United States' Air Defence in West Asia: Operational Shortcomings

Air Vice Marshal Prashant Mohan, VM (Retd)[@]

Abstract

Since the commencement of Operation Epic Fury, the combined air power of the United States (US) and Israel has attacked every possible target in Iran. On 30 Mar 2026, US President Donald J Trump announced that this coalition had struck 13,000 targets with roughly 3,000 potential targets remaining—numbers that were higher than strategic predictions that claimed the combined coalition sorties were likely to shortly exceed 10,000 by 31 Mar 2026.[1] Amidst these coalition air-attacks, Iran's response to the US-Israeli air strikes has largely been relatively measured during Mar 2026. Of late, Iran is conserving assets by being selective in its attacks. Focused on sustaining pressure on the Gulf states, Iran has opted for a strategy that can best be described as a 'Deliberate Approach'.[2] These attacks basically ride on two components: their missiles—both long and short range—and swarms of drones. While the US and Israeli air defence infrastructures are doing their best to stop these intrusions, the shield is often partially and periodically pierced. The article will try and tackle this puzzle: how and why are some Iranian missiles and drones penetrating the US-Israel coalition air defence infrastructure and what can India learn from this kinetic engagement.

[@]**Air Vice Marshal Prashant Mohan, VM (Retd)** is a fighter pilot who superannuated from the Indian Air Force on 31 Mar 2025. A qualified Flying Instructor, he has commanded a frontline fighter squadron and two front line fighter bases. The officer has also served as India's Defence and Air Attaché to the United Kingdom.

Journal of the United Service Institution of India, Vol. CLVI, No. 644, April-June 2026.

Introduction

The Iranian missiles and drones got through the United States (US)-Israel coalition Air Defence (AD) infrastructure and the reasons are many. However, one of the major factors was Iranian planning. The impact that the Iranian planning and execution had on its engagement with the US-Israeli forces needs to be studied. The major reasons for the unique resilience that have become characteristic of this Iranian response—and which can act as lessons learned for the Indian armed force apparatus—are listed below.

Calculated Escalation. Iran knows it cannot win this war outright, so it has studied and found the real soft under belly of the Gulf Cooperation Council (GCC) nations. One can say that Iran has rightly assessed the centres of gravity in this confrontation and is escalating the stakes by widening the scope of its attacks in a calculated manner. There is no doubt that Iran's inventory is fast depleting, but it has chosen to operationalise the principle of 'The longer the disruption, the more it will be hurt', not just for the US and Israel but also globally. This, in turn, will make it harder for the US–Israel coalition to continuously justify the cost of the war.

Unhurried Planning. As a result, the physical spread of Iranian strikes across the Gulf reveals a thoughtful adaptation to their opposition's defence architecture rather than arbitrary tit-for-tat targeting. For example, the United Arab Emirates (UAE) has absorbed roughly 55-60 per cent of all recorded strikes in the region. By targeting the UAE at this scale, Iran is indicating that it is strategically targeting the most visibly commercial and logistical backbone of the Gulf, specifically aiming to undermine investment in the region, disrupt its trade flows, and fracture confidence in their tourism industry. Iran is not firing missiles and drones with the same frequency and intensity everywhere across the region. Its attacks on the UAE and Saudi Arabia are heavily drone-centric, those on Qatar and Kuwait are even mix of drones and missiles, and those in Bahrain, while also drone-heavy, have a far lower volume relatively. This differentiation implies that Iranian planners are tailoring strike packages by geography—using salvos of cheap, hard-to-track drones against high-value but dispersed commercial-military nodes (the UAE, Eastern Saudi Arabia), and reserving faster, more destructive missiles for selected hardened targets.[3]

Layered but Persistent Pressure. Iran has relied heavily on a tag-team offensive beginning with mass loitering munitions (colloquially called *Kamikaze* [suicide] drones), followed first by short range and then by medium range ballistic missiles, and eventually by a limited number of cruise missiles. Intelligently designed, target-specific, mixed packages of these weapons are used to create layered but persistent pressure on the US–Israel coalition forces. On the other hand, the same objective is achieved in the Gulf region through short-range missiles and drones targeted towards the GCC nations. This is so because the distances of these targets from Iran are comparatively shorter, and ensuring that projectiles arrive at their targeted locations within minutes reduces reaction time for the opposition. To complicate things further, the weapon delivery system is designed to fire from multiple directions, simultaneously. This increases the likelihood of, at least a small fraction of, deployed weapons penetrating the target's defences, even when the overall interception rates are high.[4] In fact, an argument can be made that Iran's core advantage is the extremely low cost of the Shahed drones, and it is predicted that Tehran can sustain low-rate strikes for weeks or months by mass producing via domestic lines and with Russian support.[5]

Campaign Resilience. Iran's drone and missile campaign is showing signs of reduced intensity, but the resilience of the campaign is both surprising and remarkable. For Iran, this is not like any other conflict; it is an existential fight. "This is an all-out war", said Fawaz Gerges of the London School of Economics, adding, "They believe their very survival is at stake. They're willing to bring the temple down on everyone's heads". This sentiment was also echoed by Alex Vatanka, a senior fellow at the Middle East Institute and an expert on Iranian politics, who added, "They're like a bleeding animal—wounded, therefore, more dangerous than ever".[6]

Targeting the 'Eyes and Communication'. Another aspect of Iran's strategic plan has been the deliberate damage it has inflicted on the US missile defence and Command and Control (C2) network. A *New York Times* analysis of satellite imagery found significant damage to facilities associated with communication and radar systems in at least seven US used sites.[7] *Cable News Network*, too, using commercial satellite imagery, reported that the radar system for a US Terminal High Altitude Area Defense

(THAAD) battery at Muwaffaq Salti Air Base in Jordan was struck.[8] At the Al-Ruwais Air Base in the UAE, Iran struck a shelter near the Army/Navy Transportable Radar Surveillance-2 (AN/TPY-2) radar and targeted vehicles carrying the THAAD system. Similarly, in Saudi Arabia, Iran hit the Prince Sultan Air Base, which also houses the AN/TPY-2 radar and vehicles from the THAAD system. Furthermore, Iran's Islamic Revolutionary Guard Corps publicly claims to have destroyed the Army-Navy Fixed Radar, Search 132 early warning radar at Al Udeid Air Base in Qatar.[9] Most recently, there has been an alleged strike on the E-3 Sentry airborne warning and control system parked at the Prince Sultan Air Base in Saudi Arabia. These Iranian strikes on antennas, radomes, and associated facilities show tactical pre-meditation and seem aimed at disrupting long-distance communication and command networks, which impairs their opposition's missile and drone detection infrastructure.

Targeting the Vulnerabilities. The bedrock of this deliberate disruption strategy is to focus on tactical vulnerabilities in the opposition's military infrastructure. In this case, Iran has focused on the region's AD which is 'Very capable but finite and, thus, not leak-proof across its vast geography'.[10] The defence grid is more optimised for high-altitude ballistic missiles than low-altitude drones and cruise missiles, and that is precisely the weakness that Iran sought to exploit. Moreover, this AD structure is built around point-defence systems. These points are strategically selected and arranged to protect specific high-value targets. They do not provide a continuous, impenetrable wall. Iranians have also capitalised on these gaps in their AD network as a second point of vulnerability that allows for a targeted attack.

Mixed Strike Packages. This mixed strike packages approach, where a combination of drones, cruise missiles, and ballistic missiles arrive in waves from different directions at different altitudes, also aims to saturate the radar and fire control capacity of the intended target. The contrast between Iran's approach, which relies heavily on asymmetric warfare, and that of the conventionally oriented US–Israel coalition is quite stark. As Kelly Grieco, a senior fellow with the 'Reimagining US Grand Strategy' programme at the Stimson Centre, remarked, "……. The US and Israel are excelling where you would expect them to excel—in the airspace, higher altitudes, fighting the more traditional fight …….".[11] However,

it seems that the coalition has not trained for a scenario where such a confrontation takes place with Iran.

Vulnerabilities of the United States' Air Defence Umbrella in West Asia

Having understood the Iranian strategy as a 'Deliberate Approach'[12], the question now raises about whether the US-provided AD system is invincible against an attack of such kind. There is no argument that the system itself is quite capable, but what seems evident is that it is not impervious to systematic, sustained pressure. The vulnerabilities listed in the succeeding paragraphs show why and how this AD system could be susceptible to prolonged attrition.

Exposed High Value Radar Sites. Iran, having studied the infallibility of this system, created a plan of attack accordingly; for example, it has systematically targeted static sensors in the US missile defence architecture. These static sensors were left exposed since they did not have terminal defences defending them. One plausible explanation for this gap in planning is that the American tacticians did not entertain the possibility of Iranian attacks to take this form.

Short warning Threats. Iran has exploited the geography of the region; for instance, given the proximity of the Gulf states, it chose to attack them with short range ballistic missiles that have a significantly short-flight time. As a result, the reaction window for the defending GCC countries was substantially reduced despite early warning radar functionality. When these ballistic missiles are combined with slower, low flying drone swarms, defenders have to simultaneously manage a mass and a mix of targets. This stretches the C2 structure and increases the risk of system penetration.

Vulnerable Critical Infrastructure. Furthermore, Iran has deliberately struck critical economic and civilian infrastructure like the Bahraini desalination plant[13], Aramco's Ras Tanura refinery in Saudi Arabia, facilities in the Shaybah oil field, Kuwait International Airport, and multiple other high value sites in the UAE, Kuwait, and Bahrain. These targets are typically relatively more difficult to harden, and as expected, the US supplied systems provided comprehensive defence only for select bases and cities. The broader web of energy, water, and transport infrastructure—the

true centres of gravity for Gulf states—remained only partially covered by point defences, giving Iran many soft but tactically impactful targets which they strategically exploited.

Gaps Against Swarms and Multi-directional Low End Drones. Moreover, the AD system in the region is optimised for high altitude ballistic and cruise threats and remains largely unprepared for attacks by saturating swarms of small, low flying drones. Current dedicated counter Unmanned Aircraft System (UAS) layers, within this defence infrastructure, are comparatively thin. Iran has exploited these gaps, especially over wide rear areas and at low altitude contexts.

System of Systems Fragility. AD effectiveness depends on a comprehensive system of enablers like sensors, communication links, C2 nodes, and interceptor batteries. Without redundancy, if even one critical layer is compromised, performance of the whole architecture can rapidly degrade. The Iranian strikes show that by focusing their attacks on enabling nodes within the US AD apparatus, it can achieve disproportionate operational and strategic effect against a very expensive, relatively technologically advanced but structurally brittle US designed defence network.[14]

Interoperability and Political Friction. There is also an element of political friction in the region, hiccupping attempts at a coordinated defence strategy on part of the Gulf states. Even technologically advanced systems such as Patriot and THAAD cannot fully compensate for limited data-sharing or slow-to-integrate GCC-level Integrated Air and Missile Defence (IAMD). Distrust among regional partners over intelligence-sharing, C2 authority, and integration with Israeli systems has historically kept the architecture 'Sub-optimal', meaning that localised gaps remain in the AD apparatus, and these gaps can be further exploited by an adversary like Iran.[15]

Lack of Layered Defence. The central lesson from this 2025-26 US–Israel–Iran conflict in West Asia is that one cannot rely on a single silver-bullet platform (for example, Patriot or THAAD or Iron Dome). Operational evidence clearly indicates that only a layered, multi-system architecture—stacked across different altitude bands and tailored to different threats—can credibly mitigate the combined challenge of ballistic and cruise missiles, and that of loitering munitions. The US-provided AD certainly lacks this.

Overconfidence. Another plausible source of vulnerability for the US AD system could be a certain degree of overconfidence on part of the US strategists, who presumably had ample warning about Iran's missile–drone concept and the cost asymmetry therein. Yet, the US defence architecture was not updated fast enough to keep abreast of intelligence received, nor was it adapted comprehensively enough to integrate lessons learnt from the Ukraine conflict. In fact, Israel's AD architecture centres on a highly integrated multi-layered system (Iron Dome for short-range, David's Sling for medium, Arrow for ballistic), optimised for dense, close-range, and long-range threats. However, the US seemingly did not inculcate these lessons from its coalition partner, Israel. It is hard to see this as anything other than overconfidence. This is especially the case if it is considered that long before this conflict started, think tanks and media analyses warned that the Gulf AD architecture was structurally unsustainable against an attack like a swarm of cheap Iranian missiles and drones.[16]

Lessons for India

With two quite active borders, India has to prepare for the worst-case scenario, i.e., both borders becoming active simultaneously. A wide assortment of projectiles can be directed towards India from both of these borders, and they are likely to be rather potent. Therefore, it is imperative for India to further develop its AD capabilities. Suggestions for the same are listed below:

- **Plan for Saturation, Coverage, and Depth, in other words, 'Multi-tiered'**. The US experience demonstrates that even when interception percentages are high, a determined adversary can still get enough projectiles penetrated with a layered persistent attack. India must assume that attacks from Pakistan or China or both will be a mix of assorted systems operating, simultaneously, in most likelihood. For India, this would mean to have an Indian AD system that is networked, integrated, redundant, and multi-layered, so that it can sustain saturation. The priority should be depth of fire coverage across all levels. And, globally, the demand for 'Mosaic Defence' is definite to increase. However, it is critical that this defence structure is not simply aped. Rather, it should be studied thoroughly, discussed adequately, and debated at length before it is executed.

- **Strengthen Unity of C2 for AD**. In Operation Epic Fury, there was at least one well-documented case of fratricide (blue-on-blue) in the AD domain. On 02 Mar 2026, three US Air Force F-15E Strike Eagles were shot down over Kuwait by Kuwaiti AD Short-Range AD (SHORAD) systems. The aircraft were not intercepted by Iranian missiles. The IAMD in Operation Epic Fury aggregated US Patriot Advanced Capability-3, THAAD, Israeli Arrow, David's Sling, Iron Dome, and SHORAD systems in Kuwait, Saudi Arabia, and the UAE. It was dense AD architecture but under different national command authorities, following different Rules of Engagement (ROEs), linked to US Central Command only via partial, sometimes intermittent datalinks. It was not a single unified C2 node. The available open-source analysis points to the following AD set-up[17]: it had fragmented C2, it lacked a unified, real-time, shared operational picture, it was a system-of-systems mismatch—different vendors, ROEs, training cultures, and incomplete deconfliction in the same airspace and with insufficient redundancy in oversight. This fratricide in question is consistent with a decentralised-execution model of C2, operating under conditions of saturation, cognitive overload, and brittle Identification Friend or Foe (IFF) and deconfliction, rather than a clean, tightly centralised C2 architecture.[18]

- **Centralised Command and Control in Integrated Air Defence**. In case of centralised C2, data from satellites, ground, maritime, and air-based sensors, and radars, with the help of advanced IT systems, is fused at a central node. This fused picture is then distributed in real time to various AD weapon systems. The advantages of a centralised C2 are improved overall situational awareness, prevent fratricides, systematic deconfliction, enforcement of strict IFF rules or ROEs, assignment of weapons to enemy tracks, coordinate overlapped AD zones so that multiple batteries do not engage the same track and having a single, auditable decision-making node. A central authority can prioritise which assets to protect (e.g., C2 nodes, bases, logistics hubs), allocate limited missile inventories, and sequence engagements across a layered integrated AD system (long-, medium-, shortrange). This is especially useful in saturation-threat scenarios where 'Shot-management' is crucial.19 The AD during Operation Sindoor was centralised C2, and it was effective and successful.

Harden and Duplicate C2. An argument can be made that Iranian hits on US static radars and C2 facilities were history repeating itself. As such, there should be no compromise in undergrounding, hardening, and duplicating India's C2 facilities. These facilities need to be sufficiently dispersed with automatic switch-over from a primary system to a backup when the primary is compromised. Airborne C2, satellite communication-based mobile and relocatable C2, and extensive use of decoys should undoubtedly be the order of the day.

Scalable Counter-UAS Tier. Evidence has shown that traditional ground-based AD is structurally ill-suited to defeat drone swarms. The 'Last 05-10 kms' layer has to be both dense and cost-efficient.[20] One way to achieve this objective is to ensure that Quick Reaction Surface-To-Air Missile (QRSAM) and Akash should be complemented by mass-produced low-cost anti-drone solutions like radar-cued guns, proximity-fused shells, Man-Portable Air-Defence Systems (MANPADS), directed-energy weapons, and radio frequency or electro-optical-based soft-kill systems, all integrated via Integrated Air C2 System (IACCS).

Rear-Area Sanctuaries. India has geographic depth. The long-range drones or loitering munitions and ballistic missiles now have ranges that will threaten 'Rear-area Sanctuaries' in, say, Uttar Pradesh, Tamil Nadu, Vizag, Bengaluru, Bombay harbour or docks, Bombay high, refineries, etc. Investments must go in for their protection by a layered AD. Critical national asset, even in depth, should have layered point defence. These point defences have to be networked with the larger integrated national AD.

Rethinking through Basing of Enablers. The damage to (parked in the open) US tankers and an airborne warning and control system at the Prince Sultan Air Base explicitly demonstrates that even if the base is in the rear, just one successful strike can be tactically catastrophic. Moreover, fuel farms, munitions depots, and critical national assets have been shown to be vulnerable to first-person view drones and missile strikes during this conflict. Therefore, India needs to rework dispersing combat assets, hardening shelters, and support infrastructure.

Public–Private Model of Domestic Designing and Production Capacity. The two ongoing wars have shown that during active combat, interceptor and drone consumption can rapidly outstrip

peacetime production. Both Russia and the US scrambled and are still scrambling, respectively, to ensure a steady supply of interceptors and drones, among other things.[21] In the case of Russia, it had to rapidly adapt to designing and producing drones and anti-drone systems. This is an important lesson for India as well. India, in any contingency, either with China or Pakistan, or both, cannot assume an uninterrupted supply of military hardware and software. It relies on its own capabilities and pushes for a much larger public–private model of domestic designing and reinforced production capacity with an ability to generate a surge output, if needed.

Maven Equivalent Artificial Intelligence (AI) AD Tool. Palantir has provided Maven Smart System, an AI tool, to the US Armed Forces.[22] Maven Smart System is a battlefield C2 and weapons targeting AI platform built especially for the Pentagon. It fuses torrents of data from satellites, drones, radars, sensors, and intelligence reports, subsequently using AI to automatically flag potential targets, giving commanders an AI-assisted real time battlefield picture. It has typically been used for broader operational decision making. India could similarly consider AI tool(s) for its integrated AD architecture.

Training. The character of war has become dependent on evolving technology. But it is important to remember here that the destructive nature of technology is limited to its user's maleficent traits. Notwithstanding those traits, in the present day scenario—where AD operators face drones, cruise missiles, hypersonics, and heavy electronic warfare—the training should reflect this complexity by being intrinsically multi layered: joint, adaptive, cognitive, and interoperable across domains.

Doctrines. As the character of war evolves, air-defence doctrines must shift from asset-centric to network-centric, adaptive, joint frameworks.[23] Air-defence doctrine should explicitly embed space, cyber, electronic warfare, and AI-enabled sensing rather than treating them as 'Support'. Modern AD doctrine must define how human operators supervise, override, and audit machine-driven decisions.[24] It must combine centralised-intent and execution, especially under high-tempo, degraded C2, or escalation-management.

Conclusion

The biggest learning for India, then, is that the US, in spite of having air superiority and state-of-the-art technology, has been held at ransom against saturation strikes by massed cheap drones. This central lesson should be taken seriously for Mission Sudarshan Chakra, India's ambitious multi-layered air and missile defence initiative, which aims to create an indigenous, AI-enabled shield protecting Indian airspace from asymmetric threats like cheap drone swarms. Priority has to be given to the integration of sensors, shooters, and C2 (like IACCS/Akashteer) over standalone high-end platforms, while addressing cost asymmetry through scalable low-end layers (guns, MANPADS, QRSAM). Balancing high-end (air dominance) with low-cost scalability will indubitably prevent India from repeating the US's errors in its conflict with Iran against threats posed by Pakistan or China.[25]

Endnotes

[1] Parker Hempel, Adham Fattah, Ria Reddy, Katherine Wells, and Annika Ganzeveld, "Iran Update Evening Special Report", *Critical Threats and the ISW*, 30 Mar 2026, accessed 22 May 2026, https://www.criticalthreats.org/analysis/iran-update-evening-special-report-march-30-2026

[2] Mark F Cancian and Chris H Park, "Assessing the Air Campaign After Three Weeks: Iran War by the Numbers", *Center for Strategic and International Studies*, 25 Mar 2026, accessed 22 May 2026, https://www.csis.org/analysis/assessing-air-campaign-after-three-weeks-iran-war-numbers

[3] Kateryna Bondar, "Unpacking Iran's Drone Campaign in the Gulf: Early Lessons for Future Drone Warfare", *Center for Strategic and International Studies*, 10 Mar 2026, accessed 22 May 2026, https://www.csis.org/analysis/unpacking-irans-drone-campaign-gulf-early-lessons-future-drone-warfare; and Can Kasapoglu, "Operation Epic Fury Situation Report I Battlefield Effects and Early Strategic Signals", *Hudson Institute*, 10 Mar 2026, accessed 22 May 2026, https://www.hudson.org/missile-defense/operation-epic-fury-situation-report-battlefield-effects-strategic-outcomes-can-kasapoglu

[4] Jonathan Ruhe and Ari Cicurel, "Iran's Evolving Missile and Drone Threat", *JINSA's Gemunder Center for Defense and Strategy*, Feb 2026, accessed 22 May 2026, https://jinsa.org/jinsa_report/irans-evolving-missile-and-drone-threat/

[5] Nicholas Kulish, “In Iran War, Cheap Drones Remain Wild Card”, *The New York Times,* 25 Mar 2026, accessed 22 May 2026, https://www.nytimes.com/2026/03/25/world/middleeast/iran-war-cheap-drones.html

[6] “‘Wounded but more dangerous than ever’: Iran bets on endurance, energy disruption to outlast enemies”, *The Straits Times*, 10 Mar 2026, accessed 22 May 2026, https://www.straitstimes.com/world/middle-east/iran-bets-on-endurance-energy-disruption-to-outlast-us-israel

[7] Devon Lum, Haley Willis, and Riley Mellen, “Iran Strikes US Military Communication Infrastructure in Mideast”, *The New York Times,*03 Mar 2026, accessed 22 May 2026, https://www.nytimes.com/2026/03/03/world/middleeast/iran-strikes-us-military-communication-infrastructure-in-mideast.html

[8] Thomas Bordeaux and Gianluca Mezzofiore, “Radar bases housing key US missile interceptor hit in Jordan, Saudi Arabia, and UAE, satellite images show”, *CNN*, 06 Mar 2026, accessed 22 May 2026, https://edition.cnn.com/2026/03/05/middleeast/radar-bases-us-missile-defense-iran-war-intl-invs

[9] “Iran Claims Destruction of AN/FPS-132 Radar in Qatar Used for U.S. Missile Warning”, *Defense News Army*, 02 Mar 2026, accessed 22 May 2026, https://www.armyrecognition.com/news/army-news/2026/iran-claims-destruction-of-an-fps-132-radar-in-qatar-used-for-u-s-missile-warning

[10] Bradley Bowman, Andrew Gabel, and Mikhael Smits, “Iran attack highlights US missile defense vulnerability”, *Defence News,* 13 Jan 2020, accessed 22 May 2026, https://www.defensenews.com/opinion/commentary/2020/01/13/iran-attack-highlights-us-missile-defense-vulnerability/

[11] Kelly Grieco et al, “Untangling the Web of US Alliances”, *Stimson Centre*, 05 May 2026, accessed 22 May 2026, https://www.stimson.org/event/untangling-the-web-of-us-alliances/

[12] Michael Young, “Iran Rewrites Its War Strategy”, *Carnegie Middle East Center*, 30 Mar 2026, accessed 22 May 2026, https://carnegieendowment.org/middle-east/diwan/2026/03/iran-rewrites-its-war-strategy

[13] Shannon Renfore, “Bahrain desalination plant struck as water infrastructure becomes latest front in Iran war”, *Stars and Stripes*, 08 Mar 2026, accessed 22 May 2026, https://www.stripes.com/theaters/middle_east/2026-03-08/bahrain-desalination-plant-water-20995370.html

[14] Jennifer Kavanagh, "Iran wipes out US-Israeli radars & sensors, changing course of war", *Responsible Statecraft*, 30 Mar 2026, accessed 22 May 2026, https://responsiblestatecraft.org/iran-radars-airstrikes/

[15] Nafja Alkuwari, "GCC Air Defense Between Challenge and Transformation", *Middle East Council of Global Affairs*, 25 Mar 2026, accessed 22 May 2026, https://mecouncil.org/blog_posts/gcc-air-defense-between-challenge-and-transformation/

[16] Asiye Latife Yilmaz, "Cost asymmetry in Gulf air defense exposes long-term sustainability risks", *Anadolu Ajansi*, 04 Mar 2026, accessed 22 May 2026, https://www.aa.com.tr/en/middle-east/cost-asymmetry-in-gulf-air-defense-exposes-long-term-sustainability-risks/3847942

[17] "Blue-on-Blue Air Defence Coordination Challenges", Norsk Luftvern, 03 Mar 2026, accessed 22 May 2026, https://norskluftvern.com/2026/03/03/blue-on-blue-air-defence-coordination-challenges/

[18] Lieutenant Colonel Alan Docauer, "Peeling the Onion, Why Centralized Control / Decentralized Execution Works", *Air and Space Power Journal*, Mar–Apr 2014, accessed 22 May 2026, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28_Issue-2/ASPJ-Mar-Apr-2014.pdf

[19] Lieutenant Colonel Andreas Schmidt, "Possibilities and Limits of a C2 (R)Evolution", *Joint Air Power Competence Centre*, Feb 2022, accessed 22 May 2026, https://www.japcc.org/articles/possibilities-and-limits-of-a-c2-revolution/

[20] Vijainder K Thakur, "India's World-Beating Akash and Very Short-Range Air Defense Missiles Are Owner's Pride, Other's Envy", *The Eurasian Times,* 03 Apr 2026, accessed 22 May 2026, https://www.eurasiantimes.com/aws-vshorads-successes-make-drdo-a-world-leader/

[21] Julian McBride, "The 2026 Iran War Shows the Urgent Need for U.S. Enhanced Missile Defense Upgrades", *Atlas Institute for International Affairs,* 04 Mar 2026, accessed 22 May 2026, https://atlasinstitute.org/the-2026-iran-war-shows-the-urgent-need-for-u-s-enhanced-missile-defense-upgrades/

[22] David Jeans, "Exclusive: Pentagon to adopt Palantir AI as core US military system, memo says", *Reuters*, 20 Mar 2026, accessed 22 May 2026, https://www.reuters.com/technology/pentagon-adopt-palantir-ai-as-core-us-military-system-memo-says-2026-03-20/

[23] Lieutenant Colonel Kim Vogt, "Adapting Air and Missile Defence Training and Doctrine for Hypersonics and Drones", *Joint Air Power Competence Centre*, May 2025, accessed 22 May 2026, https://www.japcc.org/articles/adapting-air-and-missile-defence-training-and-doctrine-for-hypersonics-and-drones/

[24] Vishal Giare and Grogory A Miller, "Air and Missile Defence: Defining the Future", *Johns Hopkins APL Technical Digest*, Volume 35, Number 4, 2021, accessed 22 May 2025, https://secwww.jhuapl.edu/techdigest/content/techdigest/pdf/V35-N04/35-04-Giare.pdf

[25] Gaurav Pradhan, "Lessons for the Indian Military from the Iran War: A Strategic Perspective", *LinkedIn*, 07 Mar 2026, accessed 22 May 2026, https://www.linkedin.com/pulse/lessons-indian-military-from-iran-war-strategic-pradhan—rcdzc/