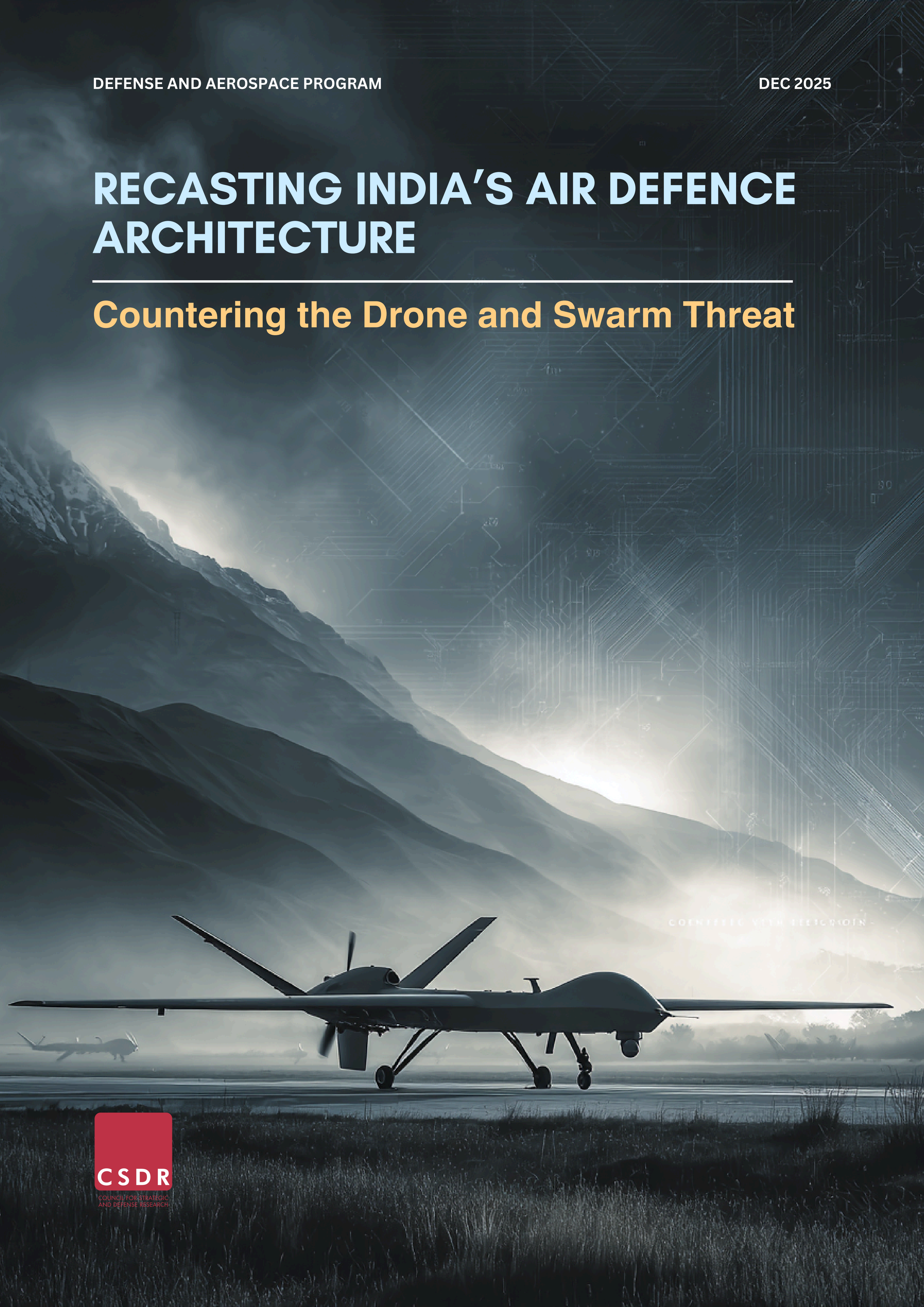
DEFENSE AND AEROSPACE PROGRAM

DEC 2025

RECASTING INDIA’S AIR DEFENCE ARCHITECTURE

Countering the Drone and Swarm Threat



CSDR

COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

Recommended citation:
CSDR (2025). Recasting India's Air Defence Architecture: Countering the Drone and Swarm Threat. New Delhi: Council for Strategic and Defense Research.

C-21, 3rd Floor, Qutub Institutional Area, New Delhi, India - 110016.
Phone: 011-43104566 | Email: office@csdronline.org | Web: www.csdronline.org | Twitter:@CSDR_India

ABOUT THIS REPORT

This report argues that India's traditional air defence (AD) architecture—reliant on expensive, centralized missile systems—is becoming obsolete against the proliferating threat of low-cost, autonomous drone swarms. The May 2025 "Operation Sindoor" crisis exposed a critical "cost asymmetry": expending million-dollar interceptors against disposable $2,000 FPV drones is economically unsustainable, allowing adversaries to easily exhaust India's magazine depth.

To address vulnerabilities in low-altitude detection and siloed Electronic Warfare (EW) capabilities, the report proposes shifting from a static defense model to an agile "kill web". This new architecture rests on three core abilities: Detect (using distributed sensors like LLLWRs), Survive (ensuring redundancy through decentralized command), and Sustain (prioritizing "soft-kill" jamming over kinetic missiles).

Key recommendations include immediately upgrading legacy L-70 and Shilka gun systems to proximity-fused ammunition for cost-effective point defense, and fast-tracking the integration of the IAF's IACCS and the Army's Akashteer systems to create a seamless Joint Engagement Zone. Ultimately, the report concludes that modern deterrence relies not on an impenetrable shield, but on a resilient ecosystem that renders saturation attacks futile.

ABOUT CSDR'S DEFENSE & AEROSPACE PROGRAM

CSDR's Defense & Aerospace program conducts research, policy analysis, and business consulting. It collaborates with government entities to present various policy options for achieving defense manufacturing, indigenization, and export goals. It also supports private industry in these sectors through comprehensive market research and strategy development services.

ABOUT COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

Founded in January 2020 by Lt. Gen. D.S. Hooda (Retd.) and Dr. Happymon Jacob, CSDR is an innovative think tank and consultancy specializing in foreign policy, geopolitical risk, connectivity, and critical areas of defense and aerospace. With a focus on the Indian subcontinent, Eurasia, and the Indo-Pacific, CSDR is committed to generating strategic insights that drive meaningful change. Read more at www.csdronline.com

RESEARCH TEAM

Hely Desai, Research Associate, CSDR
Shashank Tiwari, Research Assistant, CSDR
Dr. Gaurav Saini, Co-founder, CSDR

RESEARCH DIRECTION

Lt Gen D S Hooda (retd), Co-founder, CSDR

Executive Summary

This report argues that India’s traditional air defence (AD) approach—relied upon for decades to deny airspace through expensive, centralized missile systems—is becoming obsolete against the proliferating threat of low-cost, autonomous drone swarms. The May 2025 "Operation Sindoor" crisis served as a strategic inflection point, revealing that while India maintains formidable high-altitude denial capabilities (via systems like the S-400), it faces critical vulnerabilities in low-altitude detection and economic sustainability against saturation attacks.

The central strategic challenge is an unsustainable "cost asymmetry": the economic imperative of expending million-dollar interceptors against disposable $2,000 FPV drones bleeds national resources and invites exhaustion strategies. The report details how China’s doctrine of "multi-domain precision saturation" and Pakistan’s asymmetric use of loitering munitions are explicitly designed to exploit these gaps—specifically aiming to overwhelm India’s magazine depth and blind its centralized command nodes. Key vulnerabilities identified include significant blind spots in low-level radar coverage, a scarcity of operational AWACS platforms, and the dangerous siloing of Electronic Warfare (EW) from kinetic AD operations.

To ensure survival in the "opening hour" of future conflicts, the report proposes a paradigm shift from a static, linear defense model to an agile, integrated "kill web." This new architecture is built on three core abilities: Detect (replacing a few large radars with thousands of distributed small sensors), Survive (ensuring redundancy through decentralized command), and Sustain (adopting a "soft-kill first" hierarchy that prioritizes jamming and directed energy over kinetic missiles).

The implementation roadmap prioritizes immediate "quick wins," such as upgrading legacy L-70 and Shilka gun systems with proximity-fused ammunition for cost-effective point defense and fast-tracking the induction of Low Level Lightweight Radars (LLLWR). Structurally, the report calls for the urgent fusion of the IAF’s IACCS and the Army’s Akashteer systems to create a seamless tri-service Joint Engagement Zone. Long-term recommendations focus on indigenizing critical subsystems (seekers, data links) and deploying Directed Energy Weapons (DEWs). Ultimately, the report concludes that deterrence in the drone age depends not on an impenetrable shield, but on a resilient ecosystem that renders saturation attacks futile.

The Shifting Air Threat Landscape

For decades, India's air defence doctrine rested on a conventional foundation: denying adversaries access to its airspace through layered missile and radar systems. Investments centered on radar-guided guns, surface-to-air missile (SAM) networks, and centralized command architectures designed to detect and neutralize manned aircraft or cruise missiles. This framework defined air defence through most of the late 20th and early 21st centuries.

However, the emergence of small, low-cost, and low-observable drones — especially first-person-view (FPV) platforms and loitering munitions — has upended this traditional paradigm. The effectiveness of expensive, centralized systems is increasingly challenged by the proliferation of autonomous, disposable aerial threats that operate below radar coverage and at minimal cost.

The 2020s marked a decisive inflection point. Conflicts in Ukraine, Gaza, and the Caucasus — and most recently, the 2025 India–Pakistan confrontation ("Operation Sindoor") — revealed that aerial dominance no longer depends on controlling the skies, but on surviving the opening hour of drone and missile saturation. In this short but intense five-day conflict, Indian forces faced a complex fusion threat: Pakistani platforms augmented by real-time Chinese intelligence and material support. Although a ceasefire was brokered by May 10, the confrontation exposed both the strengths and vulnerabilities of India's air defence (AD) architecture.

The evolution of aerial threats has revealed a critical imbalance between cost and capability. A $2,000 FPV quadcopter can destroy a $2 million tank, while Shahed-type drone swarms have demonstrated that inexpensive unmanned systems can impose unsustainable costs on traditional air defence architectures. This imbalance has also highlighted the limitations of legacy systems — including the Akash, Pechora, and even the advanced S-400 batteries — which were optimized for high-altitude, fast-moving targets rather than dozens of small, low-radar-cross-section (RCS) vectors operating at treetop level. Operation Sindoor underscored the urgency of modernization and adaptation within India's air defence ecosystem.

"The evolution of aerial threats has revealed a critical imbalance between cost and capability. A $2,000 FPV quadcopter can destroy a $2 million tank, while Shahed-type drone swarms have demonstrated that inexpensive unmanned systems can impose unsustainable costs on traditional air defence architectures. This imbalance has also highlighted the limitations of legacy systems — including the Akash, Pechora, and even the advanced S-400 batteries — which were optimized for high-altitude, fast-moving targets rather than dozens of small, low-radar-cross-section (RCS) vectors operating at treetop level.

India's current AD network remains a multi-layered construct, integrating SAM systems, ballistic missile defence units, radar platforms, and interceptor aircraft — anchored by the Indian Air Force's formidable fleet of approximately 1,750 aircraft, including nearly 900 fighters. Yet the rise of drones, loitering munitions, and hypersonic platforms has rendered parts of this architecture increasingly obsolete. These new-age threats are not only harder to detect and intercept but also create an unsustainable cost imbalance: using million-dollar interceptors against thousand-dollar drones is a losing economic equation.

S-400. Photo: Russian Ministry of Defense

To remain effective, India's air defence must evolve beyond the traditional linear model. The next-generation AD architecture must be flexible, integrated, and autonomous — capable of reacting in real time, adapting to asymmetric and high-velocity threats, and operating seamlessly in dense, data-driven battle environments.[1] Moreover, this conflict has also reaffirmed the strategic urgency of indigenizing defence technologies. The push for self-reliance in unmanned systems and next-generation interceptors is no longer just an economic imperative; it is a cornerstone of national security.

The Akash surface-to-air missile is indigenously developed by the DRDO. Source: NDTV

The Proliferation of Tactical Drones and Loitering Munitions

Small drones have evolved from reconnaissance curiosities into precision strike instruments. The FPV drones deployed across Ukraine and Syria weigh under five kilograms, fly at 100–150 km/h, and carry modest warheads equivalent to a hand grenade.[2] However, their high speed, agility, and ability to operate beneath radar clutter pose a significant challenge to traditional air defence radars, which are calibrated to detect larger, more distinct aerial signatures. Loitering munitions such as Iran's Shahed-136 or Russia's Lancet-3 have further extended this challenge: capable of travelling over 100 km with warheads of 40–90 kg, these systems blend the attributes of cruise missiles and expendable drones.[3]

For militaries such as those of Pakistan and China, the affordability and operational effectiveness of such systems make them particularly compelling investments for enhancing deterrence and expanding asymmetric capabilities. They offer high psychological impact, near-zero attrition cost, and plausible deniability. Pakistan has imported and locally produced multiple variants of the Shahpar and Burraq UAVs,[4] but its attention has shifted toward smaller swarming FPV and "suicide quadcopter" platforms — hundreds of which were observed in Sindoor-era skirmishes. China's PLA has taken this to another level, developing modular swarm-control systems capable of commanding hundreds of UAVs from a single ground node, reportedly integrating them into artillery regiments and EW brigades.

The attraction lies in economics. Shooting down a $3,000 quadcopter with a $150,000 missile is an unsustainable exchange ratio. Even India's older L-70 and Shilka guns — effective against helicopters — struggle to acquire and track FPVs whose RCS is <0.01 m^2. While loitering munitions can still be countered by short-range SAMs or medium-calibre guns, FPVs and micro-UAVs pose a fundamentally different problem: they operate in the blind spots between radars and optical sensors, in cluttered terrain, and are often guided manually or semi-autonomously via video feed rather than GPS.

"While loitering munitions can still be countered by short-range SAMs or medium-calibre guns, FPVs and micro-UAVs pose a fundamentally different problem: they operate in the blind spots between radars and optical sensors, in cluttered terrain, and are often guided manually or semi-autonomously via video feed rather than GPS.

This erosion of cost symmetry, visibility, and predictability makes FPVs the new centre of gravity in air defence planning. The evolution from “aircraft defence” to “drone defence” is not cosmetic — it requires a different architecture, sensor philosophy, and logistical discipline.

As swarming low-RCS threats rise on India’s horizons, the frontline of air defence requires evolution toward a cost-effective C-UAS layer interoperable with electronic warfare (EW) and cyber capabilities. Prioritizing “seeing what is about to kill” over “killing what we see,” moving from centralized control to resilient decentralization, and emphasizing mobility, endurance, and response capacity over static defence would provide critical benefits to India’s air defence architecture. Strengthening hard-kill interceptors for drones, expanding soft-kill electronic warfare capabilities, and fusing them via AI-enabled command networks will ensure that India’s air defence architecture remains resilient even under massive saturation attacks. This integrated approach – intercepting cheaply, disrupting enemy swarms, and rapidly cueing missiles only for what leaks through – is crucial to preserve India’s air superiority and deterrence in the drone age.

Gaps in India's Current System

Despite significant advancements and a multi-layered approach, India's air defence system remains vulnerable to evolving threats from China and Pakistan.

- **First-Day Resilience**

During the recent standoff, India’s air defence faced challenges, including limited low-altitude radar coverage, which impeded early detection of small, slow-moving UAVs. The coordination between manned interceptor aircraft and ground-based air defence systems was constrained by communication bottlenecks and delayed decision-making. Furthermore, the absence of sufficient counter-drone technologies reduced the effectiveness of neutralizing drone swarms, allowing some threats to penetrate deeper into critical zones. However, those threats could not cause damage.

In a dual-front contingency, the AD picture's first-day survivability determines whether India fights the rest of the period on its terms. In mountainous sectors, valley masking can delay low-RCS detection and reduce track quality; AWACS scarcity magnifies gaps. Under coordinated jamming/cyber probes, the Recognised Air Picture (RAP) can degrade in minutes unless redundant sensors, passive RF, and decentralised C2 fallbacks are active. A notional 200–300-drone opening raid, split LoC/LAC, creates 600–900 simultaneous tracks; even with 50% early neutralisation, leakers targeting C2 nodes/fuel farms may fragment the network and force localised, non-networked fires. That is precisely the window adversaries design for saturation.

- **Low-Altitude Coverage and Point-Defence for High-Value Targets**

India's air defence architecture, while comparatively robust at medium and high altitudes, has notable gaps in low-altitude coverage and point defence for critical high-value targets such as military installations and air bases. Ground-based radars, which form a significant component of the air defence network, are inherently limited by line of sight, making them ineffective for detecting low-flying objects, particularly those below 300 feet, at greater distances.[5] This creates blind spots that adversaries can exploit with low-flying cruise missiles, drones, and rotorcraft.

To compensate for ground radar limitations, modern militaries rely on Airborne Warning and Control Systems (AWACS) – high-flying radar aircraft that can look down and see low-altitude intruders. However, the IAF has only a limited AWACS fleet: three Israeli-built Phalcon AWACS (on Il-76 airframes) and two indigenous Netra AEW&C aircraft, some of which are aging technologically.[6] Maintenance and upkeep further constrain their availability – all five platforms are rarely mission-ready at the same time. This limited AWACS coverage means India's ability to detect and track low-flying threats in real time, especially over broad areas, is far from comprehensive.

Operational consequence modelling indicates that in the event of AWACS denial — whether by direct attack, long-duration jamming, or maintenance downtime — valley-hugging micro-UAS can remain undetected until within 6–10 km of high-value targets. At typical micro-UAS speeds (70–100 km/h), this allows only 4–6 minutes for threat classification and engagement. With current point-defence reaction timelines, this window compresses further in saturation raids, making "single point" defences brittle under volume stress.

The proximity of India's borders with Pakistan further exacerbates point-defence vulnerabilities. This geographical contiguity provides minimal reaction time, adversely affecting the effectiveness of air defence systems, even modern ones like the S-400, which require up to 35 seconds for identification, tracking, and engagement.[7] Small drones, with their exceptionally low radar cross-sections (RCS as small as 0.001 square meters), are particularly difficult to detect even by advanced radar systems, making them ideal weapons for precision targeting or harassment.[8] Even if a system is defended by low-cost kinetic and non-kinetic measures, the affordability of drones allows them to be deployed in swarms that can overwhelm any point-defence system through saturation. In mountainous terrain, where aerial intruders like small drones can fly between valleys, effective engagement necessitates air defence guns or short-range SAMs. These systems, however, have limited detection ranges and require real-time information sharing and command to engage targets effectively. While the Indian Army is procuring Low Level Lightweight Radar (LLLWR) systems designed to detect micro-drones and swarm drones with small RCS, and has inducted the SAMAR system for low-altitude, quick-reaction defence, the sheer volume and evasive tactics of modern low-altitude threats continue to pose a significant challenge.

> The proximity of India's borders with Pakistan further exacerbates point-defence vulnerabilities. This geographical contiguity provides minimal reaction time, adversely affecting the effectiveness of air defence systems, even modern ones like the S-400, which require up to 35 seconds for identification, tracking, and engagement.

First-Hour Stressors & Mitigations (Indicative)

Stressor	Operational effect	Immediate mitigation	Structural mitigation
Valley-floor micro-UAS at 70–100 km/h	4–6 min to classify + engage; high leaker risk	Pre-plotted gun/DEW baskets; EO/IR towers	Aerostat belts; HAPS; passive RF mesh
Jamming of key links	RAP latency; false tracks; hold-fire	Alternate paths; emission control; pre-cleared ROE	Multi-bearer comms; frequency-agile radios; spectrum ops cell
AWACS unavailability	Low-altitude SA gaps; delayed cueing	Civil ATC fusion; tethered towers	A321 AEW&C induction; distributed C2
Magazine stress	Rationing; deterrence erosion	Prox-fused rounds; interceptor triage	Low-cost interceptors; DEW scale-out

- **Lack of Networked Air Defence and Control Architecture Across IAF, IA, IN (Tri-service integration challenge)**

Another critical vulnerability within India's air defence architecture is the persistent challenge of achieving seamless tri-service integration of command and control (C2) systems across the Indian Air Force (IAF), Indian Army (IA), and Indian Navy (IN). While the Air Force Network (Afnet) and the Integrated Air Command and Control System (IACCS) demonstrated effectiveness during Operation Sindoor, successfully integrating sensors from all three services to intercept Pakistani drones and missiles, significant gaps remain.[9]

A major limitation in India's air defence ecosystem is the absence of seamless integration across the three services. While there are communication links between the Army, Navy, and Air Force, true real-time data fusion—a hallmark of network-centric warfare—remains largely unachieved. As a result, coordination is often hindered during fast-paced operations. One clear manifestation of this gap is in battlefield information dissemination. For instance, while Army headquarters may have access to satellite imagery and intelligence concerning developments along the Line of Actual Control (LAC), such critical inputs rarely reach frontline units in real time. These valuable resources remain concentrated at higher headquarters, far removed from the tactical edge. While Akashteer, the Indian Army's Air Defence (AAD) system, is designed to connect smoothly with IACCS (IAF) and TRIGUN (Indian Navy) to create a clear, real-time battlefield picture and enable quick use of offensive and defensive weapons, the full realization of this synergy across all operational levels remains a work in progress. This lack of seamless integration limits India's ability to maintain a unified and timely air defence response, increasing the risk of delayed or fragmented decision-making during rapidly evolving conflicts. Without real-time data fusion across the services, India's air defence remains vulnerable to saturation attacks and exploitation of gaps between domains.

By comparison, India's regional adversaries have prioritized integrated command-and-control architectures to overcome these challenges. China, for example, has invested heavily in its "Qu Dian" system,[10] while Pakistan is gradually fielding its "Rehbar" network[11]—both designed to generate unified tactical-level situational awareness and enable rapid multi-domain coordination. In contrast, India's command-and-control networks remain fragmented, particularly at the operational and tactical tiers. This weakens India's ability to compress the decision cycle, a key requirement when facing fast-moving threats like drone swarms, loitering munitions, or stealthy cruise missiles. Without a resilient and agile sensor-to-shooter chain, India's OODA (Observe–Orient–Decide–Act) loop remains slower than it should be—posing serious risks in high-intensity or time-sensitive scenarios. This fragmentation and resulting sluggishness in decision-making underscore deeper

> A major limitation in India's air defence ecosystem is the absence of seamless integration across the three services. While there are communication links between the Army, Navy, and Air Force, true real-time data fusion—a hallmark of network-centric warfare—remains largely unachieved. As a result, coordination is often hindered during fast-paced operations. One clear manifestation of this gap is in battlefield information dissemination.

vulnerabilities in India's air defence posture, particularly when confronting novel aerial threats. Compounding these challenges is a critical gap in India's inventory of soft-kill systems—an area increasingly vital for countering micro drones and loitering munitions economically and effectively. This shortfall is not unique to India; recent conflicts have highlighted how modern air forces adapt to similar threats when faced with massed drone attacks.

- **The Missing Link: Electronic Warfare and Air Defence**

For instance, Ukraine's experience is a case study in adaptive air defence. Facing mass Shahed and Lancet strikes since late 2022, Ukraine fielded a mix of Western and Soviet-era systems: Patriot, NASAMS, Buk-M1, Osa, and the 1980s-vintage Gepard twin-barrel guns. Ukraine also pioneered improvisations.[12] Civilian acoustic sensors were networked to local command nodes, smartphones were turned into early-warning devices, and ex-Soviet guns were refitted with digital sights and night optics.[13] More importantly, Ukraine fused electronic warfare and air defence — an integration few nations had achieved before. The Kvertus Atlas network connected thousands of small jammers and drone detectors, allowing real-time cueing between EW teams and gun crews. This distributed "anti-drone web" blurred the traditional distinction between offensive jamming and defensive interception.[14]

Strela-10, one of the local and international air defense systems used by Ukraine in its war with Russia, as seen in Donetsk Oblast, Ukraine, on Feb 27, 2023. Strela-10 systems, modernized and provided to Ukraine by allied countries, are used extensively against Russian attacks. (Source: Mustafa Ciftci - Anadolu Agency)

Part of the Rheinmetall-made Skynex air defense system. Figures published by the German government show Berlin has delivered two Skynex systems along with ammunition to Ukraine. Source: NewsWeek

The operational lesson is clear: EW and AD must act as a single nervous system. Jammers must not only disrupt enemy drones but also feed targeting data into the AD picture. Conversely, radars should cue EW units to jam specific frequency bands, preventing over-broad interference that blinds one's own sensors. Ukraine's C2 structure allowed this horizontal flow of information, drastically reducing reaction times and fratricide risks.

To contextualize, India, by contrast, continues to treat EW and AD as separate verticals — an institutional silo that could prove catastrophic in a future swarm attack. Army EW regiments operate under Signals and Intelligence commands, focusing on communication intercepts and battlefield jamming. The Air Force runs its own electronic warfare squadrons, largely to protect aircraft. This division creates latency and confusion. Moreover, in a sustained saturation attack, relying solely on hard-kill interceptors becomes economically and logistically untenable, underscoring the urgent need to assess India's inventory of soft-kill systems and their effectiveness against micro drones and loitering munitions.

- **Inadequate Inventory of Soft-Kill Systems Against Micro Drones and Loitering Munitions**

India's present mix of interceptors makes it economically unsustainable to counter prolonged saturation. A notional 300-drone, 90-minute raid — with targets split between LoC and LAC sectors — would require between 250–350 missile shots from systems like Akash, Barak-8, or SPYDER if relying on hard-kill alone. At ~$360,000–$1.2 million per interceptor, this translates to ~$90 million – $420 million expended in a single engagement, with reloads constrained by magazine capacity and transport time. By contrast, the attacking force may spend under ₹150 crore to generate the same volume. Without a cost-effective C-UAS layer of Radio Frequency (RF) jammers, directed energy weapons, and proximity-fused gun systems, this disparity invites adversaries to bleed India's readiness in a matter of days.

Hard-kill (physical destruction) and soft-kill (electronic warfare, jamming, spoofing) systems are specifically designed to counter the burgeoning threat of micro drones and loitering munitions. While India has demonstrated capabilities against these threats, as seen in Operation Sindoor, where Akash and other indigenous systems intercepted Pakistani drones and loitering munitions, the sheer volume and low cost of these modern threats pose a sustainability problem.[15]

India's soft-kill capabilities — intended to neutralize drones through non-kinetic means such as jamming, spoofing, or directed energy — are still in development or at the pilot stage. While DRDO and BEL have made progress in developing RF jammers[16] and electro-optical detection tools,[17] these systems are not yet widely deployed or operationalized across the

“India's soft-kill capabilities — intended to neutralize drones through non-kinetic means such as jamming, spoofing, or directed energy — are still in development or at the pilot stage. While DRDO and BEL have made progress in developing RF jammers and electro-optical detection tools, these systems are not yet widely deployed or operationalized accross spectrum of Indian defence installations, especially in forward and vulnerable areas.

spectrum of Indian defence installations, especially in forward and vulnerable areas. Directed Energy Weapons (DEWs), such as high-energy lasers or microwave-based drone neutralizers, are still undergoing trials and have not been integrated into a combat-ready ecosystem.[18] Additionally, India lacks AI-integrated electronic warfare solutions that can autonomously detect, classify, and respond to the diverse signatures of commercial, tactical, and swarm-capable drones — a capability increasingly standard among advanced militaries.

Beyond technological shortfalls, India's air defence challenges further extend into doctrine and training. The absence of AI-driven electronic warfare capabilities reflects a broader lag in adapting operational concepts to the evolving nature of aerial threats. This doctrinal gap hampers India's readiness to counter asymmetric and hybrid challenges effectively in the modern battlespace.

These internal challenges are compounded by a changing regional threat environment, in which adversaries are rapidly modernizing and refining their air-offense concepts. Understanding India's vulnerabilities requires examining the evolving capabilities and strategic approach of China's aerial forces.

China's Evolving Air Offence Capabilities

China's air offensive capabilities are characterized by rapid modernization, integration of advanced technologies, and a strategic focus on multi-domain saturation tactics aimed at defeating adversary air defence networks.

The PLA's doctrine, reflected in its 2023 Science of Military Strategy, envisages "multi-domain precision saturation" — coordinated attacks using drones, cruise missiles, electronic deception, and cyber operations to overwhelm adversary C4ISR.[19] In Tibet and Xinjiang, China has deployed several EW-UAV brigades equipped with low-band jammers and synthetic aperture radars.[20] Their UAVs — including Wing Loong II and CH-5 — are designed to cue smaller, expendable drones that can be launched from trucks or artillery batteries. By 2024, satellite imagery confirmed "UAV cluster bases" in Ngari and Hotan, less than 300 km from Indian positions.[21]

> In Tibet and Xinjiang, China has deployed several EW-UAV brigades equipped with low-band jammers and synthetic aperture radars.[20] Their UAVs — including Wing Loong II and CH-5 — are designed to cue smaller, expendable drones that can be launched from trucks or artillery batteries. By 2024, satellite imagery confirmed "UAV cluster bases" in Ngari and Hotan, less than 300 km from Indian positions

More notably, China is nearing operational deployment of the Jiu Tian ("High Sky") drone mothership, a high-altitude, long-endurance platform capable of carrying up to 100 smaller kamikaze drones and loitering munitions for coordinated mid-air swarm release over ranges of up to 7,000 km—designed explicitly for overwhelming enemy AD systems via mass saturation.[22]

Further, the PLA has developed containerized CH-901 loitering munitions, which can be launched in rapid waves—either from vehicles or loyal-wingman drones like the FH-97—to confuse and deplete air-defence interceptors. These swarm-capable systems enable Beijing to engage in cost-asymmetric saturation warfare, forcing defenders to expend expensive SAM interceptors against low-cost unmanned assets—a strategy that severely stresses traditional AD doctrines.

CH-4 exists in two variants: the CH-4A, a long-range reconnaissance drone with a 3,500–5,000 km range and 30–40 hour endurance, and the CH-4B, a mixed attack-reconnaissance platform capable of carrying six weapons with a payload capacity of 250 to 345 kg. It can fire air-to-ground missiles from an altitude of 5,000 meters, enabling it to stay outside the range of most anti-aircraft guns while offering a wider field of view.
Source: Defence Hub

Wing Loong II is designed for both reconnaissance and strike missions. It can carry up to 12 air-to-ground weapons with a maximum payload of 480 kg and has an endurance of over 20 hours. It features an inverted V-tail, a ventral electro-optical turret, and straight wings with underwing hardpoints.
Source: Global Times

WZ-7 (Soaring Dragon) is a HALE UAV developed by China for strategic reconnaissance.
Source: REUTERS PHOTO: X01793

Pursuing its concept of "intelligentized warfare", China is integrating AI with modern drone technology for military applications. This includes extensive experimentation in drone swarms designed to operate autonomously, coordinate effectively as an "intelligent cloud," and potentially neutralize enemy radar systems before launching saturation strikes.[23]

- **AI-enabled EW systems and Space-based C4ISR**

The People's Liberation Army (PLA) has also developed sophisticated layered and Electronic Countermeasure (ECM)-integrated strike doctrines, fundamentally aimed at achieving "battlespace information dominance" as a precursor to kinetic strikes. This overarching strategy, termed "informationized warfare," is considered by the PLA to be the key to controlling the battlespace and maintaining operational initiative.[24] The PLA's approach mirrors a well-established military playbook: to render enemies deaf, dumb, and blind, then engage disconnected forces with long-range precision fires.

Integral to this strategy is China's formidable electronic warfare (EW) capability. The PLA possesses both the technological capabilities and significant EW capacities to conduct extensive offensive and defensive electromagnetic spectrum operations. These operations are designed to enable, if not ensure, initial PLA information dominance in any counter-intervention scenario. The PLA's Strategic Support Force (SSF), created in late 2015, is now transformed into the Information Support Force (ISF), which focuses on building and defending China's network information systems.[25]

"The PLA possesses both the technological capabilities and significant EW capacities to conduct extensive offensive and defensive electromagnetic spectrum operations. These operations are designed to enable, if not ensure, initial PLA information dominance in any counter-intervention scenario.

A critical enabler for China's precision strike capabilities is its rapidly expanding space-based Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) infrastructure. Over the past five years, the number of PLA ISR satellites in geostationary orbit (GEO) has doubled, while those in low Earth orbit (LEO) have tripled.[27] This extensive network of surveillance and reconnaissance satellites directly enhances China's ability to detect, track, and target adversary forces and critical infrastructure with high precision, providing real-time intelligence for its missile operations. The development of robust space support infrastructure, including new space support ships such as the Liao Wang-1, is integral to the PLA's ambition to become an "informatised and intelligentised military" with global reach.[28]

The PLA recognizes the limitations of conventional air defence against drone swarms, with training exercises showing that anti-aircraft artillery is only 40% effective against small swarms.[29] This highlights the need for a layered defence combining electronic jamming, surface-to-air missiles, close-in weapon systems (CIWS), and directed energy weapons (DEWs).[30] The integration of AI-driven systems is also emphasized to counter sophisticated drone swarms and cross-domain autonomous threats, and to shorten decision-making timelines for precision targeting. The operational implication for India is that its air defence system, particularly its Integrated Air Command and Control System (IACCS) and Akashteer networks, which are designed for real-time coordination and network-centric operations, become prime targets for such multi-domain saturation attacks. If India's C4ISR is degraded or compromised, its ability to coordinate layered defence, assign targets, and prevent friendly fire will be severely hampered, even with advanced missile systems, underscoring a critical need for robust cyber and EW resilience within India's AD architecture.

- **Implications for India**

For India, China's integrated use of swarms, hypersonics, and electronic warfare presents a formidable multi-domain threat. A Chinese air campaign would likely not come as lone aircraft penetrating borders, but rather as a coordinated onslaught: swarms of drones and decoys to soak up or confuse defences, cyber/EW attacks to blind radars and cut communications, followed by precision strikes from ballistic or hypersonic missiles aimed at command nodes, and possibly backed by fighter aircraft launches of cruise missiles from standoff range. It is a scenario explicitly crafted to defeat traditional air defence and impose high costs. The PLA's own analyses acknowledge that only a layered defence combining electronic jamming, SAMs, close-in weapons, and directed-energy weapons has a hope of countering a sophisticated swarm. Thus, if India does not adapt, its current air defence architecture – however advanced on paper – could be overwhelmed by a Chinese saturation strike in the opening hours of a conflict.

This imbalance is a major driver behind India's need for a doctrinal and technological rethink of its air defence (as elaborated in later sections). Maintaining credible deterrence against China will depend on convincing Beijing that India's defences cannot be easily blinded or exhausted, and that any attempted first strike would be blunted or foiled.

While maintaining deterrence against China is primarily about countering a peer adversary, India's air defence must also contend with regional actors who pursue asymmetric approaches to exploit vulnerabilities. Understanding Pakistan's strategies is therefore essential to comprehensively assess India's air defence posture.

> A Chinese air campaign would likely come as a coordinated onslaught: swarms of drones and decoys to soak up or confuse defences, cyber/EW attacks to blind radars and cut communications, followed by precision strikes from ballistic or hypersonic missiles aimed at command nodes, and possibly backed by fighter aircraft launches of cruise missiles from standoff range. It is a scenario explicitly crafted to defeat traditional air defence and impose high costs.

Pakistan's Air Offence Doctrine

While Pakistan's technological capabilities remain comparatively limited relative to China, it has adopted innovative asymmetric approaches to challenge India's air defence systems. In recent years, Islamabad has prioritized the development and deployment of unmanned aerial systems and unconventional tactics to offset India's conventional military superiority. Consequently, Pakistan's air offence doctrine increasingly relies on the strategic employment of drones, cruise missiles, and cost-effective platforms designed to maximize operational impact by exploiting vulnerabilities within India's air defence architecture.

- **Growing Use of Drones (Burraq UCAVs, Turkish drones)**

Pakistan has made notable strides in developing and acquiring unmanned combat aerial vehicles (UCAVs). The Burraq, Pakistan's first armed UCAV, marks the development of a domestic precision-strike capability. Based on the Chinese CH-3, it is a MALE drone with a 960 km range and 12-hour endurance, capable of carrying laser-guided missiles or bombs. Demonstrated in Operation Zarb-e-Azb, it supports ISR and targeted strikes.[30]

Beyond indigenous development, Pakistan has also acquired a significant number of Turkish-origin drones. During Operation Sindoor in May 2025, Pakistan deployed a large fleet of these drones, including Bayraktar TB2 and Bayraktar YIHA-III kamikaze drones, as well as micro-drones such as Songatri and eYatri. These were launched in a mass incursion, with estimates ranging from 300 to 400 drones across 36 locations, targeting Indian military installations.[31]

Shahpar-II is a MALE drone developed by Pakistan's Global Industrial & Defence Solutions (GIDS) for intelligence, surveillance, and precision strike missions. It features a pusher-propeller configuration, high-mounted straight wings, and a V-tail. The drone is equipped with electro-optical sensors and can carry guided air-to-surface munitions. Shahpar-II has an endurance of over 14 hours and supports both day and night operations.
Source: Aaj Tak

Burraq is based on Chinese designs. It features a pusher-propeller configuration, straight wings, and a V-tail. Designed primarily for precision strike missions, Burraq is equipped with laser-guided air-to-surface missiles and has been used in counterterrorism operations within Pakistan's borders
Source: Millennium Post.

While India's Akashteer system proved highly effective in neutralizing these threats, the sheer scale of the attempted attack highlights Pakistan's strategic intent to overwhelm Indian air defences through saturation tactics. These drones could operate beyond the effective range of conventional anti-aircraft guns, such as the L70, which has an effective range of approximately 3,500 meters against aerial targets.[32] Further complicating the matter, it could be capable of operating "above 5,000–10,000 feet," revealing a deliberate strategy to exploit perceived gaps in India's low-altitude and lower-medium altitude air defence coverage.

While India possesses systems like VSHORADS and SAMAR for very short-range, low-altitude threats[33] and is acquiring Low Level Lightweight Radars (LLLWRs)[34], vulnerabilities may persist at the upper end of the low-altitude spectrum or lower end of the medium-altitude spectrum against coordinated swarm attacks. Such attacks would compel India to rely on more expensive SAMs, further depleting its missile stockpile.

Bayraktar TB2 is a Turkish MALE armed UAV designed for surveillance and precision strikes. It features a distinctive twin-boom tail, high-mounted straight wings, and a pusher-propeller configuration. The TB2 can carry up to four laser-guided munitions and has an endurance of over 24 hours.
Source: Baykar

Bayraktar Akıncı, developed by Baykar, features a twin-boom tail, turboprop engines mounted on each wing, and a large fuselage for advanced sensors and weapon systems. Akıncı can carry a wide range of munitions—including air-to-ground and air-to-air missiles—with a payload capacity of up to 1,500 kg and an endurance exceeding 24 hours.
Source: Baykar

Bayraktar YIHA-III is a low-cost loitering munition (kamikaze drone) co-developed by Turkey's Baykar and Pakistan's National Aerospace Science and Technology Park (NASTP). It uses an OMTAS-based missile fuselage with wings and rear-mounted propeller, can loiter before a precision terminal attack, and supports both runway and catapult launch modes.
Source: Defence Blog

The intent behind this drone onslaught was to saturate and overwhelm India's air defences. By attacking on multiple fronts with so many drones, Pakistan tested whether India's sensors could track everything and whether its SAMs could intercept such a high volume of targets. Some of these drones deliberately flew at altitudes of 5,000–10,000 feet – just above the effective range of India's legacy anti-aircraft guns (like the L-70) but still low enough to evade certain radars.[35]

By forcing India to expend costly interceptors against low-cost drone swarms operating at the fringes of detection, adversaries effectively impose an attrition strategy aimed at exhausting India's missile inventory and degrading its readiness over time. This incremental erosion weakens India's ability to shift quickly from defence to offence, thereby ceding strategic momentum to adversaries. This approach fits within a broader strategic pattern of probing and shaping operations, in which persistent, low-intensity incursions erode India's deterrence credibility and compel the diversion of resources to defence at the expense of offensive modernization.

- **Implications for India**

Pakistan's improvements and tactics pose a unique challenge to India's deterrence: They blur the line between low-level conflict and war. By using drones and deniable actors, Pakistan can continuously needle India (for example, drone drops of weapons to insurgents, ISR drones probing Indian airspace) without crossing the conventional war threshold. In a crisis, Pakistan's military doctrine might favor early saturation strikes – e.g., opening a conflict not with manned air raids that invite full retaliation, but with a massive drone swarm at an Indian forward division or a barrage of missiles on one airbase – hoping to throw India off balance. From India's perspective, this means its air defence must be on guard not just for the textbook scenario of Pakistani aircraft crossing the border, but for a multitude of asymmetric triggers. It underscores the need for a fundamental shift (as discussed in previous sections) toward a flexible, integrated C-UAS and missile defence posture. Pakistan's "many small punches" approach can only be countered by an air defence that is agile, omnipresent at low altitudes, and economically sustainable.

> "Pakistan's military doctrine might favor early saturation strikes – e.g., opening a conflict not with manned air raids that invite full retaliation, but with a massive drone swarm at an Indian forward division or a barrage of missiles on one airbase – hoping to throw India off balance. From India's perspective, this means its air defence must be on guard not just for the textbook scenario of Pakistani aircraft crossing the border, but for a multitude of asymmetric triggers. It underscores the need for a fundamental shift (as discussed in previous sections) toward a flexible, integrated C-UAS and missile defence posture.

If India's defences remain heavy, slow, and expensive to operate, Pakistan may perceive an opportunity to exploit them in a future skirmish or crisis. This necessitates a fundamental shift in India's counter-swarm strategy from a "one-to-one" interception mindset to a "one-to-many" counter-swarm capability, such as the Bhargavastra system under development.[36] The threat extends beyond state-sponsored military operations; Pakistani Islamist militants have also begun employing commercially acquired quadcopter drones to drop bombs and mortar shells on security forces, indicating a pervasive, low-cost asymmetric threat that complicates internal security efforts.[37]

Impact on India's Regional Deterrence and Crisis Stability

China and Pakistan exploit India's air defence vulnerabilities to impose strategic pressure and shape conflict dynamics to their advantage. China's deployment of hypersonic glide vehicles and advanced electronic warfare targets India's fragmented command and control networks, aiming to disrupt coordination and slow response times during critical phases of conflict. This capability supports China's broader strategic goal of achieving rapid operational dominance along contested borders, undermining India's ability to sustain prolonged defense or counterattacks. By focusing on saturating low-altitude defences and exploiting gaps in joint-force integration, China seeks to create confusion and force India into reactive postures, thereby securing leverage in any escalating confrontation.

Pakistan operationalizes these vulnerabilities through persistent asymmetric tactics, leveraging drone swarms and low-cost unmanned systems to overwhelm India's limited point-defence and short-range detection capabilities. This strategy aims to degrade India's air defence resilience over time, diverting resources and complicating operational planning. Strategically, Pakistan's use of saturation attacks aligns with its doctrine of protracted, hybrid conflict, designed to stretch Indian forces thin and maintain a constant state of pressure without provoking full-scale war. By exploiting coordination challenges among India's tri-service forces, Pakistan aims to maximize disruption and exploit windows of opportunity for cross-border incursions or grey-zone escalations, keeping India on the defensive.

- **Deterrence by Denial Under Strain**

The exploitation of these vulnerabilities by China and Pakistan carries profound implications for India's broader strategic posture. It directly challenges the principle of deterrence by denial, which depends on maintaining a credible air defence capable of deterring adversaries by convincing them that any attack would fail. India's traditional reliance on a strong Indian Air Force and surface-to-air missile (SAM) network embodies this approach, but identified weaknesses—such as low-altitude detection gaps, limited AWACS coverage, and slow tri-service integration—threaten to undermine its effectiveness.

For example, Pakistan's use of large-scale drone swarms signals to Indian planners that key installations are not impervious. Conversely, it may embolden Pakistani leadership to believe that under the right conditions, India's defences could be overwhelmed. If Islamabad concludes that saturation drone attacks could degrade India's armoured brigades or disable forward air defences long enough to achieve tactical gains, it may lower the threshold for conflict initiation or escalate grey-zone tactics during crises. This dynamic fuels Pakistan's strategy of "bleeding" India through persistent low-level provocations, exploiting perceived defence gaps to incrementally erode deterrence as India hesitates to escalate in response to attacks below a critical threshold.

- **Escalation Risks and Miscalculation**

The introduction of swarms and hypersonics creates what analysts call "use-it-or-lose-it" pressures and compresses decision-making time, destabilizing. If India detects what appears to be a massive drone swarm headed toward its forces, the pressure to respond quickly (possibly even pre-emptively across the border) will be immense – rapid decisions could lead to mistakes or inadvertent escalation. Similarly, if Pakistan fears India's superior conventional forces, it might be tempted to use a saturation strike early in a conflict to compensate – for example, launching a barrage of drones and missiles at the outset (as it did on May 7–8,

2025) in hopes of gaining an early advantage. Such an attack, even if conventionally armed, could be misinterpreted by India as a prelude to something larger (like a nuclear strike on the horizon), thereby triggering escalation.

- **Diplomatic Leverage and Psychological Effect**

Perceptions of vulnerability or strength in air defence also translate to diplomatic leverage in peacetime disputes or standoffs. If India's defences are believed to be porous against certain threats, China or Pakistan could use the implicit threat of those capabilities as bargaining chips. For example, during border talks, Chinese negotiators may subtly allude to the PLA's advanced capabilities in hypersonic missile technology and electronic warfare as a strategic signal to caution against escalation, implying that China possesses the means to inflict damage through avenues that are difficult for India to counter effectively. On the other hand, if India demonstrably improves its air defence (for instance, by publicizing successful tests of anti-drone lasers or conducting live intercept drills), it strengthens India's hand by showcasing resilience. In 2021–22, the deployment of the S-400 system in India was seen as a major boost to India's strategic deterrence; indeed, during the 2025 conflict, the S-400's successful interception of a Pakistani missile raid was highlighted as enhancing India's deterrence. Such feats have a psychological impact: adversaries take note when their cutting-edge attacks are blunted. The fact that, by May 10, 2025, Pakistan had "virtually no observable damage" to show for its drone and missile attacks, while India had hit multiple Pakistani targets precisely, shifts the perception of who holds the advantage. It not only deterred Pakistan from going further in that crisis, but will also induce caution in the near term.

Responding to the Challenge: Priorities for India's Air Defence

To address the strategic and operational challenges described in the previous sections, India will need to reframe its approach to air defence. Unlike a stand-alone switch, air defence will need to be nested within a concept of operations that explicitly links it to a campaign plan through which a joint force ends the strategic threat, in which active air defence is only part of the solution.[38]

Building the Architecture: Integration, Innovation, and Resilience

India's air defence (AD) structure, built incrementally since the 1970s, was designed for an era when the principal threat was from aircraft and stand-off missiles. It evolved into a "layered umbrella" — long-range missiles like S-400 and Barak-8 for high-altitude threats, Akash and Pechora for medium-range threats, and guns or MANPADS for close defence. Each layer was organized by service, geography, and threat type.

But this layered approach is struggling to adapt to what the military strategist Paul Scharre calls the saturation age of air warfare[39] — when thousands of cheap, autonomous drones and loitering munitions arrive in waves that no linear hierarchy can manage. The architecture must therefore move from layered to adaptive, from static coverage to fluid orchestration.

An adaptive air defence architecture is characterized by five principles:

- **Distributed Sensing:** Every sensor — radar, camera, EW antenna, drone, or soldier's tablet — contributes to a shared air picture.

- **Decentralized Control:** Tactical nodes can make autonomous fire decisions based on proximity and rules of engagement (ROE).
- **Dynamic Tasking:** Assets shift roles dynamically; an EW node becomes a tracker, a radar becomes a jammer, a UAV becomes a decoy.
- **Resilience-by-Redundancy:** Multiple independent networks ensure continuity if one grid is degraded.
- **Cost Discipline:** Interceptors must match the economics of the threat — guns and jammers before missiles.

This architecture must blend hard-kill and soft-kill effects, link electronic warfare with kinetic fires, and integrate drones as both sensors and interceptors. India's future AD system should look less like a missile wall and more like a digital nervous system — sensing, prioritizing, and responding through a single kill chain.

Toward a Principle of Architecture: Three Abilities for the Drone Era

Experts have proposed that India's counter-drone architecture rests on three interlinked abilities — detection, survival, and sustainment. These can serve as the core design principles for future AD reforms.

- **Ability to Pick Up and Respond to Small Vectors:**

Detecting small, low-RCS (radar-cross-section) targets presents significant challenges — effective architectures therefore rely on diverse, multi-sensor/algorithmic integration to compensate for weak returns and heavy clutter.[40] Instead of a few powerful radars, India must field thousands of small, overlapping sensors — short-range 3D radars, electro-optical (EO) cameras, acoustic detectors, and RF sniffers. These feed into local Akashteer nodes that use AI algorithms to classify and prioritize threats. Integration with civilian networks, such as airport radars and ADS-B receivers, can help filter false positives. The response mechanism must be automatic: once a target is verified, local guns, MANPADS, or jammer drones engage without waiting for top-down clearance.

- **Ability to Survive Despite Extensive Attack:**

Survivability begins with redundancy. Every radar and EW node should have backup power, frequency agility, and mobility. Decentralized C2 cells ensure that if one node is knocked out, others assume control. Camouflage, mobility drills, and signature management — long-neglected skills — must be revived. Additionally, communications must operate in multiple bands (HF, SATCOM, and fiber) to prevent single-point failure.

- **Ability to Sustain Operations Under Stress:**

Air defence is an ammunition-intensive enterprise. In a swarm scenario, thousands of rounds may be fired in a matter of minutes. Logistic resilience demands pre-stocked magazines, forward ammunition points, and automated resupply through UAVs or robotic carriers. BEL and OFB should develop modular ammunition pods for quick reloading of 35 mm and 40 mm guns. The focus must shift from individual kills to sustained operational tempo.

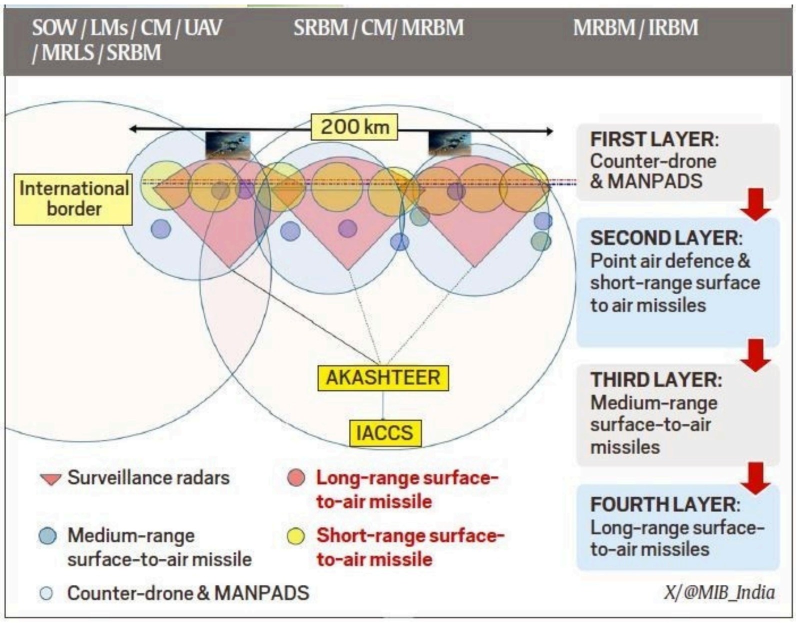
These three principles — detect, survive, sustain — convert air defence from a reactive shield into a living system capable of enduring saturation and chaos.

Layer Overview: India's Multi-Tiered Air Defence Architecture

India's air-defence posture remains a multi-ringed construct designed to intercept aerial threats as they close in — from long-range standoff fires to short-range drones and rockets — but that architecture is now evolving rapidly. Recent experiments and integration tests have accelerated that evolution: India has begun running more realistic, multi-sensor, multi-effector trials that demonstrate simultaneous engagement across tiers and showcase the possibilities (and limits) of an integrated kill web. At the same time, legacy shortfalls — low-altitude detection gaps, logistics and magazine stress, and network vulnerability to saturation and EW — persist and must be weighed against these recent advances.

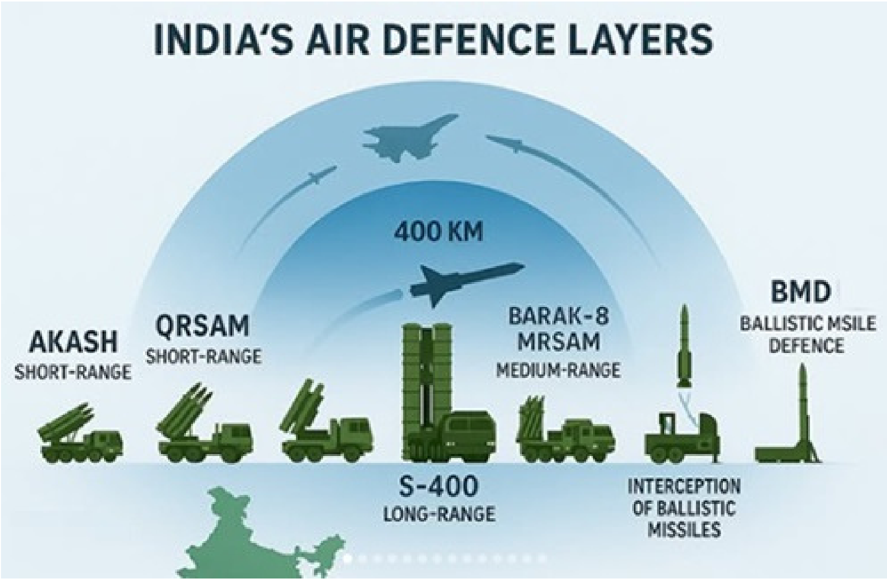
Strategic Layer (≈400–100 km): India's Outer Shield

At the apex sits India's long-range SAM capability: imported S-400 batteries enlarge denial depth and complicate an adversary's standoff calculus. The S-400 provides an outer umbrella that extends detection and engagement reach and — by its mere presence — strengthens strategic deterrence. Media coverage during the May 2025 crisis emphasised that India's long-range assets were an important element of that response, even as official accounts focused more generally on the integrated defensive posture rather than naming individual systems. Government summaries of Operation Sindoor emphasised the role of integrated, networked AD responses, while some reporting attributed successful interceptions to S-400 batteries (these claims were widely reported in the press, even where official releases remained circumspect).



Strategically, India is also pushing indigenous capabilities to complement S-400 coverage. DRDO's longer-horizon Ballistic Missile Defence (BMD) programme continues: the AD-1/AD-2 interceptor family and related sensors aim to add exo and endo-atmospheric layers that will, over time, close the gap above ~100 km and provide a comprehensive strategic envelope. The long-term objective is a layered strategic shield in which indigenous interceptors and long-range systems operate alongside imported systems to reduce single-point dependence. (See also the DRDO integrated-AD test coverage below.)

S-400s are powerful but not panaceas. Terrain and deployment constraints — particularly in the Himalaya and other high-relief sectors — slow emplacement and reduce continuous coverage. They also remain susceptible to coordinated multi-domain attacks (EW, loitering munitions, decoys) intended to saturate or blind long-range sensors. Reported combat use in 2025 highlights the deterrent effect, but it must be read alongside the larger point: strategic-range interceptors buy time and shape, they do not guarantee invulnerability.



Source: Sankritiias

Medium Layer (≈100–30 km): The Core Engagement Belt

This band is the workhorse of India's AD posture — where most engagements against aircraft, cruise missiles, and larger loitering munitions should occur. Key systems include the Indo-Israeli Barak-8 family (MR-SAM), the indigenously matured Akash family, and mobile SR/MR complements such as SPYDER. Barak-8 continues to provide a long-end medium reach and maritime/land interoperability; its multi-function radars and cooperative engagement modes let networked shooters cover approaches in depth.

The Akash family remains central to the domestic medium-range layer. Newer variants (Akash Prime and Akash-NG) have demonstrated improved seekers, electronic counter-countermeasure features, and high-altitude performance — tests in 2025 validated Akash Prime in rarefied, high-altitude conditions, underlining its growing operational utility for the northern and eastern theatres.

Crucially, India has also begun to validate integrated medium-layer behaviour in more realistic scenarios: Akashteer nodes tied into the IACCS mesh have been field-validated in

“ The Akash family remains central to the domestic medium-range layer. Newer variants (Akash Prime and Akash-NG) have demonstrated improved seekers, electronic counter-countermeasure features, and high-altitude performance — tests in 2025 validated Akash Prime in rarefied, high-altitude conditions, underlining its growing operational utility for the northern and eastern theatres.

live trials and validation exercises (one Akashteer–IACCS integration site reached a successful operational demonstration), illustrating how Army and Air Force sensors and shooters can now cooperate more tightly than before. That trend — connecting Akash, Barak-8, and regional radars into a fused picture — is the most operationally significant development in the medium band.[41]

Medium-range systems are more flexible than strategic interceptors, but they are also the most likely place to bleed missile inventories during prolonged swarm or saturation attacks. The solution is not just more missiles; it is better prioritisation (soft-kill first), a larger inventory of low-cost interceptors, and tightly integrated cueing from lower-altitude sensors that reduce wasteful launches.

Tactical & VSHORAD Layer (≈30–0.5 km): Point Defence and Inner Protection

The innermost rings protect airfields, logistics hubs, and fielded formations. The QRSAM (Quick Reaction Surface-to-Air Missile) programme — developed to be highly mobile and to provide quick engagement for manoeuvre forces — has completed multiple development and user trials and is moving toward finalisation, with user trials and procurement planning progressing in the mid-2020s. Meanwhile, VSHORADs (MANPADS), upgraded gun systems (Shilka, L-70 with proximity rounds), and short-range adapted CIWS solutions form the immediate point-defence mix.[42]

Recent operational experience and exercises have underlined the comeback of high-rate gun and soft-kill layers: programmable airburst rounds fired from gun systems, combined with portable EW pods and HPM/DEW experimentation, offer a cheaper first line against FPVs and small loiterers. This tactical layer now increasingly includes mobile C-UAS kits and interceptor drones specifically intended for close-in engagements.

QRSAM test as part of Integrated Air Defence Weapon System (23 August 2025).
Source: Press Information Bureau, Ministry of Defence, Government of India

The tactical ring is arguably the most stressed by current threat economics. Small FPVs and micro-UAS exploit low-altitude clutter and challenge radar discrimination; hence, the tactical layer needs a mosaic of EO/IR, RF sniffers, acoustic sensors, aerostats/HAPS, and dense short-range radars (LLLWR). Guns and jammers must operate in close coordination to avoid fratricide and friendly-jamming incidents — a problem India has already encountered in limited form during prior high-intensity operations.

Underpinning these layers is a network-centric C4ISR backbone

IACCS (Integrated Air Command & Control System): A secure, IP-based grid that fuses data from ground radars, airborne platforms (AWACS, UAVs), and civilian ATC radars into a Recognized Air Picture, enabling centralized monitoring and tasking of SAM batteries.

- **Akashteer:** The Army's mobile C2 system, linked into IACCS at key nodes, which automates sensor-to-shooter loops for Akash and QRSAM units. Together, IACCS and Akashteer form a de facto Joint Air Defence Centre, smoothing Army–Air Force coordination.
- **TRIGUN (Naval Integration):** Progress continues toward integrating the Navy's Trigun/Shikari radars and Barak 8 on warships into the joint IACCS network—expanding maritime surveillance and enabling coastal defence assets to feed into the national AD grid.

Akashteer ('Sky Arrow') is an AI-enabled, fully automated Air Defence Control & Reporting System, which is designed, developed and manufactured by Bharat Electronics in collaboration with Defence Research and Development Organisation and Indian Space Research Organisation. Source: BEL

Over the past year, the emphasis has shifted from isolated capability to integrated behaviour: DRDO and industry have moved to demonstrate multi-target, coordinated intercepts across tiers. Notably, DRDO announced maiden flight tests of an Integrated Air Defence Weapon System (IADWS) — a bundled, multi-layer engagement demonstration that simulated layered interception and multi-target engagement — marking a milestone in demonstrating indigenous integrated behaviours at scale.[43] These trials do not eliminate operational frictions. Tests show the technical feasibility of a joint kill-web; the larger challenges are doctrinal, logistical, and human: aligning rules of engagement, delegated authority, spectrum discipline, and ammunition resilience so the integrated picture produces timely, economical shooter decisions on the ground.

Addressing Immediate Gaps Through Interim Alternatives

Budgetary Flexibility and Procurement Acceleration

In the immediate term, while long-term policies and large-scale procurements are underway, India must prioritize swift, actionable measures to plug critical gaps and enhance readiness. Financially, the Defence Ministry has confirmed there is no shortage of capital expenditure, with efforts already underway to accelerate contract signing and improve fund absorption, aiming to reduce weapon-buying timelines from 5-6 years to 2 years.[44] This budgetary flexibility should be immediately leveraged to fast-track critical acquisitions and upgrades.

Upgrading Legacy Air Defence Guns and Radars

Concurrently, immediate upgrades to existing low-level air defence guns and radars with advanced fire control and thermal imaging capabilities are crucial to enhance their effectiveness against low-flying drones and loitering munitions. The Ukraine conflict has shown that high-rate gun systems remain indispensable. The German Gepard's 35 mm Oerlikon cannons achieved a kill rate of nearly 85% against Shaheds, using programmable ammunition that detonates at precise distances.[45] Ukraine's modification of older Soviet guns (Shilka, ZU-23) with digital sights also proved decisive. Similarly, Israel's new Iron Sting 120 mm system integrates radar, laser, and EO sensors to engage low-flying drones.[46] India's legacy L-70 and Shilka systems, if upgraded with modern radars and proximity-fused rounds, can fill this cost-effective niche.

Strengthening Low-Level Surveillance

The ongoing procurement of 10 Low Level Lightweight Radar (LLLWR) systems by the Indian Army, designed to detect micro-drones with exceptionally small radar cross-sections, should be expedited, along with the rapid deployment of existing specialized counter-UAS systems, such as Bharat Electronics' Anti-Drone System, in vulnerable border areas and high-value targets.[47]

Addressing AWACS Vulnerabilities and operationalisation of S-400

Addressing the aging Israeli-origin Phalcon AWACS fleet, which faces maintenance issues due to its Russian-manufactured airframes, requires exploring immediate leasing options or accelerating the procurement of additional AWACS platforms to bolster early warning and surveillance capabilities.[48] Furthermore, the successful operationalization and full integration of the three currently deployed S-400 squadrons in north-west and east India must be ensured, while contingency plans are developed for potential delays in the delivery of the remaining two squadrons from Russia.

Doctrinal Innovation and Drone Defence Units

Doctrinally, immediate conceptualization and pilot programs for "Drone Defence Units" at Brigade/Corps levels should commence, focusing on training personnel to operate existing and newly acquired counter-drone systems.[49] This includes enhancing real-time intelligence sharing and rapid-response protocols for cross-border drone incursions, leveraging existing surveillance assets such as UAVs, advanced satellite systems, and thermal imagers to identify and neutralize threats immediately.

Long-Term Measures: Building a Resilient, Adaptive Kill Chain

Over the longer horizon, India needs a doctrinal and industrial reset to transition from a fragmented, platform-centric air defence model to a resilient, networked, and adaptive kill chain. This implies a shift in both mindset and planning — from deploying radars and interceptors in isolated pockets to engineering an ecosystem that can detect, decide, and destroy threats autonomously across domains.

Establishing Cooperative Engagement Capability & Joint Engagement Zones

A key priority is investing in Cooperative Engagement Capability (CEC) and Joint Engagement Zones (JEZ) — technologies that enable different sensors and shooters to operate as a single distributed network. The US Navy's Naval Integrated Fire Control-Counter Air (NIFC-CA) program demonstrates how radar on one platform can cue interceptors on another in real-time, creating seamless coverage and distributed lethality. The Ministry of Defence should formally mandate the expansion of Akashteer–IACCS integration to multiple regional nodes, prioritizing rollout in western and northern theatre commands by the end of 2026. Already, one Akashteer site is fully integrated with the IAF's Integrated Air Command & Control System (IACCS), and systems are being progressively deployed at additional locations.[50] This multi-site integration should be reinforced through a tri-service JEZ doctrine, creating a unified kill chain in which sensors and shooters across the Army, Air Force, and Navy act cohesively.

Indigenisation of Critical Subsystems: Radars, Seekers, and Data Links

Another long-term objective must be the indigenisation of critical air defence subsystems — such as seekers, dual-pulse motors, and secure data links — to break dependence on single-source supply chains, such as those from Russia or Israel. Without control over key components, India's air defence readiness will remain hostage to geopolitical disruptions. Strategic partnerships under the iDEX and DPEPP frameworks must go beyond prototypes and push towards production-scale timelines. Just as South Korea partnered with local firms to co-develop the KM-SAM with Russian assistance and eventually built its own systems[51], India must look beyond Transfer of Technology (ToT) and create long-term innovation loops.

Architectures for Saturation Resilience: Redundant and Integrated AD Layers

In parallel, India must build a saturation-resilient air defence architecture. This means accounting for the fact that in future wars, the threat will not come in the form of isolated missile launches or slow-moving aircraft, but as swarms, salvos, and multi-domain coordinated attacks. Every major conflict from Nagorno-Karabakh to Ukraine illustrates this shift. India should accordingly plan for redundant radar networks, mobile launcher units, distributed energy-based defence (DEW), and deception capabilities like false emitters and inflatable decoys. It also requires a new generation of low-cost interceptors — akin to Israel's Tamir missiles or South Korea's Chiron — that can be fielded in large numbers without budgetary strain.

Modern AD systems no longer rely solely on kinetic effectors. The integration of soft-kill (jamming, spoofing, cyber denial) and hard-kill (missile or gun) options is central to sustainability. In Ukraine, EW systems like Bukovel and Nota routinely jam GPS and video feeds of Russian drones, while guns finish off the stragglers. Israel's Drone Dome and NATO's C-UAS "effector chains" employ the same principle: a soft kill first, followed by kinetic engagement only if necessary. India's future C-UAS doctrine must embed this sequence into engagement logic. EW pods and jammers should attempt disruption first; guns and MANPADS should engage only drones that resist or reappear. This approach drastically reduces ammunition expenditure and preserves SAM stocks for higher-value threats.

Reimagining Air Defence Deterrence through Demonstrable Resilience

Lastly, India's military planners must reimagine deterrence in the air defence domain. Deterrence is no longer based solely on retaliation; it is increasingly about the proven ability to deny objectives in real-time. A credible AD posture today requires demonstrable capability, tested resilience, and strategic signalling — not just classified inventory. India should publicly conduct interception tests, release footage of successful drone swats, and showcase redundancy drills to deter adversaries from probing its defences in peacetime or in grey-zone environments.

India's future deterrence credibility will therefore rest on three pillars:

- Visible Readiness: Regular demonstrations of counter-drone drills and public interception footage create psychological deterrence.
- Operational Continuity: The ability to maintain air operations and logistics even under saturation attack sustains strategic tempo.
- Adaptive Recovery: Rapid reconstitution of damaged sensors or launcher signals so that India cannot be paralyzed by surprise strikes.

By institutionalising resilience, India can convert air defence from a static shield into a dynamic system of denial.

Procurement and Industrial Roadmap

Short-Term (0–3 years): Quick Wins	Medium-Term (3–7 years): Institutionalization	Long-Term (7–15 years): Transformation
Upgrade Legacy Guns: Modernize all L-70 and Shilka batteries with EO sights, proximity rounds, and networked fire control.	**Akash-NG and QRSAM Expansion**: Equip all operational commands with modular launchers capable of anti-drone engagements.	**Full-Spectrum Kill Web**: Expand Akashteer–IACCS to a nationwide integrated air picture including civil radars and satellites.
Field C-UAS Batteries: Deploy BEL's Drone Kill Systems at major airbases and forward command posts.	**Directed-Energy Pilots**: Deploy HEL prototypes in Rajasthan and Punjab sectors for testing.	**Operational Lasers and Microwaves**: Field truck-mounted DEWs and high-power microwave systems for base defence.
Stockpile Ammunition: Restart 40 mm and 35 mm shell production with proximity fuses.	**Joint Air Defence Command Operationalization**: Establish tri-service HQ with subordinate regional commands.	**Drone-on-Drone Warfare Units**: Raise dedicated interceptor UAV squadrons in each Theatre Command.
Integrate EW: Connect Samyukta and Himshakti EW nodes with Akashteer command centers.	**AI-Based Threat Classification**: Integrate machine-learning algorithms into Akashteer for automated drone identification.	**AI Autonomy**: Enable autonomous engagement of drones under human-on-the-loop oversight.
Joint Exercises: Conduct live drills simulating drone swarms and electronic denial across services.	**Indigenous C-UAS Manufacturing**: Encourage private industry (IdeaForge, Zen Technologies, Tonbo Imaging) to develop interceptor drones and radar–EO pods.	**Export and Collaboration**: Position India as a C-UAS exporter, leveraging DRDO-BEL systems for partner nations in ASEAN and Africa.

Conclusion

The strategic audit of India's air defence architecture presented in this report leads to an inescapable conclusion: the paradigm of "deterrence by denial," historically predicated on the physical interdiction of manned aircraft via layered missile screens, is approaching a terminal crisis of relevance. The proliferation of low-cost, autonomous unmanned systems—exemplified by the "Operation Sindoor" crisis and the broader commoditization of precision strike capabilities—has fundamentally inverted the economics of air superiority. India faces a security environment where adversaries like China and Pakistan have operationalized "cost asymmetry" as a central tenet of their offensive doctrines, leveraging swarm tactics to exhaust high-value interceptors and saturate command nodes. Consequently, the imperative for New Delhi is no longer merely the modernization of legacy platforms, but a structural migration toward a "Kill Web" architecture defined by distributed lethality, sensor fusion, and economic sustainability.

The most immediate strategic vulnerability identified is the "opening hour" fragility of the current centralized command architecture. In a high-intensity engagement, the reliance on a limited number of high-power sensors and hierarchical C2 nodes creates single points of failure that peer adversaries are specifically drilling to exploit. China's concept of "multi-domain precision saturation" is designed to blind these centralized nodes before kinetic engagement begins. Therefore, the proposed shift to a Detect-Survive-Sustain framework is not doctrinal jargon but a survival necessity. By replacing the linear "shield" model with a decentralized mesh of thousands of low-cost sensors—LLLWRs, RF sniffers, and acoustic arrays—India can illuminate the low-altitude blind spots that currently grant impunity to FPV and loitering munitions. This distributed sensing capability is the prerequisite for the "Survive" function, ensuring that the degradation of individual nodes does not collapse the broader Recognised Air Picture (RAP).

> India faces a security environment where adversaries like China and Pakistan have operationalized "cost asymmetry" as a central tenet of their offensive doctrines, leveraging swarm tactics to exhaust high-value interceptors and saturate command nodes. Consequently, the imperative for New Delhi is no longer merely the modernization of legacy platforms, but a structural migration toward a "Kill Web" architecture defined by distributed lethality, sensor fusion, and economic sustainability.

Furthermore, the economic dimension of air defence must be treated as a decisive operational variable. The current exchange ratio—expending kinetic interceptors priced in the millions against disposable platforms priced in the thousands—is a trajectory toward magazine exhaustion. To restore deterrence, India must institutionalize a "Soft-Kill First" hierarchy. This requires breaking the institutional silos that currently segregate Electronic Warfare (EW) from kinetic Air Defence. In the proposed architecture, EW is not an ancillary support function but the primary layer of engagement, tasked with disrupting swarms at zero marginal cost per engagement. Kinetic interception must be reserved for "leakers" and high-value targets, thereby preserving magazine depth for the ballistic and cruise missile threats that will inevitably follow the initial drone wave.

Operationally, the path forward demands the urgent fusion of service-specific networks into a genuine Joint Engagement Zone (JEZ). The integration of the IAF's IACCS and the Army's Akashteer systems cannot remain an aspirational goal; it must be the baseline for theatre-level operations. Current fragmentation creates latency in the sensor-to-shooter loop, a delay that is fatal against autonomous swarms operating at machine speed. The roadmap outlined in this report—prioritizing the "quick win" retrofitting of legacy gun systems with programmable ammunition while simultaneously pursuing long-term indigenization of directed energy weapons (DEWs) and AI-driven command systems—offers a phased approach to closing these gaps.

Ultimately, the credibility of India's deterrence will depend on convincing Beijing and Islamabad that their saturation strategies will fail to achieve paralysis. This requires a transition from "visible capacity" (parading S-400s) to "demonstrable resilience" (publicizing rapid reconstitution drills and counter-swarm effectiveness). By building an ecosystem that is economically sustainable, structurally redundant, and technologically agile, India can deny its adversaries the strategic utility of the drone swarm. The goal is not just to intercept incoming fire, but to render the saturation attack an inefficient and futile avenue of coercion. In the drone age, the victor will not be the side with the most missiles, but the side with the most resilient network.

> Operationally, the path forward demands the urgent fusion of service-specific networks into a genuine Joint Engagement Zone (JEZ). The integration of the IAF's IACCS and the Army's Akashteer systems cannot remain an aspirational goal; it must be the baseline for theatre-level operations. Current fragmentation creates latency in the sensor-to-shooter loop, a delay that is fatal against autonomous swarms operating at machine speed.

Endnotes

[1] Surendra Singh. “Can’t Win Today’s Warfare with Yesterday’s Weapons, desi Drone Tech Must: CDS General Anil Chauhan.” The Times of India, 17 July 2025, https://timesofindia.indiatimes.com/india/cant-win-todays-warfare-with-yesterdays-weapons-desi-drone-tech-must-cds-general-anil-chauhan/articleshow/122592318.cms
[2] “Tiny 10-inch FPV drone with 11-pound payload power introduced in Ukraine.” Interesting Engineering, 29 Oct. 2024, https://interestingengineering.com/military/tiny-10-inch-fpv-drone-with-11-pound-payload-power-introduced-in-ukraine
[3] Zampronha, Daniel, and Aline Albuquerque. “Cheaper Precision Weapons: An Exploratory Study about the HESA Shahed 136.” Advances in Aerospace Science and Technology, vol. 9, 2024, pp. 40–59. https://www.scirp.org/pdf/aast_2024031813573106.pdf
[4] Mehdi, Syed Eesar, and Toseef Ahmad Bhat. “Understanding Pakistan’s Unmanned Aerial Vehicle (UAV) Programme.” International Centre for Peace Studies, 28 Mar. 2024, https://www.icpsnet.org/comments/Pakistan-Unmanned-Aerial-Vehicle-UAV-Programme
[5] Haider, Usman. “India’s Evolving Air Defence Capabilities and Options for Pakistan.” Journal of Security & Strategic Analyses, vol. 11, no. 1, July 2025, pp. 88–109. https://www.researchgate.net/publication/393296093_India's_Evolving_Air_Defence_Capabilities_and_Options_for_Pakistan/download
[6] Peri Dinakar, “IAF looking at 12 early warning aircraft under two different programmes.” The Hindu, 6 Oct. 2024. https://www.thehindu.com/news/national/iaf-looking-at-12-early-warning-aircraft-under-two-different-programmes/article68725847.ece
[7] Haider, Usman. “India’s Evolving Air Defence Capabilities and Options for Pakistan.” Journal of Security & Strategic Analyses, vol. 11, no. 1, 2025, pp. 88–109. https://www.researchgate.net/publication/393296093_India's_Evolving_Air_Defence_Capabilities_and_Options_for_Pakistan/download
[8] “Indian Army bolsters air defence with procurement of 10 Low-Level Lightweight Radars.” Indian Defence Research Wing, 14 July 2025,https://idrw.org/indian-army-bolsters-air-defence-with-procurement-of-10-low-level-lightweight-radars/
[9] Jee, Sudhakar. “Network-Centric Warfare: Pakistan’s edge and India’s wake-up call.” India Sentinels, 21 July 2025, https://www.indiasentinels.com/opinion/network-centric-warfare-pakistans-edge-and-indias-wake-up-call-6933
[10] Chansoria, Monika. “’Informationising’ Warfare: China Unleashes the Cyber and Space Domain.” Centre for Land Warfare Studies (CLAWS), Jan. 2010. https://claws.co.in/wp-content/uploads/2025/01/MP20_Informationising-Warfare-China-Unleashes-the-Cyber-and-Space-Domain.pdf
[11] Katoch, P.C. “Foreclosure of Army’s Battlefield Management System.” SP’s Land Forces, 10 Jan. 2018, https://www.spslandforces.com/experts-speak/?id=336&h=Foreclosure-of-Army-s-Battlefield-Management-System#:~:text=Pak%2DIBMS(Rehbar)%20also%20facilitates%20commanders%20in%20remote%20firing%20of%20AAMG%20by%20auto%20tracking%20the%20aerial%20and%20ground%20targets%20from%20inside%20the%20tank.
[12] Kryzhanivska, Olena. “Stopping Shaheds: Ukraine’s Solutions.” Ukraine’s Arms Monitor, 19 July 2025, https://ukrainesarmsmonitor.substack.com/p/stopping-shaheds-ukraines-solutions?utmsource=substack&utmmedium=email
[13] Di Mizio, Giorgio, and Michael Gjerstad. “Ukraine’s Ground-Based Air Defence: Evolution, Resilience and Pressure.” International Institute for Strategic Studies, 24 Feb. 2025, https://www.iiss.org/online-analysis/military-balance/2025/02/ukraines-ground-based-air-defence-evolution-resilience-and-pressure/#:~:text=24th%20February%202025-,Ukraine's%20ground%2Dbased%20air%20defence:%20evolution%2C%20resilience%20and%20pressure,support%20at%20current%20levels%20uncertain.
[14] Encarnacion, Ethan M. “Ukraine Unveils New System That Links ‘Thousands’ of EW Drones.” The Defense Post, 10 July 2025, https://thedefensepost.com/2025/07/10/ukraine-system-ew-drones/
[15] “India’s Robust Air Defence System Highlights Vulnerabilities On Unproven Chinese Technology.” Indian Defence News, 10 May 2025, https://www.indiandefensenews.in/2025/05/indias-robust-air-defence-system.html
[16] “BEL develops customisable drone detection radar with 360-degree coverage.” Bharat Electronics Ltd, 14 Dec 2021, https://bel-india.in/news-bel/bel-develops-customisable-drone-detection-radar-with-360-degree-coverage/
[17] “Electronic Warfare.” Defence Research and Development Organisation, Ministry of Defence, Government of India, https://drdo.gov.in/drdo/en/offerings/technology-foresight/electronic-warfare

Endnotes

[18] “DRDO tests directed energy weapon system that can disable drones, missiles.” The Hindu, 13 Apr 2025. https://www.thehindu.com/news/national/drdo-tests-directed-energy-weapon-system-that-can-disable-drones-missiles/article69446266.ece#:~:text=The%20Defence%20Research%20and%20Development%20Organisation%20(DRDO),*%20Destroying%20enemy%20surveillance%20sensors%20and%20antennae
[19] “China PLA Way of War – Active Defence & MDPW.” Security Risks, 16 Dec. 2022, https://www.security-risks.com/post/china-pla-way-of-war-active-defence-mdpw#:~:text=Soldiers%20and%20the%20people%20are,these%20future%2Doriented%20operational%20concepts.
[20] Nithiyanandam, Y. “Shifting Shadows: Military Radar Dynamics in Tibet.” Takshashila Geospatial Bulletin, 30 Aug. 2023 https://geospatialbulletin.takshashila.org.in/p/shifting-shadows-military-radar-dynamics
[21] Jha, Mausam. “China’s air power expansion along LAC revealed in latest satellite images.” LiveMint, 1 June 2023 https://www.livemint.com/news/world/chinas-air-power-expansion-along-lac-revealed-in-latest-satellite-images-11685595057695.html
[22] “China Drone Mothership Jiu Tian Features Swarm Capabilities, Global Security.” Firstpost, Firstpost Media, 2025, https://www.firstpost.com/explainers/china-drone-mothership-jiu-tian-features-swarm-capabilities-global-security-13889954.html#:~:text=With%20stealth%20capabilities%2C%20high%2Daltitude,many%20modern%20air%20defence%20systems.
[23] Chawla, A.K. “China’s Strategy of ‘Informationised and Intelligent’ Warfare.” SP’s Naval Forces, Feb 2022, https://www.spsnavalforces.com/story/?id=802&h=Chinas-Strategy-of-Informationised-and-Intelligent-Warfare#:~:text=Thus%2C%20the%20Informationised%20War%20doctrine,onforce%20competition%20with%20the%20US.
[24] Dahm, J. Michael. “China C4ISR and Counter-Intervention.” Mitchell Institute for Aerospace Studies, 21 Mar. 2024, https://www.mitchellaerospacepower.org/app/uploads/2024/03/03.21.24-PLA-C4ISR-USCC-Testimony.pdf
[25] Meia Nouwens. “China’s New Information Support Force.” IISS, 3 May 2024, https://www.iiss.org/online-analysis/online-analysis/2024/05/chinas-new-information-support-force/#:~:text=On%2019%20April%202024%2C%20the,Logistics%20Support%20Force%20(JLSF).
[26] Dahm, J. Michael. “China C4ISR and Counter-Intervention.” Mitchell Institute for Aerospace Studies, 21 Mar. 2024, https://www.mitchellaerospacepower.org/app/uploads/2024/03/03.21.24-PLA-C4ISR-USCC-Testimony.pdf
[27] Nouwens, Meia. “China’s Dual-Use Space Sector Goes Global.” IISS, 17 July 2025, https://www.iiss.org/online-analysis/charting-china/2025/07/chinas-dual-use-space-sector-goes-global/
[28] Suciu, Peter. “China’s Military Just Tried to Fight a ‘Drone Swarm’. It Didn’t Go Well.” The National Interest, 10 Sept. 2024, https://nationalinterest.org/blog/buzz/chinas-military-just-tried-fight-drone-swarm-it-didnt-go-well-212679
[29] Cheung, Sunny, and Joe McReynolds. “Autonomous Battlefield: PLA Lessons from Russia’s Invasion of Ukraine.” Jamestown China Brief, vol. 25, no. 6, 28 Mar. 2025, https://jamestown.org/program/autonomous-battlefield-pla-lessons-from-russias-invasion-of-ukraine/
[30] Ansari, Usman. “Pakistan Surprises Many With First Use of Armed Drone.” Defense News, 8 Sept. 2015, www.defensenews.com/air/2015/09/08/pakistan-surprises-many-with-first-use-of-armed-drone/.
[31] “Bayraktar busted: Pakistan’s drone fiasco — How Indian radars exposed Turkish tech.” The Times of India, 30 May 2025, https://timesofindia.indiatimes.com/india/bayraktar-busted-pakistans-drone-fiasco-how-indian-radars-exposed-turkish-tech/articleshow/121519222.cms
[32] “China-Pakistan axis may deploy high-flying swarm drones to challenge Indian air defences.” IDRW, 14 July 2025, https://idrw.org/sino-pak-axis-may-deploy-high-flying-swarm-drones-to-challenge-indian-air-defences-warns-analyst/
[33] “India’s Defence Future: DRDO’s Ambitious 10-Year Vision.” Indian Defence News, 15 July 2025, https://www.indiandefensenews.in/2025/07/indias-defence-future-drdos-ambitious.html
[34] “Indian Army Bolsters Air Defence with Procurement of 10 Low-Level Lightweight Radars.” IDRW, 13 July 2025, https://idrw.org/indian-army-bolsters-air-defence-with-procurement-of-10-low-level-lightweight-radars/
[35] “China-Pakistan Swarm Drone Raises New Challenge To India.” Indian Defence News, 14 July 2025, https://www.indiandefensenews.in/2025/07/china-pakistan-swarm-drone-raises-new.html#:~:text=According%20to%20Indian%20defence%20analysts,reach%20of%20about%203%2C500%20meters
[36] Trivedi, Saurabh. “Pakistan drones failed to do any damage during Operation Sindoor, says Gen. Anil Chauhan.”

Endnotes

The Hindu, 16 July 2025, , https://www.thehindu.com/news/national/self-reliance-in-uavs-counter-unmanned-aerial-systems-strategic-imperative-for-india-cds-chauhan/article69817607.ece
[37] Ali, Mushtaq; Shahzad, Asif. "Pakistani Islamist militants use drones to target security forces, officials say." Al-Monitor, 21 July 2025, https://www.al-monitor.com/originals/2025/07/pakistani-islamist-militants-use-drones-target-security-forces-officials-say
[38] Kaushal, Sidharth; Archer Macy; and Alexandra Stickings. The Future of NATO's Air and Missile Defence.RUSI Occasional Paper, July 2021. https://static.rusi.org/NATOMissileDefence2021.pdf
[39] Scharre, Paul. Autonomous Weapons and Stability. PhD diss., King's College London, 2020. https://kclpure.kcl.ac.uk/ws/portalfiles/portal/129451536/2020_Scharre_Paul_1575997_ethesis.pdf
[40] Bothra, Bindu; Apurba Rani Panda; Subhasis Pradhan; Md. Ashfaque Hussain; Dillip Dash. "Low RCS Target Detection: A Review." International Journal of Engineering Trends and Technology, vol. 45, no. 4, Mar. 2017, pp. 137–144 https://ijettjournal.org/2017/volume-45/number-4/IJETT-V45P231.pdf
[41] Tripathi, Prateek, and Kartik Bommakanti. "Air Defence Mechanisms: A Primer on India and Pakistan." Observer Research Foundation, 29 May 2025, https://www.orfonline.org/research/air-defence-mechanisms-a-primer-on-india-and-pakistan
[42] IADN Editorial Team. "QR SAM Development cum User Trials." IADNews, 2022, https://iadnews.in/qr-sam-development-cum-user-trials/
[43] PIB. "DRDO Successfully Conducts Maiden Flight-Tests of Integrated Air Defence Weapon System." Press Information Bureau, 24 Aug. 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2160257
[44] "No More Long Delays: Defence Secretary Says India Plans to Reduce Weapon Buying Timeline from 6 to Only 2 Years." The Economic Times, 21 June 2025, https://m.economictimes.com/news/defence/no-more-long-delays-defence-secretary-says-india-plans-to-reduce-weapon-buying-timeline-from-6-to-only-2-years/articleshow/121993271.cms
[45] Axe, David. "The German-made Gepard gun vehicle is one of Ukraine's best defenses against swarms of Russian Shahed drones." League of Ukrainian Canadians , 24 July 2025, https://www.lucorg.com/the-german-made-gepard-gun-vehicle-is-one-of-ukraines-best-defenses-against-swarms-of-russian-shahed-drones/
[46] " Iron Sting Weapon System, Israel." Army Technology, 22 May 2024, https://www.army-technology.com/projects/iron-sting-weapon-system-israel/#:~:text=View%20all,effectiveness%20on%20a%20dynamic%20battlefield.
[47] "Indian Army Bolsters Air Defence with Procurement of 10 Low-Level Lightweight Radars." IDRW, 13 July 2025, https://idrw.org/indian-army-bolsters-air-defence-with-procurement-of-10-low-level-lightweight-radars/
[48] Haider, Usman. "India's Evolving Air Defence Capabilities and Options for Pakistan." Journal of Security & Strategic Analyses, vol. 11, no. 1, July 2025, pp. 88-109. https://www.researchgate.net/publication/393296093_India's_Evolving_Air_Defence_Capabilities_and_Options_for_Pakistan/download
[49] "Ukraine Conflict Shows High Interception Rate for Russian Subsonic Missiles: Implications for India's Cruise Missile Strategy." IDRW, 20 July 2025, https://idrw.org/ukraine-conflict-shows-high-interception-rate-for-russian-subsonic-missiles-implications-for-indias-cruise-missile-strategy/
[50] Deshpande, Smruti. "How IAF, Army Are Moving Towards Jointness With Integration of Air Defence Systems." The Print, 15 Jan. 2025, https://theprint.in/defence/how-iaf-army-are-moving-towards-jointness-with-integration-of-air-defence-systems/2445411/
[51] "M-SAM (Cheolmae II / 'Iron Hawk') — Medium-Range Surface-to-Air Missile." Global Security, 12 Apr. 2023, https://www.globalsecurity.org/military/world/rok/m-sam.htm

CSDR

COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

C-21, 3rd Floor, Qutub Institutional Area, New Delhi, India - 110016.
Phone: 011-43104566 | Email: office@csdronline.com | Web: www.csdronline.com | Twitter:@CSDR_India