CENTRE FOR AEROSPACE POWER AND STRATEGIC STUDIES (CAPSS)

Forum for National Secuirty Studies (FNSS)

AEROSPACE NEWSLETTER

The Centre for Aerospace Power and Strategic Studies (CAPSS) organised the 9th Jasjit Singh Memorial Lecture on 28 July 2026 to honour its Founder Director General, Air Commodore Jasjit Singh AVSM, VrC, VM (Retd). The lecture was themed "Beyond Borders: Reimagining India's Strategic Neighbourhood in the 21st Century."

VOL VI NO 08 **05 August 2026**

Centre for Aerospace Power and Strategic Studies | @CAPSS_India

Centre for Aerospace Power and Strategic Studies | Centre for Aerospace Power and Strategic Studies

"The growing participation of our private sector is opening new frontiers and accelerating innovation."

- Prime Minister Shri Narendra Mod

Contents

Opinions and Analysis

Air Power

Space

Aerospace Industry

Opinions and Analysis

A Tale of Two Strategic Attacks: The Race to End the War in Ukraine

Benjamin Jensen and Yasir Atalan |

15 July 2026

Source: CSIS | https://www.csis.org/analysis/tale-two-strategic-attacks-race-end-war-ukraine

Photo: Ivan Antypenko/Suspilne Ukraine/JSC "UA:PBC"/Global Images Ukraine/Getty Images

The war in Ukraine is now a race between two competing, attritional theories of victory. Ukraine is focused on maximizing drone production alongside novel use of AI and low-cost, high payoff deep strikes integrated with cyber and electronic warfare designed to hold Russia's oil and gas, and by proxy its economy, at risk. Russia is trying to increase its punishment campaign, targeting critical infrastructure and major political and economic centers like Kyiv to force a negotiation that favors the Kremlin's interests. While the battlefield still matters, these dueling deep strike campaigns are the lines of effort most likely to force a settlement over the next six months.

Ukraine's Energy Blitz

Ukraine is executing strategic attacks against Russian energy infrastructure designed to impose economic costs and fracture elite support for the Kremlin. The campaign targets the financial engine of the state by striking refineries, export terminals, and storage facilities well beyond the front line. This operational design bypasses the stalemate on the ground to threaten the revenue streams funding the war effort. As oil profits decline and domestic fuel shortages rise, the strikes compel Russian power brokers to absorb the physical consequences of the conflict. By holding these critical economic nodes at risk, Kyiv seeks to alter the decision calculus of regime insiders and create political friction within the capital.

Ukraine's launches of air and drone strikes in Russia have increased significantly over the war, according to data from ACLED. In 2023, there were around 580 strikes or strike events; this number increased to 7,244 in 2024. Of these events, 901 aimed at energy infrastructure, such as fuel storage, oil depots, refineries, and pipelines. The data ends in June 2025, but in the first half of 2025 alone, there were 6,176 air and drone strikes, suggesting that the total number of attacks in 2025 may have nearly doubled the 2024 total. Russia suffers from these attacks due to its dependence on oil and gas: Just before the full-scale invasion, taxes and export tariffs related to oil and gas comprised 45 percent of Russia's

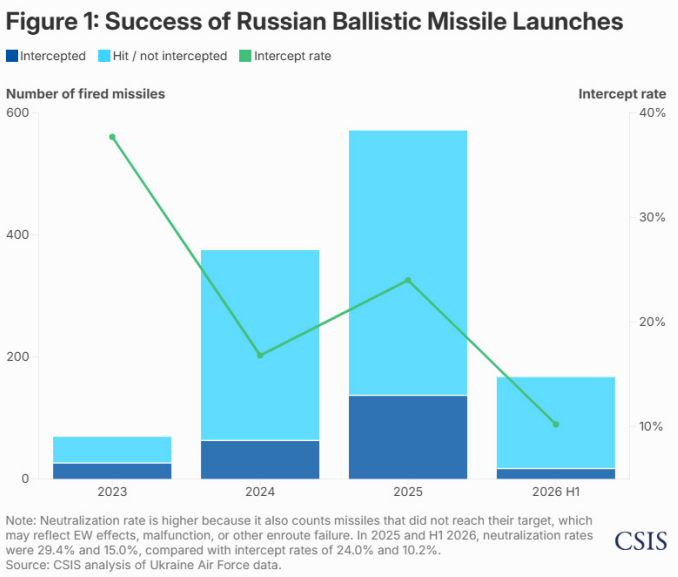
federal budget revenues.

Ukraine has also extended its campaign from fixed infrastructure to maritime energy logistics. Aerial and Sea Baby drones have been actively used against tankers in Russia's shadow fleet. Ukraine drone strikes also recently attacked 90 Russian vessels, which led to the suspension of shipping in the Sea of Azov.

Russia's Punishment Campaign

Russia's firepower strike strategy operates as a deliberate punishment campaign designed to substitute for stagnant ground offensives by breaking the political resolve of both Kyiv and its international backers. By launching large salvos of ballistic missiles and drones against critical infrastructure, Russia seeks to exhaust Ukrainian air defenses and inflict paralyzing psychological strain on the civilian populace. This pressure creates a cruel mathematical reality where sheer munitions volume overcomes interception capabilities to directly shape the strategic environment. The Kremlin calibrates these bombardments to attempt to force Ukrainian leadership into premature concessions and secure a negotiated settlement that cements Russian interests regardless of localized battlefield realities.

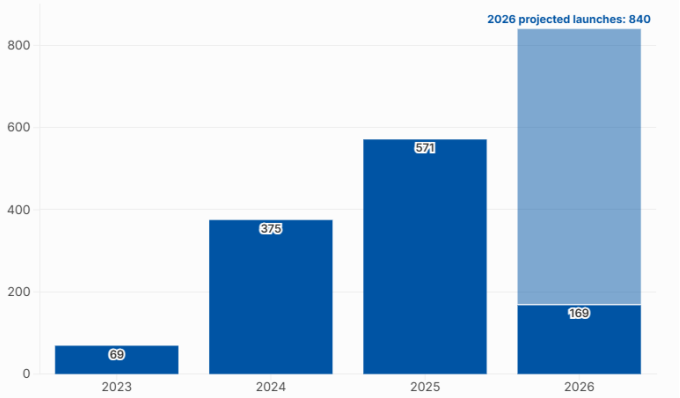
While Ukraine has proved agile in fielding new classes of long-range strike drones and cruise missiles, the key variable to watch in these dueling strike campaigns is ballistic missiles. As documented in the CSIS Russian Firepower Strike Tracker, Ukraine has successfully intercepted drones and cruise missiles since the start of the war: Ukraine often intercepts long-range one-way attack drones like the Shahed over 85 percent of the time. However, ballistic missiles are another story. Between 2023 and 2025, Russia increased the number of ballistic missiles it fired at Ukraine, and by extension its production capacity, by over 700 percent. However, the share of ballistic missiles Ukraine was able to intercept and neutralize dropped by 36 percent. Worse still, the current interception rate in 2026 is only 10.2 percent, a drop of over 200 percent from the beginning of the war. This coercion drives increasing pressure on the Ukrainian president and his supporters to find an off-ramp to the war despite recent battlefield gains.



The trend of decreasing success of intercepting ballistic missiles appears to be getting worse in 2026. To date, since January 1, 2026, Russia has fired 167

ballistic missiles at Ukraine. Yet, the past trend shows that Russia generally ramps up its ballistic launches toward the end of the year. If this trend holds, Moscow is on track to fire up to 840 ballistic missiles in 2026 (Figure 2).

Figure 2: Ballistic Missile Launches by Year



Note: 2026 shows actual launches to date plus a shaded projection based on the 2023–2025 linear trend.
Source: CSIS analysis of Ukraine Air Force data.

CSIS

For Ukraine to successfully defend against Russian attacks, it must increase the rate at which air defenses intercept ballistic missiles. If only 10.2 percent of 840 ballistic missiles are intercepted, that leaves 754 devastating strikes that could alter the balance of resolve. Kyiv needs to limit the number of ballistic missile strikes that reach their target and buy time for its attacks on Russian energy infrastructure to change the decision calculus in Moscow.

How Ukraine's International Backers Can Help

Ukraine's international partners can address the increased use of Russian ballistic missile strikes to support the Ukrainian deep strike campaign along three lines of effort: revisiting sanctions evasion, increasing intelligence support, and accelerating coproduction.

Revisit Sanctions Evasion: Since the start of the war, Russia has found ways to bypass sanctions and acquire important electronic components that support its long-range strike campaign. Recent reporting documents how Russia uses a special military intelligence unit, the 20th Directorate, to buy foreign electronics and evade sanctions.

To choke off the supply of foreign electronics feeding the Russian war machine, the United States and its allies must aggressively target the global networks orchestrating parallel trade. Russian military intelligence units like the 20th Directorate continually exploit gaps in customs enforcement, lax jurisdictions and shell companies to procure critical dual-use components. Washington should combat this illicit pipeline by rapidly declassifying and passing actionable intelligence on these front operations directly to partner enforcement agencies. Armed with this precise targeting data, the Treasury Department can then expand secondary sanctions against the specific third-country intermediaries and foreign financial institutions facilitating these covert supply chains. Synchronizing active intelligence sharing with expanded economic coercion will fracture the procurement hubs enabling Moscow and steadily degrade the sustainment capacity of the Russian defense industrial base.

Increase Intelligence Support: International partners can blunt the lethal math of the Russian salvo campaign

by expanding intelligence sharing to support Ukrainian deep strikes. Western agencies should provide actionable targeting packages that support attacking the ballistic missile threat at its source. High-priority target sets include mobile Iskander launchers, manufacturing plants deep inside Russian territory, and critical supply chain vulnerabilities like rocket motor production facilities. Disrupting these nodes before missiles enter the logistical pipeline reduces the immediate burden on Ukraine's strained air defense network. Shifting a portion of Kyiv's long-range strike capacity toward active ballistic missile launch platforms and component bottlenecks creates operational friction, forces Moscow to pull assets further back, and slows the overall generation of Russian firepower.

Accelerate Coproduction: In 2024, Germany, Spain, Romania, and the Netherlands signed an almost $6 billion contract to manufacture Patriot interceptors (PAC-2) at a new facility run by defense company MBDA in southern Germany. During the July NATO summit, Under Secretary of Defense Michael Duffey signaled a willingness to explore additional coproduction in Europe outside of Germany. These efforts are in addition to calls to license Patriot production in Ukraine, an effort which, while crucial, could take years to materialize.

Therefore, European states should tap European Investment Bank Group funding for additional production lines, both at the MBDA plant and in other areas. Accelerating PAC-2 production would allow European states to transfer additional Patriot interceptors to Ukraine without incurring significant long-term risk.

***

Analysis: How Ukraine is Reimagining Strategic Attack

Lt. Gen. David A. Deptula, USAF (Ret.) | 10 July 2026

Source: Air and Space Forces | https://www.airandspaceforces.com/analysis-how-ukraine-is-reimagining-strategic-attack/

Ukraine's FP-1 drone in May 2025. Photo by oboronka.mezha.ua

Since Russia's 2022 invasion, outside observers have measured Ukraine's prospects by a familiar yardstick: miles of territory gained or lost on the ground. By that standard, the war often appears static, attritional, and brutally expensive. But Ukraine is now demonstrating an alternative—and more effective—means to fight, taking the war deep into Russian territory not simply to punish Moscow, but to disrupt the systems that enable its military to continue fighting.

This is not a new idea. It is one of the oldest tenets of airpower: Attack the sources of an enemy's military power directly, paralyze the systems on which the enemy depends, and impose costs that change the adversary's strategic calculus. What is new is the means. Ukraine is executing strategic attacks with improvised, long-range, one-way uncrewed aircraft—more accurately described as low-cost cruise missiles. It is also employing special operations, maritime strike systems, cyber-enabled intelligence, and adaptive targeting.

One recent analysis suggests Kyiv pursue strategic neutralization: to shift away from measuring success solely by territorial movement on the ground and toward a broader objective of making Russia's aggression operationally futile. The concept is not simply to attrit Russian forces at the front, but to persistently disrupt the systems that allow Moscow to regenerate combat power, export energy, produce weapons, launch missiles, and sustain the political fiction that the war can remain distant from Russian society.

Ukraine's attacks on oil refineries, export terminals, military factories, command-and-logistics nodes, air defenses, airfields, semiconductor facilities, and cruise missile production centers are precisely the kinds of targets that make sense when the objective is not battlefield attrition alone, but systemic disruption.

That logic reaches back to the early Airmen of the 1920s and 1930s. Giulio Douhet, Billy Mitchell, Hugh Trenchard, and the Air Corps Tactical School all argued in different ways that modern states had become vulnerable because they depended on interlocking industrial, transportation, energy, and command systems. The Air Corps Tactical School's industrial web concept held that a nation's war-making potential could be attacked through critical nodes in manufacturing, power, transportation, fuel, and other essential sectors. In my 2001 monograph on how the Desert Storm air campaign was designed and executed, this point is highlighted explicitly: the Air Corps Tactical School favored the destruction or paralysis of national organic systems such as electric power, transportation, railroads, fuel, food distribution, steel manufacturing, and related industries vital to a state's war-making capacity.

The theory was first attempted on a large scale in World War II, but technology was not yet sufficient to fully exploit its potential. Strategic airpower could reach deep into enemy territory, but it could not reliably hit precise aimpoints without enormous mass. Even after Allied forces gained air superiority over Germany in 1944, precision bombing often required hundreds of aircraft to destroy a single target because only about 20 percent of bombs aimed at precision targets landed within 1,000 feet of the aimpoint. The strategic insight was real; the execution was

only rudimentary.

That changed in 1991. The Desert Storm air campaign attacked Iraqi leadership, command-and-control, air defenses, electricity, transportation, oil, weapons production, and fielded forces in parallel to produce cascading effects. Much of Desert Storm's success is rightly attributed to stealth and precision, but what made the operation so successful was its effects-based approach to planning and execution. Starting with the desired strategic and operational outcomes, planners worked backward to identify the key systems and critical nodes whose disruption would produce those desired effects—paralyzing decision-making, blinding air defenses, isolating fielded forces, degrading mobility and logistics, and collapsing Iraq's ability to conduct coherent military operations. The objective was to orchestrate integrated attacks that would impose rapid, system-wide paralysis with speed, precision, and economy of force. It worked. The 43-day air campaign rapidly degraded Iraq's fighting capacity, paving the way for the removal of Iraqi forces from Kuwait once land forces were employed.

Operation Allied Force in 1999 reinforced these lessons under different conditions. Though politically constrained and not a pure example of parallel warfare, the defense of Kosovo from Serbian aggression demonstrated how precision attacks against selected systems could achieve coercive effects. NATO's own history describes Allied Force as an air campaign launched after diplomacy failed; RAND's assessment, NATO's Air War for Kosovo, characterized it as a 78-day air war designed to compel Slobodan Milosevic to end ethnic cleansing in Kosovo. Allied Force combined global attack, parallel precision engagements and elements of an effects-based approach to achieve those objectives.

Ukraine now finds itself under far harsher constraints. It lacks the air superiority achieved by the coalition in Desert Storm and by NATO in Allied Force. It cannot send large packages of manned aircraft deep into Russian airspace. It lacks the mass of a superpower air force. Yet it has recognized the same enduring truth: modern war depends on systems, and systems contain vulnerable nodes.

That is why Russian oil infrastructure matters. Oil is Russia's economic engine, vital for revenue and political power, as well as for fuel, transportation capacity, industrial output. Ukrainian long-range cruise missile strikes against refineries, oil terminals, pumping stations, and export infrastructure are designed to reduce Moscow's freedom of action. Recent attacks against facilities near Moscow, Crimea, Krasnodar, and even Tyumen demonstrate how Ukraine is steadily expanding both the reach and strategic ambition of its long-range campaign. In doing so, it is imposing costs: lower

throughput, disrupted exports, higher repair and insurance burdens, diverted air defenses, and growing uncertainty inside Russia's political and industrial system.

This campaign has already shown strategic-economic effects, with Ukrainian President Zelenskyy asserting that in March alone, Russia suffered $2.3 billion in lost revenue as a result of intensified long-range attacks against Russian port and energy infrastructure. Sustained attacks on revenue, fuel, transport, and repair networks reduce Moscow's ability to finance, supply, and politically normalize the war.

The same logic applies to strikes on airfields, air defense systems, military production facilities, and electronics plants. Long-range strikes against facilities such as Angstrem Microelectronics in Zelenograd and MKB Raduga in Dubna are part of a campaign to reach the industrial and technological foundations of Russian military power. That is classic strategic attack: identify the systems that enable the enemy's war effort, find the critical nodes within those systems, and attack to produce operational and strategic effects disproportionate to the costs of the weapons used in the attack.

Operation Spiderweb, Ukraine's daring, covert operation to strike Russian long-range combat aircraft deep inside Russia on Russian bases with remotely operated drones, sharpened the point. The Center for Strategic International Studies described the operation delivered a major blow to Moscow's long-range bomber fleet; the Washington Post reported Ukrainian intelligence claims that up to 12 bombers, including Tu-95 aircraft used to strike Ukrainian cities, were damaged or destroyed. Even if final battle damage assessments vary, the operational message is unmistakable: Ukraine is attacking Russia's ability to project air and missile power, not merely reacting to it at the point of impact.

This is strategic attack adapted to account for the limitations of Ukraine's military. Desert Storm used stealth aircraft, cruise missiles, precision-guided munitions, airborne command and control, space-enabled navigation, and massive conventional combat aircraft and logistics capabilities. Ukraine is leveraging commercially influenced electronics, adapted airframes, distributed launch methods, maritime uncrewed systems, and intelligence fusion to the same kind of effects. Due to limits on what U.S. and European deep attack systems the West will provide, Ukraine is domestically producing its own unique long-range capabilities, such as the FP-1 Firepoint, RS-1 Bars, and Bars-SM Gladiator, to penetrate dense Russian air defenses and strike military related facilities in the Moscow region.

Ukraine is not replicating Desert Storm but rather translating the logic of that air

campaign into a new context: a war in which neither side has air supremacy, and in which Ukraine lacks sufficient weapons and faces a nuclear-armed adversary with strategic depth. Its campaign is therefore more episodic, more improvised, and more constrained. But its essence is recognizable: parallel pressure against military, industrial, energy, and psychological systems; precision sufficient to attack specific nodes; and a theory of victory that seeks to change enemy behavior by making the cost of aggression increasingly costly.

That is also why the campaign should not be judged solely by whether it produces immediate territorial gains. Strategic attack only rarely achieve their objectives with a single blow. It accumulates effects. It forces the adversary to divert air defenses from the front to the homeland. It compels dispersal of aircraft and production. It raises insurance, transport, repair, and security costs. It reduces refinery throughput. It complicates military logistics. It imposes political costs, creating uncertainty in the minds of commanders, industrial managers, political elites, and citizens.

This is precisely the realm of effects-based operations. Strategy must be understood as the orchestration of means to accomplish ends and to optimize actualization of that goal target selection must focus not on the absolute destruction of a list of targets, but on the effects desired upon target systems. That sentence captures Ukraine's emerging approach. Kyiv is not trying to bomb Russia into submission in the crude sense sometimes associated with early airpower theory. It is trying to deny Russia the ability to wage war cheaply, confidently, and indefinitely.

The moral and legal distinction is essential: Strategic attack does not mean indiscriminate attack. In fact, the maturation of airpower from World War II to Desert Storm was, in large part, the story of moving from area destruction toward more precise attacks on military and war-sustaining systems. That distinction is visible today in the contrast between Ukrainian and Russian long-range strike. Russian attacks have repeatedly targeted civilian areas, apartment blocks, hospitals, schools, civil power grids, and other nonmilitary sites. These attacks suggest either deliberate terrorism, poor intelligence, weak target development, or a disregard for civilian harm. Ukraine's legitimacy depends on continuing to do the opposite: focusing on military objectives and war-supporting infrastructure, using accurate, precise, and timely intelligence, and applying disciplined target planning to minimize civilian harm.

Russia possesses proportionately greater long-range strike capacity, but it lacks the leadership, training, perspective and doctrine required to translate that capacity into decisive strategic advantage. Ukraine has fewer means, but it is learning how to make them count. That is the

fundamental difference between the two sides: one uses strike largely as punishment and coercion against society; the other is increasingly applying strike as a targeted means of disrupting the systems that sustain aggression.

There is an important lesson for the United States and its allies here. Ukraine's campaign demonstrates that long-range strike is not a luxury, but a strategic necessity. A state that can only defend at the front is condemned to absorb punishment indefinitely. A state that can reach the enemy's arsenals, refineries, command nodes, ports, airfields, and production base can change the war's logic. That is why sustained support for Ukraine's long-range attack capacity should not be viewed as escalatory. Properly bounded, legally employed, and strategically directed, it is a means of shortening the war by attacking Russia's capacity to continue it.

The West has too often treated long-range strike as a reward to be rationed rather than as a requirement to be integrated into a coherent theory of victory. That caution has carried costs. Every delay in providing Ukraine the means to hold Russia's war-sustaining systems at risk gives Moscow the gift of time to adapt, repair, disperse, and continue its assault. Recent steps to expand Ukraine-based and European production of long-range missiles and air-defense systems are welcome, but the strategic logic should be clearer: Ukraine needs the ability to impose recurring costs on the systems that sustain Russia's aggression. The objective should not be symbolic retaliation or indiscriminate punishment. It should be the systematic disruption of the military, industrial, logistical, energy, and command systems that allow Russia to keep fighting.

The Airmen of the interwar years of the 1930s understood the vulnerabilities of modern industrial states before they had the tools to exploit them effectively. World War II proved both the ambition and the limits of their theories. The Desert Storm air campaign showed what happened when precision, stealth, information, and operational design finally converged. Allied Force showed that airpower could contribute to coercive political outcomes under severe constraints. Ukraine is now writing the next chapter: strategic attack conducted by a nation without air superiority, using improvised but sophisticated long-range systems to impose systemic costs on a larger aggressor.

Technology alone has never won wars, but strategy determines whether technology matters. Ukraine's achievement is not simply that it has built longer-range weapons. It is that it is using them in accordance with a coherent strategic logic: attack the systems that sustain Russian aggression, complicate Moscow's choices, reduce Russia's ability to generate combat power, and improve Ukraine's position for an eventual settlement.

If the United States and its allies want this war to end sooner, they should help Ukraine expand that logic—not constrain it. Providing Ukraine the long-range attack means to hold Russia's war machine at risk could accelerate the conclusion of the war by making continued aggression more costly than negotiation.

But there is another imperative as well. Ukraine is paying in blood for real-world lessons about long-range strike, air defense, uncrewed systems, electronic warfare, targeting, intelligence fusion, resilience, dispersal, deception, and the operational art of fighting a larger adversary under persistent attack. Even a modest increase in U.S. and allied investment—including the placement of U.S. military observers in Ukraine—would yield lessons that could prevent American and allied forces from having to relearn them later at far greater cost. Supporting Ukraine is therefore not only about bringing this war to a faster and more favorable conclusion. It is also about absorbing the lessons of this war before the next one imposes those lessons on us.

The weapons have changed. The theory has endured. Ukraine is proving that even improvised means, when guided by sound strategic logic, can produce effects once reserved for great-power air forces.

U.S. and allied leaders must therefore recognize that helping Ukraine achieve its strategic attack objectives may be the fastest path to ending the war, turning battlespace strength into decisive leverage, bringing closure sooner than any other available course, and ensuring that the hard lessons Ukraine is learning are not paid for again by American and allied forces in a future conflict.

***

The Drone Revolution that isn't

Sandor Fabian | 07 July 2026

Source: West Pont.edu | https://mwi.westpoint.edu/the-drone-revolution-that-isnt/

Image Source: Created by author using Chatgpt AI

Today, before a tank explodes, before a trench is overrun, and before an artillery battery is silenced, someone is usually recording.

The defining images of modern war no longer come from embedded journalists or military photographers. They are being delivered by drones. First-person-view drones racing through shattered buildings, quadcopters dropping grenades into open hatches, and loitering munitions destroying

radar systems have become the defining image of twenty-first-century battlefield. These videos dominate social media, shape public perceptions, and increasingly influence political debates about defense planning and spending. The conclusion seems to be drones have changed warfare forever. Yet, this conclusion is only half correct.

Drones have indeed become indispensable military tools. They have democratized access to aerial reconnaissance, improved tactical precision, and lowered the cost of surveillance and strike missions. But the public discourse has drifted from acknowledging their importance to declaring them revolutionary. In doing so, it risks repeating a familiar mistake. Throughout history, many generations have believed they had discovered the technology that would fundamentally rewrite the rules of war. Gunpowder, machine guns, tanks, strategic bombers, precision-guided munitions, and cyber capabilities were each hyped as revolutionary innovations that would render previous forms of military power obsolete. None of them did. Instead, they became valuable components of broader military ecosystems.

Today's fascination with drones reflects the same pattern. The problem is not that militaries are investing in drones—they indeed should. The danger is that policymakers, security experts, and even some defense planners are mistaking a tactical innovation for a strategic revolution. Doing so risks distorting procurement priorities, weakening combined arms capabilities, and encouraging the repeatedly refuted belief that technology can substitute for strategy.

The Difference Between Tactical Success and Strategic Advantage

The argument for the revolutionary power of drones is understandable. In contemporary conflicts, cheap drones have destroyed armored vehicles worth millions of dollars, provided real-time targeting for artillery, and conducted persistent surveillance—capabilities reserved only for major powers until now. These developments are genuinely significant. But tactical utility is not equal to strategic success.

Military history is filled with technologies that produced remarkable tactical results without determining the outcome of wars. German tanks were tactically formidable, yet Germany still lost World War II. Precision-guided munitions transformed air campaigns but did not eliminate the need for ground forces in Iraq or Afghanistan. Superior aircraft have repeatedly failed to secure political objectives when not integrated into broader military strategies.

War is won through the interaction of the adversaries' military forces with logistics, industrial production, political will, economic resilience, leadership, and alliances. While drones can indeed

influence many of these factors, they cannot replace them.

The current public discourse often overlooks this important distinction because drones produce extremely visible battlefield effects. Today, a successful strike is easily recorded, shared, and understood. Logistics networks, maintenance depots, industrial production, electronic warfare units, and command structures—the overall ecosystem that makes drone operations possible—are almost never shown in viral videos. One of Ukraine`s best known drone strike on Russian airbases, codenamed Operation Spiderweb, is a telling example of the requirements of successful drone operations. The lack of visibility on all parts of the ecosystem creates a cognitive bias since observers only remember the spectacular images of successful strikes but tend to ignore the invisible infrastructure that enabled it.

Viral Warfare Is Not Representative Warfare

Social media has fundamentally changed how wars are consumed by observers. Before the Ukraine conflict, the public understanding of war depended on official government briefings, the accounts of military correspondents, and postconflict documentary footage. Today, thousands of battlefield videos are shared daily on the internet, many of them recorded directly by drones. These images offer near-real-time, dramatic, high-definition perspectives naturally attracting observer attention. However, these videos tell only part of the real story.

Successful drone operations are recorded and shared because success is worth sharing. On the other hand, failed missions almost never become viral. Few videos show drones losing contact due to electromagnetic interference, crashing because of battery failure, or being defeated by camouflage and deception. The observers therefore witness a curated sample of battlefield outcomes rather than an accurate statistical representation.

Military organizations evaluate technologies differently. They analyze number of sorties, mission success rates, operational availability, replacement cycles, maintenance demands, operator training, and sustainability. These metrics present a more balanced understanding than the selective and often modified imagery dominating the internet.

This distinction is important because defense planning and spending-related decisions increasingly happen under the influence of public discourse. If political leaders made the mistake of equating viral visibility with strategic effectiveness, they risk prioritizing technologies that generate headlines over real military capabilities that produce effective and sustained combat power.

For Every Revolution a Counterrevolution

History suggests another reason to

be skeptical about drones' revolutionary impact: Military technologies have seldomly had prolonged periods of uncontested dominance. Every offensive innovation soon generated defensive adaptation.

The introduction of gunpowder and cannons led to major changes in fortification. The appearance of the tank was quickly followed by the introduction of antitank weapons. The radar quickly prompted the inventions of electromagnetic countermeasures. Precision-guided weapons encouraged major doctrinal changes such as dispersion and deception. The development of offensive cyber capabilities accelerated innovation and investments in cyber defense. Drones are no exception to this trend.

One of the countermeasures to drones has been the rapid expansion of electronic warfare. Today`s militaries increasingly view the electromagnetic spectrum as a contested battlefield. Jamming, spoofing, signal interception, and cyber interference have become routine components of military operations to counter unmanned systems. Many drones remain heavily dependent on satellite navigation, radio-frequency communications, and data links. These dependencies create potential vulnerabilities and when they are exploited drones may lose their targets, return home prematurely, or become unusable. The outcome is an ongoing technological competition between drones and counterdrone technology rather than a one-sided revolution. Improvements in drone autonomy are being matched by advances in electromagnetic warfare, air defense, passive detection systems, deception, and technologies to counter unmanned aircraft.

This dynamic should temper predictions that drones will dominate future battlefields indefinitely. Their effectiveness will not only depend on innovation in drone technology but also on the pace of defensive adaptation.

Cheap Does Not Equal Economical

Perhaps the most convincing argument surrounding drones is economic. Why invest millions in advanced aircraft or armored vehicles, critics ask, when relatively inexpensive drones can destroy them? This comparison is indeed appealing, but it is incomplete.

A drone is not simply a flying munition, but the visible tip of an extensive operational ecosystem. Effective drone operations require trained operators, maintenance personnel, communications networks, secure software, batteries, replacement components, launch equipment, intelligence support, logistics, and increasingly sophisticated electronic warfare protection.

Moreover, drones are highly consumable. In the Ukraine conflict, drone attrition rates are extraordinary. As of 2025, Ukraine was deploying nine thousand drones per day. Weather, mechanical failures, signal interference, and enemy action ensure that large numbers of drones never complete

their intended missions. For these reasons the true economic calculation for militaries is not just the cost of purchasing drones but that of sustaining drone operations over months or years of war. That requires industrial capacity, resilient supply chains, and reliable manufacturing—precisely the factors that have always determined success in prolonged wars.

Therefore, the economics of drone warfare are less revolutionary than often portrayed by advocates. Unmanned systems may be cheap, but maintaining a persistent drone capability at scale remains a demanding industrial undertaking for most countries. In this respect, drones reinforce rather than replace one of war's oldest lessons: Industrial resilience matters as much as technological ingenuity.

Drones Do Not Replace Combined Arms Warfare

One of the clearest distortions in today's drone debate is the assumption that unmanned systems are beginning to replace traditional military capabilities rather than complement them. The evidence from contemporary conflicts seems to support such claim. Observes see tanks being destroyed by first-person-view drones, infantry tracked and killed by overhead quadcopters, artillery directed by real-time aerial video feeds. Yet what is often missing from this picture is everything that makes those drone missions possible—and everything else required to hold ground, sustain operations, and achieve political objectives.

Drones do not seize cities. They do not secure supply routes or hold defensive lines. They do not evacuate civilians, repair infrastructure, or enforce political control. At best, they shape the battlefield in coordination with traditional military capabilities such as artillery, electronic warfare, infantry, and armor. At worst, they are quickly neutralized when operating in isolation against a prepared adversary.

This is why the most effective militaries do not treat drones as a replacement capability, rather they treat them as an extension of combined arms maneuver warfare. In such model, unmanned systems improve reconnaissance, enhance targeting speed, increase lethality, and reduce risk to personnel while they do not substitute for the core functions of ground forces, airpower, and naval control.

The problem with much of the current public discourse is that it isolates drones from the system that gives them meaning. A drone strike is not an independent event. It is the end point of a long chain: intelligence collection, target validation, communications relay, operator training, logistical sustainment, and often coordination with other traditional military capabilities. Remove any part of that chain, and the effectiveness of drones declines sharply.

The Other Revolutions That Weren't

The idea that drones represent a groundbreaking shift from past military practice is also weakened by historical precedent. Modern military history is filled with cases of new technologies that were believed to be decisive—only for reality to prove more complex.

For instance, airpower theorists in the interwar period argued that strategic bombing would make ground armies obsolete. World War II demonstrated instead that airpower was indeed powerful but insufficient on its own for achieving political objectives. Even the most intense bombing campaigns required ground invasions to achieve the desired outcomes.

In the 1990s, the so-called Revolution in Military Affairs suggested that precision-guided munitions, advanced sensors, and networked command systems would create near-perfect battlefield awareness and enable rapid, decisive wars. While these technologies did in fact transform certain aspects of warfare, they did not eliminate friction, uncertainty, or the need for sustained ground operations.

More recently, cyber capabilities were predicted to be capable of disabling adversaries without traditional military engagement. Yet cyber operations have instead become one component of broader hybrid strategies, not a replacement for conventional force.

The pattern is consistent. New technologies have reshaped warfare, but they have not eliminated its fundamental characteristics. Uncertainty, adaptation, friction, and the need for sustained political and military effort all remain important factors. Unmanned systems fit within this pattern: transformative at the tactical level, but evolutionary and not revolutionary at the strategic level.

Why the Drone Narrative Persists

So, if drones are not revolutionary in the strategic sense, why has the narrative of transformation become so dominant?

The first reason is extreme visibility. Drones produce real-time and visually compelling war footage almost immediately available to the public. A first-person camera flying through a trench or hitting a target creates a sense of precision and control that older forms of warfare rarely provided. This gives drones an outsized influence on public perception.

Another factor is accessibility. Unlike fighter aircrafts or precision-guided munitions, drones are relatively cheap, commercially available, and widely distributed. This creates the impression that military power itself has been democratized and suggesting that small military formations or even individuals can now deliver strategic-level effects.

Finally, there is also a structural incentive within defense industries and political systems to emphasize innovation. Defense industry stakeholders compete

for contracts and policymakers seek visible signs of modernization that provides an advantage over perceived adversaries. Drones fit neatly into narratives of technological progress.

The Real Lesson: Adaptation, Not Replacement

A more sophisticated conclusion from recent conflicts is not that drones are redefining the rules of war, but that they are accelerating a long-standing dynamic: the continuous interaction between military innovation and counterinnovation.

Drones improve situational awareness, targeting, communication, and precision-strike capabilities. In response, adversaries invest in electronic warfare, camouflage, dispersion, deception, and air defense. As drones become more autonomous, countermeasures evolve to disrupt autonomy. As swarms become more networked, efforts intensify to degrade communications and navigation systems. This is not a break from a historical pattern. It is the pattern.

The real lesson is therefore not about drones alone, but about the speed of innovation and adaptation. Militaries that integrate drones into flexible, resilient force structures gain an advantage. Militaries that treat drones as a substitute for broader capabilities risk building systems that are optimized for a narrow slice of the battlefield and vulnerable to countermeasures.

What Defense Planners Should Do Instead

If drones are overhyped as a standalone revolution, the implication is not that they should be deprioritized. It is that they should be properly contextualized within broader force design.

First, investment in drones should be matched by equal or greater investment in electronic warfare. Control of the electromagnetic spectrum is increasingly decisive in determining whether unmanned systems function effectively at all.

Second, militaries should resist the temptation to hollow out conventional forces in favor of unmanned systems. Combined arms warfare remains the foundation of modern combat effectiveness, and drones are most powerful when integrated into it.

Third, industrial capacity and logistics should be treated as central components of drone warfare. Sustained drone operations require production depth, supply chain resilience, and rapid replacement and innovation cycles. Without these, even technologically advanced drone fleets degrade quickly under combat conditions.

Fourth, defense organizations should focus less on the spectacle of individual drone strikes and more on operational metrics such as sustainability, resilience under electronic attack, integration with other systems, and performance over time.

Finally, militaries should invest in training and doctrine at least as much as in hardware. Drones amplify the importance of human decision-making; they do not eliminate it. Organizations that develop effective concepts of employment will gain more advantage than those that simply acquire larger inventories of unmanned systems.

The Enduring Logic of War

This is not to simply say that drones are overrated or that they lack value. It is that they are too often misunderstood. They are treated as symbols of a new era of warfare when they are better understood as part of an ongoing evolution in military capability. They expand what is possible at the tactical level, but they do not resolve the fundamental challenges of war: sustaining operations, adapting under pressure, integrating multiple domains of conflict, and translating military action into political outcomes.

The enduring logic of war has not changed. Technology indeed matters, sometimes even decisively at the tactical edge, but wars are still decided by the ability to coordinate complex systems over time and space, withstand adaptation by adversaries, and align military means with political ends. Drones will absolutely be central to future conflicts. But they alone will not define them.

***

The New Face of Warfare: Rise of Multi-Domain Conflict

Ali Hamza | 31 July 2026

Source: ia-forum | https://www.ia-forum.org/Content/ViewInternal_Document.cfm?contenttype_id=1&ContentID=23434

In the past, wars were mainly fought through conventional means, including tanks, infantry, aircraft and naval vessels but recent conflicts such as the Russia-Ukraine conflict, Israel's twelve-day war with Iran in June 2025 and the recent US-Israel war with Iran show that modern warfare is changing rapidly as contemporary wars move beyond traditional to multi-domain operations. Technologies like Artificial Intelligence (AI), drones, cyber capabilities, satellite systems and digital surveillance are becoming important for military strategy and operations to perform in a network-centric operational environment.

Cyber warfare has become a core element of modern conflicts in this transformation, making cyberspace a strategic battleground along with land, air and sea. Today, countries combine cyber operations with kinetic force to target critical infrastructure, military communication networks, and energy grids to disrupt adversaries' capabilities. Also, AI and autonomous systems are revolutionising militaries by increasing decision-making speed and planning, while AI-driven systems such as autonomous drones or unmanned vehicles, advanced data analysis and targeting tools are allowing armed forces to process information faster

and conduct operations quickly.

The Russia-Ukraine conflict and the US-Israel and Iran war present clear examples of using cyber operations and advanced technologies with traditional military operations. In Russia-Ukraine conflict, cyberattacks have been used alongside ground operations, missile and drone strikes to target communication systems, energy infrastructure and other critical structures. For example, a Viasat Ka-Sat satellite, owned by the US-based Company Viasat that provides internet services to Europe and a small part of West Asia, was subjected to a cyberattack on the same day the conflict started, which resulted in tens of thousands of satellite modems being disrupted across Europe including Ukraine. The conflict also highlights the extensive use of drones for surveillance, reconnaissance and precision strikes with real-time satellite imagery and data. In recent months, Ukraine has increased the use of drones to target energy infrastructure deep inside Russia. For instance, the Novokuibyshevsk refinery, which is one of Russia's largest oil refineries, with an annual processing capacity of approximately 8.8 million tons of crude oil, has repeatedly been targeted by Ukrainian drones. These strikes led to reduction of approximately 300,000 – 400,000 barrels per day in Russian oil production in April 2026.

Similarly, the US-Israel and Iran war has also highlighted the significance of cyber operations and the use of advanced AI models in modern conflict environment. Operation Epic Fury, a joint US-Israeli military campaign launched on 28 February 2026 against Iran, combined kinetic attacks with cyber warfare, AI-driven targeting, electronic warfare, space-based intelligence and real-time battlefield data integration. Based on available sources and experts' assessments, cyber operations were coordinated with kinetic attacks to disrupt Iranian command-and-control networks, military communications, missile and air defense systems including integrated radar networks. The operation also demonstrated how AI-assisted intelligence and real-time data fusion have changed the conduct of modern military operations. Before the airstrikes, the US employed AI systems to process enormous amounts of intelligence collected through satellites, reconnaissance aircraft, MQ-9 Reaper drones, cyber intelligence, signal intelligence (SIGINT), electronic intelligence (ELINT), and other intelligence, surveillance and reconnaissance (ISR) assets to accelerate target identification and military planning.

In present era, information warfare (IW) has also become a key feature of modern conflict. Though IW has always been part of conflict but advances in technology, AI, social media and cyber domain have transformed it into a main component of modern wars. Today, controlling the narrative and domination of cyberspace are as important as controlling territory on the battlefield because governments also seek to manage how wars are perceived.

States use disinformation campaigns, social media manipulation, psychological operations and digital influence campaigns to shape public perception and influence strategic outcomes.

In Gaza war, Israel employed IW as a tool to justify its illegal military actions. It targeted civilian infrastructure such as schools, hospitals, residential blocks, and mosques, framing these sites as Hamas hideouts without providing verifiable evidence. While these actions by Israel have caused large-scale civilian casualties, Israeli officials amplified these fake claims about hideouts with their influence in Western media to shift responsibility for casualties onto Hamas. This IW strategy was systematically used by Israel not to inform global audiences, but to shield its military actions that many scholars and leaders have described as war crimes and genocide.

In March 2025, former US Director of National Intelligence Tulsi Gabbard testified in the Senate Intelligence Committee that US intelligence continued to "assess that Iran is not building a nuclear weapon" and that "Iran's leadership has not authorised a nuclear weapons program." Despite the US intelligence assessments, Israel continued political messaging and media propaganda to create an image of an imminent nuclear threat posed by Iran which illustrates how IW can be used not only during conflicts but also before kinetic action to shape perceptions and justify political decisions.

The growing role of inexpensive technologies and asymmetric power becomes another important element of modern warfare. Traditional military competition relies heavily upon expensive military equipment like fighter jets, tanks and advanced missile systems but modern technologies are allowing smaller states to challenge conventionally superior militaries through low-cost drones and missiles, accessible digital tools and commercially available technologies. A cost-effective drone can now carry out surveillance, target identification and precision strikes, while commercially available satellites such as Starlink, which was not originally designed for military purposes, provide a secure communication platform, transmission of drone video, secure broadband internet and real-time data sharing, allowing smaller states to gain advanced battlefield awareness and coordination.

The use of Shahed-131 and Shahed-136 drones by Iran in twelve-day war with Israel in 2025 and by Russia in the Ukraine conflict demonstrates this shift. These drones cost between 20,000 and 50,000 USD, compared to multi-million-dollar Western military systems used in anti-drone role, such as the Patriot, Iron Dome, and Iron Beam systems. The drones were still able to penetrate sophisticated multi-layered air defence systems, resulting in the repeated use of costly interceptor missiles to intercept them. Iran has followed a similar pattern in the recent US-Israel initiated war. This imbalance shows how inexpensive modern

technologies are allowing comparatively weaker states to impose high operational and economic costs on technologically superior adversaries.

A classic application of network-centric warfare took place in an actual operational environment in May 2025 Four-Day war between India and Pakistan, where two peer military powers were engaged in high-intensity military operations. During the war, Pakistan operated in a network-centric multi-domain environment and outclassed Indian armed forces, especially the Indian Air Force. Pakistan's operational ascendancy resulted in heavy loss of frontline Indian aircraft, including Rafale and Su-30MKI, along with ground assets. In contrast, Pakistan's Air Force suffered no loss of any aircraft during the conflict. India's dismal battlefield performance drew widespread international scrutiny and raised serious questions about the effectiveness of its aggressive military doctrine, planning and preparedness.

The contemporary warfare is therefore no longer limited to conventional military operations only, as it integrates cyber capabilities, AI, IW, space-based assets and autonomous systems within a single operational environment. Success in future conflicts will depend upon a country's ability to adapt and integrate the above-mentioned technologies into a coherent multi-domain strategy. As the nature of warfare is becoming increasingly technology-driven and interconnected, embracing these realities will be important to safeguard national security and maintain international peace and stability.

***

The Gulf's New Information Battlefield: War, Technology, and the Reconfiguration of Security

Dr. John Calabrese | 23 July 2026

Source: Manara Magazine | https://manaramagazine.org/2026/07/the-gulfs-new-information-battlefield/

Introduction

During the opening days of the 2025–2026 U.S.–Israel war with Iran, Kuwait's military briefings highlighted intercepted Iranian missiles and drones while revealing little about strike locations or damage. The approach reflected a familiar wartime dilemma in which governments must reassure populations while limiting information that could aid adversaries or fuel uncertainty. Yet Kuwait's response revealed a broader shift across the Gulf. Information was no longer simply a messaging tool; it had become part of the battlefield.

The conflict accelerated a less visible but equally consequential shift in regional security governance. Gulf states increasingly treat information flows, digital platforms, and public narratives as strategic domains requiring protection and control. Building on trends that emerged after the Arab Spring uprisings, the Iran war provided a new security rationale for regulating digital behaviour, managing

information, and redefining political loyalty. Information has become strategic infrastructure, subject to the same security concerns as physical and digital assets.

War as a Battle Over Information

The Iran war demonstrated how modern conflicts are fought simultaneously on physical and informational battlefields. Military operations, cyber activity, and narrative competition increasingly reinforce one another.

Kuwait's wartime communication illustrates how governments are adapting to this new information environment. Official briefings emphasized interception statistics while limiting disclosure of strike locations and damage assessments, reflecting an effort to reassure the public without exposing vulnerabilities or amplifying narratives of the adversary. The significance of this lies in how states increasingly shape the conditions through which citizens experience conflict.

That same contest over perception extended beyond domestic audiences to the broader U.S.–Iran confrontation. The United States and Iran both waged a parallel battle over perception, legitimacy, and public interpretation, using digital provocation, amplification, and narrative manipulation as tools of statecraft. Washington sought to project military effectiveness and operational dominance, while Tehran relied on asymmetric tools to portray resilience and resistance. Iranian officials invoked historic Persian and Shiite battles of sacrifice and endurance, framing the conflict as part of a longer struggle against foreign aggression.

Neither side treated information as separate from military strategy. Narrative became another instrument of competition.

The intensification of information warfare cannot be separated from the broader hybrid conflict between Washington and Tehran. The United States has incorporated cyber capabilities into conventional military operations, reflecting a broader shift toward integrating digital tools with kinetic force. Iran, meanwhile, has developed its own asymmetric response architecture, combining cyber operations, influence campaigns, coordinated messaging, and networks of aligned actors to impose costs and create uncertainty.

These activities blur the boundary between the battlefield and information space. Cyber operations, disinformation campaigns, and narrative competition originating from the U.S.–Iran confrontation increasingly spill over into Gulf societies. For states located between Washington and Tehran – both geographically and politically – the information environment itself has become a potential vulnerability.

Social media has further complicated this environment. Recycled footage from earlier conflicts, clips from military simulation games, and AI-generated images circulated alongside authentic reporting.

AI-generated disinformation surged, with Iranian-linked networks using synthetic media, deepfakes, and recycled footage to amplify wartime success claims, while Iran waged social media campaigns against the United States to shape narratives abroad. In many cases, misleading content reached audiences before journalists or officials could verify it, making uncertainty itself part of the conflict. For example, Gulf media monitors documented wartime restrictions on sharing unverified images and rumours, including Saudi guidance against circulating videos of an unknown source.

The challenge was therefore twofold: preventing adversaries from accessing sensitive information while limiting the ability of false narratives to shape public understanding before facts could catch up. This represents more than a media problem; it is a structural feature of modern conflict. Information fragmentation has become a defining characteristic of contemporary warfare, where battles are experienced through competing interpretations as much as through military operations themselves.

From external threats to domestic controls

The wartime information challenge has also reinforced a broader regional trend toward expanding domestic mechanisms for regulating information.

Across the Gulf, governments have incorporated digital activity into national security frameworks. Cybercrime laws, national security statutes, and emergency regulations now include broad categories such as spreading false information, harming national unity, or damaging state reputation. These provisions provide authorities with significant discretion over what constitutes a security threat, particularly during moments of crisis.

The language itself is important. Restrictions on “false information” or conduct deemed harmful to national interests can encompass genuinely harmful disinformation, but they can also extend to political commentary, criticism, or the sharing of material authorities consider sensitive. During wartime, the boundary between security protection and information control becomes especially difficult to define.

The Iran war demonstrated how quickly these legal frameworks could be activated.

In Bahrain, Reuters reported that authorities stripped citizenship from 69 people accused of supporting Iranian attacks. Rights groups argued that the measures formed part of a wider campaign against political dissent, while the government defended them as necessary to protect national security. Whatever the competing interpretations, the episode illustrates a broader shift: political belonging is being evaluated through a security lens.

Kuwait has experienced a similar evolution. Historically more politically open than many of its Gulf neighbors, Kuwait has nonetheless expanded restrictions on digital expression in response to security concerns. During the Iran war, authorities warned against publishing images of missile interceptions or security operations, and journalists and citizens have been arrested for sharing war-related footage. Information that might previously have been considered public discussion increasingly became treated as a potential security issue.

Other Gulf states adopted comparable approaches. Qatar arrested more than 300 people for circulating what authorities described as misleading information and images related to Iranian attacks. Saudi Arabia reinforced restrictions through its "Photography serves the enemy" campaign, warning citizens that documenting sensitive locations or military activity could undermine national security. The United Arab Emirates arrested more than 100 people[xiv] for filming or sharing strike-related content, relying on cybercrime legislation and digital monitoring systems to restrict the circulation of such material.

These measures reveal a broader transformation in how Gulf governments understand information. Speech and digital activity are viewed not merely as forms of expression, but as potential vectors of instability.

Importantly, the war is not the cause; it is the accelerator and legitimizer of these processes. The foundations were established years earlier. Following the Arab uprisings of the early 2010s, Gulf governments invested heavily in cyber legislation, surveillance capabilities, and mechanisms for regulating online discourse. The current conflict has increased both the perceived urgency and the political legitimacy of expanding those powers.

This securitization of information also reshapes how states define political loyalty and belonging.

Citizenship and Political Loyalty

The same security logic is reshaping debates over citizenship and political membership.

Across parts of the Gulf, citizenship has increasingly become treated not only as a legal status but also as an indicator of political loyalty. During periods of heightened regional tension, governments have used citizenship policies as instruments for responding to perceived threats.

Bahrain provides one example. Authorities revoked citizenship from individuals accused of sympathizing with Iranian attacks, in a crackdown that disproportionately affected the Shiite Muslim population and pushed three Bahraini parliamentarians toward removal for pushing back. Other reporting placed the move squarely in the context of the war and a broader anti-dissent campaign, while

rights groups argued more generally that the conflict had been used to justify a wider crackdown on dissent. Supporters of the policy maintained that governments have the right to respond against individuals believed to be assisting hostile actors.

Kuwait has experienced its own debate over citizenship revocation, marked by a dramatic increase in denationalization since 2024. Amendments to Kuwait's citizenship law broadened the grounds under which citizenship could be withdrawn, including actions considered harmful to public order or national interests. Authorities have reportedly revoked citizenship over social-media posts and other war-related expressions, prompting critics to describe citizenship as a weapon of political control. Officials defended the measures as necessary to protect state integrity.

The significance of these developments extends beyond individual cases. Rather than creating an entirely new dynamic, they intensify a longstanding feature of Gulf governance in which citizenship, political loyalty, and state security are closely intertwined. In societies where citizenship carries substantial economic and political privileges, decisions over who belongs, who can speak, and whose speech is considered threatening are increasingly interconnected. Citizenship thus functions as both a legal status and a mechanism through which states manage political and informational stability.

AI, cyber warfare, and the future of conflict

Technology will intensify these pressures. The Iran war highlighted how Artificial Intelligence (AI) and cyber capabilities are transforming the information environment. Synthetic videos, fabricated battlefield imagery, and AI-generated propaganda can now be produced rapidly and distributed widely, often before governments or journalists can verify their authenticity. During the conflict's first phase, fabricated or manipulated content moved faster than official rebuttals or fact-checking systems, demonstrating how quickly synthetic media can outpace the institutions responsible for verification.

Manipulated content circulated alongside legitimate reporting, while coordinated online campaigns amplified competing narratives. The result was an environment in which speed often mattered more than accuracy, with official corrections frequently arriving too late to shape public understanding. The spread of AI-generated content creates a difficult dilemma for governments: the same technologies that enable adversaries to manipulate information also provide justification for stronger monitoring and regulation of digital spaces. As synthetic media becomes harder to distinguish from authentic reporting, states gain both a security rationale and a political incentive to expand their role as arbiters of information.

Cyber operations have similarly become integrated into modern military strategy. Attacks on infrastructure, data systems, and communications networks are now part of the broader conflict ecosystem, shaping both how wars unfold and how societies experience them. For Gulf states, this creates a difficult balance. Open information environments can support economic innovation, technological development, and international connectivity, but they can also create opportunities for adversaries to spread misinformation or exploit social divisions. These technologies are becoming cheaper, faster, and more accessible, ensuring that the challenge will persist beyond the current conflict.

The Gulf and the Future of Information Security

The Iran war did not fundamentally alter the Gulf's approach to information control. The underlying trends were already visible. Nevertheless, the conflict accelerated them by demonstrating how quickly external threats can become intertwined with domestic governance.

Across the region, tighter cyber laws, expanded surveillance capabilities, curated wartime narratives, and restrictions on digital expression reflect a broader shift in how states define security. Information is treated as strategic infrastructure.

The Gulf may therefore represent an early example of a broader global trend. As governments confront conflicts in which cyber operations, AI, and information manipulation accompany conventional military threats, similar pressures are likely to emerge elsewhere.

The central challenge for governments will be strengthening resilience against genuine security threats without permanently narrowing the space for independent information and political debate. In an era when information has become a battlefield, controlling the narrative may provide short-term stability. Durable security will depend on something more difficult: ensuring that citizens continue to trust the information they receive.

***

Air Power

IAF's Dogfight for Superiority Over AI and Statecraft

Air Vice Marshal Prashant Mohan VM (Retd) | 26 July 2026

Source: CAPSS | https://capssindia.org/from-tiger-hill-to-muridke-the-evolution-of-precisiobombing-in-the-indian-air-force/

Image Source: Press Information Bureau, Government of India

The character of aerial bombing has changed more in the past decade than in the preceding three decades, and precision has been the constant thread running through that change. The United States of America (USA) and Israel remain at the frontier of this evolution, increasingly fusing space-based cueing, cyber disruption, electronic warfare (EW), and artificial intelligence (AI) into the targeting cycle itself rather than treating them as separate enablers of a strike, a fusion visible in how quickly recent Israeli campaigns have moved from decision to precision effect against dispersed, defended target sets. India's own tryst with precision bombing began considerably more modestly, in the high Himalayas in the summer of 1999, and has advanced in fits and starts ever since, shaped as much by sanctions and improvisation as by deliberate long-term planning. Tracing that arc from Operation Safed Sagar to Operation Sindoor offers a useful lens on both how far the Indian Air Force (IAF) has come and how much distance remains to the frontier that Washington and Tel Aviv currently occupy.

Operation Safed Sagar: Precision Born of Necessity

Operation Safed Sagar was the Indian Air Force's codename for its air operations in support of Operation Vijay during the 1999 Kargil War, the first large-scale employment of air power in the Kashmir theatre since the 1971 India-Pakistan War. Its standout feature was not that precision bombing was planned for, but that it was improvised under fire. The IAF crews found themselves fighting at altitudes of 16,000 to 18,000 feet, where thinner air meant that bombs released using sea-level ballistic tables consistently overshot their targets, and where Pakistani infiltrators, dug in on the high ground, could bring man-portable Stinger missiles to bear on aircraft that were, unusually, flying below the enemy's firing positions rather than above them. This can reasonably be called the genuine start of precision bombing in Indian military aviation, rather than merely accurate bombing, because it was here that the IAF first integrated laser designation and satellite-aided targeting into a live campaign. India had purchased Paveway-series laser-guided bomb kits and Litening targeting pods, but the US sanctions following India's

1998 nuclear tests had left the integration with the Mirage 2000's 1985-vintage mission software incomplete; the IAF, with Israeli technical assistance, completed the integration in a reported twelve days once the war began.

The operational payoff came at Muntho Dhalo and Tiger Hill. A single strike by four Mirage 2000s, each dropping six 250-kilogram bombs, destroyed a major supply dump and is credited with breaking the momentum of the Pakistani defence far more decisively than the more widely publicised Tiger Hill footage. By early June the IAF had flown over 1,200 strike sorties, and the campaign is judged to have shortened the war by roughly three weeks. The psychological effect was equally significant: an Indian Army message to the Air Headquarters at the time credited the Mirage strikes with breaking enemy command and control so thoroughly that troops "literally walked over the entire Tiger Hills area," a rare instance of an army field formation crediting air power directly for an infantry advance.

From Muntho Dhalo to Muridke: The Growth Chart

Precision bombing did not resurface as a headline capability for two decades, but it did not stand still either. The next major milestone came on February 26, 2019, when twelve IAF Mirage 2000s struck a Jaish-e-Mohammed (JeM) training camp at Balakot in Khyber Pakhtunkhwa, in retaliation for the Pulwama attack, under the codename Operation Bandar. While Op Safed Sagar relied on hastily integrated laser-guided bombs, Balakot employed Israeli-made SPICE-2000 precision munitions, pre-fed with Global Positioning System (GPS) coordinates and using electro-optical terminal guidance, reportedly achieving an error margin of under three metres against targets fifty to sixty kilometres from the release point. It also marked the first time since 1971 that the IAF had struck a target inside Pakistan's mainland rather than Pakistan-occupied Kashmir (PoK), a qualitative escalation in both reach and political signalling that Op Safed Sagar had not attempted.

Operation Sindoor in May 2025 represents the next, and by far the largest, leap. Where Op Bandar was a single-target strike by one aircraft type, Op Sindoor saw the IAF strike nine locations, including the Jaish-e-Mohammed (JeM) and Lashkar-e-Taiba (LeT) headquarters at Bahawalpur and Muridke, using a coordinated mix of BrahMos supersonic cruise missiles fired from Su-30MKIs, French-origin SCALP-EG cruise missiles and HAMMER precision-guided bombs delivered by Rafale fighters. Nineteen BrahMos and nineteen SCALP missiles were reportedly employed in a single coordinated stand-off strike, marking BrahMos's first use in actual combat after two decades in service and SCALP-EG's combat debut in a state-on-state engagement. The growth from Muntho Dhalo to Muridke, in these terms, is a growth from manually retrofitted gravity bombs to imported precision-guided munitions on

a single platform, to a networked, multi-platform, multi-missile stand-off strike package capable of hitting targets roughly 150 kilometres inside Pakistan's territory with, by the IAF's own account, negligible collateral damage.

The Platforms Behind the Progress

Each leap in precision has ridden on a corresponding leap in aerial platforms. The Mirage 2000 carried Indian precision bombing through both Op Safed Sagar and Op Bandar, and remains in many respects the IAF's most combat-proven precision strike aircraft. Op Sindoor, by contrast, showcased the Su-30MKI as a heavy stand-off missile carrier and the Rafale, inducted from 2021, as a genuinely multi-role precision platform integrating French-origin munitions unavailable to earlier IAF fighters. The shift also reflects a broader doctrinal change: where Op Safed Sagar and even the operation in Balakot required aircraft to approach relatively close to their targets, Op Sindoor's cruise missiles allowed strike aircraft to remain within Indian airspace throughout, trading platform risk for munition sophistication.

Building an Indigenous Precision Arsenal

India's growing awareness of its continued reliance on imported precision munitions- SPICE-2000, SCALP-EG and HAMMER- all of foreign origin, has driven a parallel indigenous effort. The Defence Research and Development Organisation (DRDO)'s Smart Anti-Airfield Weapon, a 125-kilogram precision glide bomb with a range of roughly 100 kilometres, was employed operationally for the first time during Operation Sindoor against Pakistani airfields, and a satellite-guided variant is now being processed for wider fleet integration. In April 2025, DRDO also completed release trials of the 1,000-kilogram-class Gaurav long-range glide bomb from a Su-30MKI, achieving close to 100 kilometres of range with reported pinpoint accuracy. A jet-powered variant of the Smart Anti-Airfield Weapon (SAAW), under development since 2025, is intended to extend its range beyond 200 kilometres by converting it from a gravity-assisted glide munition into a self-propelled weapon, positioning it as an affordable complement to BrahMos rather than a replacement for it. These programmes, alongside the Rudram family of anti-radiation missiles, mark a deliberate move from assembling imported precision kits toward owning the underlying guidance and propulsion technology. However, the gap between a successful trial and full squadron-level integration has historically stretched over several years for comparable Indian systems, a lag the IAF is now trying to compress.

The Distance That Remains

Set against the American and Israeli frontier, where precision strike is now routinely fused with pre-positioned intelligence assets, satellite cueing, cyber disruption of enemy command networks, and AI-assisted sensor fusion to compress the time between decision and impact to

a matter of hours across an entire enemy air defence network, India's progress from Muntho Dhalo to Muridke, though genuine, remains an evolution in munitions and platforms rather than in the full targeting ecosystem around them. Indigenous glide bombs and cruise missiles address the hardware gap; closing the gap in space-based cueing, offensive cyber integration, and AI-driven target prioritisation is the harder, and still largely unfinished, task ahead.

***

The Sky as a Minefield: How Drone Swarms will Reshape Air Defence

Lt Gen Philip Campose (Retd) | 01 July 2026

Source: The Week | https://www.theweek.in/news/defence/2026/07/01/opinion-campose-how-drone-swarms-will-reshape-air-defence.html

This photo released by Iranian state media and geolocated

When an American F-15 went down in contested airspace this year during the West Asia war, one pilot described what he saw just before he was hit as "flying into a minefield of drones." Whether the pilot's description sticks or not, the image is apt: we are glimpsing an inflection in air warfare where the sky itself can be seeded with cheap, autonomous platforms that complicate-and sometimes defeat-expensive aircraft and missiles. The result is not simply another weapons system to be added to the shelf. It is a doctrinal rupture that will reorder tactics, budgets and the very meaning of air superiority.

For decades, air defence revolved around layered, ground-centric arrays: radar belts that detect, command posts that decide, and guided interceptors or guns that engage. These systems are effective in conventional settings, but they assume a scale and economy the modern battlefield may not permit. Missiles and manned fighters are costly; many unmanned systems are not. That asymmetry is the fuel behind the aerial minefield: by distributing risk across swarms of inexpensive drones-many expendable-an adversary can impose attrition costs and operational friction that traditional defences struggle to absorb.

From Batteries to Swarms

The essence of the aerial minefield is not a single type of drone but an integrated ecosystem. Practical implementations rest on four functional layers working together. First, persistent surveillance drones carry electro-optical, infrared and passive electronic sensors that find and track targets.

Second, communication - relay

"motherships" sustain swarm coherence and distribute targeting information to subordinate units.

Third, low-cost kinetic or kamikaze interceptors physically threaten aircraft and missiles.

Fourth, electronic-warfare platforms jam, spoof and degrade an attacker's sensors and links.

Crucially, artificial intelligence binds these layers. Swarm algorithms permit scores or thousands of nodes to distribute tasks, adapt to losses, prioritise threats and cooperate in real time. Human operators cannot micromanage such numbers; autonomy is an operational necessity, not mere convenience. The result is an aerial obstacle course: aircraft must thread formations, distinguish friends from foes, and face the prospect that every empty patch of sky could hide a lethal node.

Ukraine and Iran as Laboratories

The Russia-Ukraine war has become the world's laboratory for massed unmanned systems. Ukrainian units routinely deploy small interceptors against Russian drones, use first-person-view attack UAVs for tactical strikes, and entwine electronic warfare and cyber measures at the tactical edge. These engagements have normalised drone-versus-drone combat and shown how layered, affordable defences can blunt more sophisticated adversaries.

Iran's forays into swarm tactics-and the reported use of drones in the strikes and harassment campaigns of recent years-offer a different, worrying confirmation: states willing to mass-produce cheap UAVs can alter local air dynamics quickly. The combination of large numbers, kamikaze tactics, and electronic countermeasures produces effects disproportionate to the cost of individual units.

Economics: The Decisive Variable

Military history is full of examples where economics drives innovation. An F-35 or a long-range cruise missile carries a price tag in the tens of millions of dollars; many combat drones can be manufactured for thousands or less. Using a cheap drone to neutralise an expensive asset flips the attrition calculus. Nations with manufacturing scale and doctrinal commitment to swarms-notably China, Iran, Russia and Pakistan-are already exploiting this asymmetry.

China's investments are especially consequential. Its exercises have demonstrated hundreds of coordinated UAVs operating under AI-enabled control, and its industrial base means it can field such systems at scale. For India-which faces both a technologically advanced neighbour on one border and growing drone inventories on the other-this is not a hypothetical threat; it is a near-term strategic reality.

AI: Software as a Strategic Asset

If platforms are the body of a drone force,

software is the nervous system. Swarm intelligence, distributed decision-making, graph neural networks for perception, and resilient ad-hoc communications convert fleets of airframes into effective defensive lattices. The state that masters sovereign AI for contested environments-secure, explainable, and operable under electronic attack-will enjoy a decisive edge.

That raises two connected points. First, reliance on foreign cloud services or opaque commercial autonomy is a wartime vulnerability. Second, the competitive advantage will accrue less to the buyer of the most airframes than to the developer of robust, field-hardened autonomy. In practice, that means substantial investment not just in airframes, but in algorithmic research, data collection, simulation infrastructure and explainable systems that can operate without pristine networks.

Manned Aircraft will not be Discarded

A common fear is that swarms will make manned fighters obsolete. The reality is more nuanced. The foreseeable future is one of manned-unmanned teaming. Pilots will increasingly operate as commanders of constellations: fighters will orchestrate swarms that scout, screen, jam and absorb enemy fire so the manned platform can prosecute the mission with reduced risk. In other scenarios, expendable swarms will undertake the most dangerous tasks entirely.

The core measure of air superiority will shift from the performance envelope of a single airframe to the quality of networks and software that coordinate many platforms. A squadron of autonomous agents, well commanded and resilient, can impose strategic effects that even the best fighter fleets will find hard to counter.

Counters and Limits

Aerial minefields are not invulnerable. Electronic warfare-jamming, spoofing and cyber intrusions-can sever swarm cohesion. Directed energy weapons, high-power microwaves, and even mass small-arms fire can reduce drone density. Weather, terrain, and logistics impose operational limits. And engineering robust, low-latency, secure communications at scale under attack is extraordinarily hard.

Thus, the coming decade will see a contest between swarms and counter-swarm technologies: mesh nets versus jammers, lasers versus curtain formations, and cyber offensives against autonomy stacks. Doctrine, training and redundancy will matter as much as hardware.

What India should do

For India, the response must be strategic, not ad hoc. Three broad lines of action should guide New Delhi:

- Create theatre-level drone air-defence units tasked with persistent aerial denial and interception, integrated with existing missile and radar networks.

Make interceptor drones a standard element of air-defence brigades rather than experimental add-ons.

- Prioritise sovereign swarm-AI research and development within DRDO, IDEX and the private sector, with clear pathways from prototype to fielding. Invest in secure, explainable autonomy, contested-environment testing ranges, and high-fidelity simulation for tactics and logistics.

- Build industrial scale and supply-chain resilience for low-cost airframes, sensors and propulsion so that "mass through autonomy" is an industrial reality as well as doctrine. Concurrently, fold electronic warfare and cyber capabilities into every swarm architecture, and establish hard rules for anti-spoofing and counter-deception.

Institutional reform will help. An autonomous systems command could codify doctrine, procurement, safety, testing and operational employment. That office should coordinate with civilian regulators, academic centres and industry to accelerate innovation while safeguarding safety and interoperability.

Policy and Ethical Guardrails

As India pursues autonomy, it must also set guardrails. Rules of engagement for autonomous systems, minimum human-in-the-loop thresholds for lethal decisions, export controls to prevent proliferation, and safeguards against unintended escalation are essential. India should also champion international dialogue on responsible military AI and explore cooperative norms or arms-control measures for swarms. Without norms, the risk of miscalculation and rapid escalation grows.

Conclusion: Code as Deterrent

Military revolutions have a pattern: those who adapt doctrine, industry and procurement together win. The aerial minefield is plausible now because airframes, sensors, networking and AI have converged. Whether it becomes a dominant paradigm depends on how quickly states integrate autonomy with existing defence structures and close industrial and algorithmic gaps.

For India, the lesson is stark and actionable. The future of air defence will be less about buying a few exquisite systems and more about fielding many intelligently coordinated ones. The decisive advantage may come not from a stealthy jet or a longer-range missile, but from the nation that best combines mass production, secure software and sovereign AI. In the coming age, the most important weapons will not only be forged in factories-they will be written in code.

***

Reforming India's Higher Defence Organisation

Gp Capt V P Naik, VM and Wg Cdr Akash Godbole | 08 June 2026

Source: ORF | https://www.orfonline.org/research/reforming-india-s-higher-defence-organisation

Introduction

Reforms in the Higher Defence Organisation (HDO) have been an unfinished agenda for India since Independence. To be sure, successive attempts have been made towards the goal, including the Kargil Review Committee (KRC) recommendations and the subsequent Group of Ministers (GoM) review in 2000–2001, as well as the creation of the Department of Military Affairs (DMA)and the post of the Chief of Defence Staff (CDS). However, the Government of India (GoI) Allocation of Business (AoB) Rules for the Ministry of Defence (MoD) remain unchanged, continuing to assign critical war-fighting functions to the Department of Defence (DoD) under the Defence Secretary. The continued assignment of "Defence of India and every part thereof" to the DoD can be read as a deliberate affirmation of civilian control, even after the creation of the DMA and the establishment of the post of CDS. Yet, without a corresponding investment in specialised civilian capacity, this formal concentration of authority in the DoD risks reinforcing existing weaknesses rather than correcting them.

This directly contradicts the much-advertised "whole of nation" approach to national security that Prime Minister Narendra Modi called for in his address at the "Swavlamban" seminar on 18 July 2022, where he emphasised the need to activate India's comprehensive national power (CNP). However, if the framework for national security is to be genuinely whole-of-nation, reforms in the HDO cannot be confined to the armed forces alone, which have not been the principal source of vulnerability in India's national security. The armed forces have consistently delivered operationally, fighting with what they had, be it during the Kargil conflict, despite acknowledged shortages of weapons and equipment[5] and serious delays in critical supplies, or during the more recent Operation Sindoor.

The real institutional deficit lies within the HDO, the decision-making machinery at the MoD level, which plans and directs the use of force. Yet, compared to the demand for change in the armed forces—as evidenced in the sweeping reforms being pursued at breakneck speed through proposed theatre commands—the ministerial machinery that frames policy and allocates authority remains untouched. The process does not provide a coherent assessment of ends, ways, and means across the entire national defence architecture. A system that has repeatedly proven its worth in battle requires reform, not in "how to fight" but rather in "how to plan, fight, and win".

This brief extends the civil–military relations (CMR) debate in India beyond

the primary concern of purely military intervention into questions of how civilian mechanisms for effective control should be designed. It argues that optimum civilian control is essential for India's national security. India's current HDO suffers from a structural deficit of defence expertise within the civilian bureaucracy, and higher defence reforms must therefore encompass both the ministry and the military. Specifically, the brief proposes creating a dedicated specialist defence management cadre in the MoD as a critical enabling reform to achieve more effective civilian control.

An Overview of India's Higher Defence Organisation

India's civilian control over its military is rightly celebrated as one of its great democratic achievements. India has been an outlier among post-colonial states, where fragile civil–military relations have often led to military coups and praetorian regimes. However, this achievement has come at the cost of military effectiveness. A popular characterisation of India's civil-military arrangement is that "politicians enjoy power without any responsibility, bureaucrats wield power without any accountability, and the military assumes responsibility without any direction." In The Absent Dialogue, Anit Mukherjee argues that once civilian control is firmly established, most systems shift their attention to "second-order" questions of military effectiveness and institutional efficiency. In India, however, that transition has remained incomplete. The problem, therefore, lies in the way civilian control has been institutionalised.

Under the Transaction of Business (ToB) Rules, the Cabinet Committee on Security (CCS) remains the apex body for decisions on defence policy, while the Raksha Mantri (RM) is the minister-in-charge responsible for the proper transaction of business in the MoD. However, because the higher defence organisation is largely staffed by generalists with limited domain expertise, it tends to pass complex or contentious issues up the chain without developing well-worked options or assuming institutional responsibility for long-term choices. In the absence of sustained political engagement, this combination of formal authority at the top and weak civilian capacity below effectively pushes the burden of strategic judgement onto political leadership. Standards acceptable in a relatively permissive security environment are no longer adequate when contemporary conflict threatens not just soldiers on the frontline but also national leadership, critical infrastructure, and civilians.

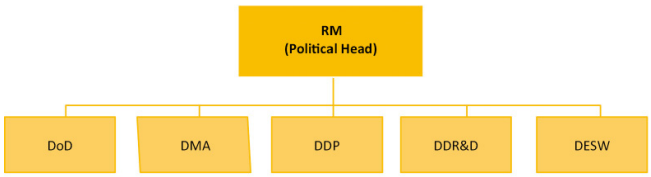
Structural Challenges

Bureaucrats in India's MoD are predominantly generalists from the Indian Administrative Services (IAS). Most appointments do not require domain specialisation, and the bureaucrats move from one department to another throughout their careers, with portfolios shifting from agriculture to health to defence. This design feature has systemic consequences for national defence. In the United States, the Office of the Secretary of Defense

(OSD), the principal civilian staff element for policy development, planning, resource management, and oversight, employs more than 2,200 staff who build defence expertise throughout their careers and assist the Secretary and Deputy Secretary of Defense. In contrast, in India, the Joint Secretary handling defence policy may have spent the previous posting managing fertiliser subsidies. As early as the late 1960s, a government committee warned that "the subordination of the military to civil power should be interpreted in the political and not in the bureaucratic sense." This distinction has seldom been honoured in practice.

In its report tabled in Parliament on 23 February 2000, the KRC observed: "India is perhaps the only major democracy where the Armed Forces Headquarters are outside the apex governmental structure." For over five decades after Independence, the three Service Headquarters were classified as "Attached Offices" of the DoD. In effect, they were administrative subordinates rather than participants in national security policymaking. The GoM recommended that Service Headquarters be redesignated as "Integrated Headquarters of the MoD" and that the GoI ToB Rules be "appropriately amended and issued" to give effect to this integration. While the redesignation was approved by the CCS in May 2001, the corresponding amendment to the ToB Rules, necessary to formalise the role of service Chiefs in apex decision-making, was never promulgated. Consequently, India's higher defence reforms have, to date, been conceived almost entirely as "reforms of the military"—including theatre commands, jointness, inter-service integration, and the CDS architecture. While 2025 was designated as a year of reforms for the MoD, no reforms were made to the ministry's bureaucratic structure.

Figure 1. The Current Civilian Bureaucratic Structure



Source: Authors' adaptation from Government of India, Ministry of Defence, Allocation of Business Rules (Ministry of Defence and its Departments)

Figure 1 shows how the current civilian bureaucratic structure functions. Political authority in defence rests with the RM and the CCS, while the secretariat is organised through the DoD, the DMA, the Department of Defence Production (DDP), the Department of Defence Research and Development (DDR&D), the Department of Ex-Servicemen Welfare (DESW), and Defence Finance. In practice, however, the DoD has overseen all matters of policy, strategic character, finance, and interdepartmental coordination. Until the formation of the DMA in 2019, the armed forces were attached offices to the MoD. It is the first time since Independence that the armed forces now have an institutional presence within the MoD through DMA. The proposed defence reform is thus not aimed at replacing the existing civilian structure but restructuring the HDO, where specialised expertise is urgent and indispensable.

Figure 2: Branches of All-India Services

Source: Authors' adaptation from Government of India, Department of Personnel and Training, "Classification of Central Government Posts."

India's civil services are broadly organised into All-India Services, Central Civil Services, and State Civil Services, with Union Services further classified into Groups A, B, C, and D according to responsibility and complexity. Group A is the higher administrative tier and includes both the All-India Services and specialised Central Civil Services (see Figure 3). The proposed defence-management cadre belongs at this level, since it is intended for policy, planning, acquisition, finance, and coordination posts, not routine administration.

Figure 3. Branches of Specialised Central Services Group A

Source: Authors' adaptation from Government of India, Department of Personnel and Training, Schedule I – Central Civil Services, Group "A"

India is not entirely without a specialised civilian presence in the defence establishment. The Armed Forces Headquarters Civil Services already provides an administrative civilian nucleus within the integrated headquarters system. However, this arrangement is not a substitute for a higher-defence management cadre, since its orientation remains largely secretarial and administrative. The structural deficit lies higher up the chain—in policy, planning, acquisition, finance, strategy, and cross-departmental coordination. The reform challenge, therefore, is not inventing specialisation from scratch, but expanding and professionalising it.

Half-Hearted Reforms

The creation of the CDS and DMA in December 2019 was the most significant structural reform in India's higher defence management since Independence and was a necessary and welcome step. However, the reform's transformative potential has been constrained by the administrative architecture it left untouched. The CDS is designated as the Principal Military Adviser on tri-service matters, a significant but narrower remit, exercised within policy limits and resource constraints set by a department the CDS does not head. The ToB Rules governing the processing of allocated business reinforce this asymmetry. Interdepartmental matters with a bearing on defence policy continue to be processed through the DoD, while key policy advisory bodies remain chaired by civil service officials and substantive disagreements are often filtered before they reach the political level. While the CDS participates in major bodies such as the Defence Acquisition Council and the Defence Planning Committee, it functions as a member contributing inputs rather than as the authority determining policy or allocating resources.

These dynamics form a pattern that appears repeatedly throughout India's defence reform history. When Service Headquarters were redesignated as "Integrated Headquarters of the MoD" following the 2001 GoM recommendations, the ToB Rules were not amended to give service chiefs a formal role in apex decision-making. Without an alteration to the associated authority, the redesignation amounted to nothing in practice. The 2019 reforms, while much more substantive, have not addressed this asymmetry. The bureaucracy continues to control the most important matters of policy, acquisition and strategy, while the DMA and CDS mechanisms remain enablers at best. The reforms represent a genuine and overdue step forward for an HDO long resistant to change. The concern that remains is whether the pace of reforms can keep up with the expanding remit of warfare.

Institutionalising the Cadre

The proposed defence-management cadre sits firmly within a wider Indian civil services reform conversation.

The Case for a Specialist Defence Cadre

If the core problem is not the existence of civilian control but its institutionalisation, then strengthening the civilian side of the HDO is essential. Management of defence is one such government function that requires specialised and dedicated professional tenures, given the emerging character of war and the evolving geopolitical landscape. Force planning, weapons technology, and crisis decision-making cannot be treated as just another posting in a generalist career.

As the Parliamentary Standing Committee on Defence has noted, the size of India's defence apparatus and budget demands that decision-making structures be upgraded and strengthened, so that the decentralised authority can deliver greater speed, efficiency, and accountability rather than merely avoiding delays.

Proposed Structure

The proposed defence-management cadre could be structured in one of two ways. In its most ambitious form, it could be created as a new All-India Service under Article 312 of the Constitution. A more incremental and administratively feasible route, however, would be to begin by creating it as a specialised Group A civil service, within the existing Union service architecture. Since the GoI already maintains a range of specialised Group A services and an existing AFHQ civil-service nucleus in the defence establishment, the proposed cadre does not require a separate entry procedure.

Upon selection into the cadre, candidates will be exposed to subjects such as acquisition law, strategic studies, technology assessment, and defence economics, in addition to regular IAS training. Through prolonged exposure, these specialists will gain first-hand experience in military operations, defence policy, and

perspective planning. Consequently, when they eventually occupy key positions, their specialist training and institutional depth can translate into better-informed decisions. Further, tenure experience will help them better understand the operator's language, enhancing communication between uniformed officers posted at MoD and their civilian counterparts. This, in turn, is likely to result in a better-informed and enmeshed network of politicians, bureaucrats, and soldiers, which is the essence of effective CMR.

The posting tenures of defence-management cadre must be within defence-related verticals, such as DoD, DMA, integrated headquarters, and national security institutions, including operational Wings, Commands, Academies, National Defence College, Staff colleges (DSSC and MILIT), and War colleges (CAW, AWC, NWC, CDM). These responsibilities may begin with undersecretary-level civil administration duties before they move up the chain, occupying suitable portfolios.

This structure addresses two anxieties at once: that specialisation will be professionally unrewarding, and that the cadre will be too narrow to attract high-calibre entrants. One must expect these anxieties in a system that has consistently rewarded generalist services with flexible deployment across departments, seniority-based promotions, and rotational breadth. Moreover, to minimise friction with the IAS, cadre reviews must identify and reserve for specialist officers positions that mandate specialist defence expertise while keeping several core secretariat functions open to generalists, such as general administration, parliamentary work, and broad coordination. This ensures that key defence posts are no longer treated as interchangeable with unrelated domains.

The cadre design should consciously provide space for lateral absorption. Prior experience in defence with proven capabilities, such as DRDO, PSUs, and the armed forces, must be leveraged through possible lateral entry into mid-career earmarked posts. At the same time, there should be equal opportunity for defence-cadre officers to be deputed to important government departments such as the National Security Council Secretariat (NSCS) and other ministries, where their expertise in defence can be gainfully utilised. This will broaden the national security talent pool and avoid creating silos.

Expected Outcomes

Security Guidance and Strategic Planning: In the current system, civilian officials largely play gatekeeping roles instead of actively contributing to policymaking or capability-building, even in critical areas such as defence planning, weapons acquisition, and the nuclear domain. A specialist cadre can break the pattern wherein strategic assessments are produced exclusively within the military, without informed civilian input or filtered through officials lacking the domain knowledge to evaluate them. The presence

of defence-trained civilians in key policy and planning posts will increase the number of mixed civilian–military drafting teams for major strategy documents. This will lead to clearer, earlier integration of military advice into instruments such as the Defence Planning Committee and long-term plans, rather than consultation at the tail-end of the file.

Coordination: The GoM report has highlighted the lack of coordination among the departments in the MoD. A defence cadre will allow key cross-cutting areas to be staffed by officers who can comprehend operations, finance, and production, and whose tenures are long enough to see proposals through from conception to sanction, reducing the back-and-forth that currently delays decisions. Expert officials who understand both operational requirements and administrative constraints are the only durable solution. Moreover, officials with longer tenures can build institutional memory in a way that rotating generalists cannot.

Civilian–Military Expertise and Continuity: The Parliamentary Standing Committee on Defence explicitly recommended the appointment of "Armed Forces personnel of requisite expertise at the level of Joint Secretary (JS) and/or Additional Secretary (AS) so that the Armed Forces Headquarters are intrinsically involved in national security management and apex decision-making processes." Subsequent reforms have partially responded to this concern by establishing three Joint Secretary-level and one Additional Secretary-level uniformed posts in the DMA. However, these posts sit within the DMA rather than the wider MoD secretariat. Within the DoD, military officers on deputation typically hold mid-level positions. These are lower positions than the JS and AS levels envisaged by the Committee. A specialist cadre can institutionalise cross-domain expertise on the civilian side, ensuring that key policy, planning, and finance posts are held by officials whose careers have been deliberately structured around defence. Over time, this should result in a much higher proportion of JS/AS-level incumbents with deep cumulative defence experience, and a more balanced dialogue between civilian and military advisers at the apex level.

Professionalism and Training: An analysis of the Indian civil services points to several systemic challenges: the tendency to favour generalists, limited lateral entry, weak induction, and in-service training. A dedicated defence cadre can improve the professional output of civilian officials in the MoD. Creating a structured training architecture, setting clear domain-competence expectations, and linking career progression more closely to demonstrated expertise in defence management will gradually replace the current system of ad hoc learning with a more disciplined institutional culture of civilian professionalism in national security administration. To ensure that the "Pleasure of the President" (under Article

310) is exercised based on the actual delivery of national security capability, the cadre should also adopt modern digital governance tools, such as the SPARROW framework for 360-degree performance appraisals.

Capability Delivery and Fiscal Performance: A report by the Comptroller and Auditor General (CAG) of India found that in 72 percent of the contracts examined, items were not delivered within the stipulated timelines under emergency procurement, despite waivers being specifically granted post-Galwan 2020. In a compliance audit, the CAG noted that there was an additional expenditure of INR 227 crore on aeroengine procurement due to the Indian Air Force's failure to project long-term requirements in time. The root cause, consistently identified across official assessments since 2001, is the combination of short civil servant tenures and the absence of specialist acquisition knowledge. France offers a useful comparison in this context: its dedicated armament engineering corps, whose programme managers bring 15 to 20 years of domain experience to a single assignment, recorded an average cost overrun of just 4.5 percent across 48 major contracts between 1994 and 2005. While a mature defence cadre may not eliminate all delays or overruns, it will lead to fewer emergency contracts breaching timelines and fewer "avoidable extra expenditure"—gradually facilitating more predictable cost and schedule performance in major programmes.

The Second Administrative Reforms Commission (2nd ARC) recommends a shift towards a function-based framework. The cadre structure proposed here adds legislative weight to the framework by aligning it with broader national administrative trends.

Comparative Practices

India is not the first democracy to confront the problem of weak civilian expertise in defence. Across countries, policymakers have invested continuously in the civilian side of their defence structures to balance between civilian control and military effectiveness. France addressed similar challenges in the early 1960s by creating the Direction générale de l'armement (Directorate General of Armament), staffed by a corps of ingénieurs de l'armement (armament engineers) drawn from the Grandes Écoles (Elite Schools). In the United States, the Defence Acquisition University (DAU) and a professional acquisition workforce were established under the Defence Acquisition Workforce Improvement Act (DAWIA) of 1990. In the United Kingdom, the 2011 Levene reforms restructured the country's Ministry of Defence and strengthened the Defence Equipment and Support (DE&S) organisation.

These cases point to specialist civilian capacity as a critical capability for effective defence management compared to generalist administration. The idea is not to mimic their institutions but to acknowledge the institutional effectiveness of specialised defence-domain expertise.

Roadmap for Reform

In a large, democratic country like India, plans must consider institutional realities to be sustainable. The path forward should therefore be gradual, incremental, and sequential. A realistic roadmap for success includes short-, medium-, and long-term phases.

Short Term (0–2 years): The first requirement is a clear political direction. Political leadership must state unambiguously that higher defence reform will address the HDO as a whole and not be confined to the armed forces. Under the ToB Rules, the CCS and the RM already bear responsibility for the proper transaction of business in defence, making political backing a necessary starting point for such a substantial structural reform. Concurrently, the government must commission a time-bound internal review of the MoD's structure and staffing patterns, mapping all mid- and senior-level key planning, finance, and strategy posts and classifying them as essential, desirable, or optional in terms of defence expertise.

A small set of portfolios should be ring-fenced, with longer tenures and specialised training introduced immediately as a pilot project before a formal cadre is created. Tangible outcomes expected within this period include greater continuity in key posts and improved civil-military consultation on specific subjects. In practice, HDO reforms are unlikely to precede the full operationalisation of theatre commands. Thus, the roadmap proposed here assumes that these changes to the civilian side of the ministry would proceed in parallel with the ongoing military reorganisation, and would ultimately depend on the political appetite for reform. The bottom line is that when large reforms are taking place, they must be complete and not piecemeal.

Medium Term (3–5 years): The medium-term priority is to establish the defence management cadre by staffing it at scale against clearly identified portfolios, defining cadre norms and culture, and setting transparent career progression pathways. As the specialist pool of officers grows and occupies these posts, the government should examine whether the arrangement warrants progression towards a new All-India Service, modelled on the IAS or IPS, through the constitutional mechanism under Article 312. In parallel, targeted amendments to the AoB and ToB Rules should be rolled out to begin aligning decision-making channels with the emerging cadre architecture and the CDS system, in a manner consistent with the intent of the KRC and GoM recommendations. Tangible outcomes during this phase include the production of strategic policy documents, long-term capability roadmaps, and measurable reductions in chronic delays and associated cost overruns in major defence programmes.

Long-Term (6–10 years): By this stage, the reform should have moved from experimental intervention to institutional practice, resilient to political and bureaucratic

turnover. Posts identified as requiring defence expertise should, as a matter of course, be occupied by defence-cadre officers, or lateral entrants with comparable experience, and JS/AS-level appointments in defence policy, planning, acquisitions, and finance should predominantly draw on officials with substantial cumulative exposure to the said domain. Subject to demonstrated performance and political consensus, far-reaching measures including full recourse via Article 312 route for a new All-India Service and formal codification of AoB and ToB Rules can then be considered as consolidation rather than initiation of reform. The broader impact should be visible not only in staffing and process metrics but also in external evaluation that should record a systematic reduction in chronic delays and avoidable extra expenditure, and more credible formulation of and delivery of defence programmes.

Conclusion

India's higher defence management requires not only better military advice but also an MoD whose civilian machinery possesses the domain expertise to exercise that advice intelligently. At present, the civilian side of the MoD remains structurally non-specialised and continues to exercise authority without a corresponding institutional base for the requisite knowledge. The result is a persistent structural mismatch between responsibility and expertise, undermining the defence decision-making machinery, which successive reforms focused on military structures alone have failed to resolve.

The defence cadre proposed in this brief offers a practical, administratively feasible way to correct this balance. By creating a pool of professionals whose careers are deliberately built around defence administration, policy, and strategy, it addresses three recurrent deficits: inadequate domain knowledge, limited continuity, and weak integration between military expertise and civilian decision-making.

Over time, such a cadre can ensure that civilian control functions as genuine integrator rather than a procedural bottleneck, and that higher defence reform is understood as a ministerial project as much as a military one. Only when civilian structures professionalised alongside military ones will India's model of civilian control fulfil both of its democratic mandates: to keep the armed forces firmly under constitutional authority, and to provide effective stewardship of national defence.

***

Space

SUPARCO Gearing up Strategic Role Against India

Prof (Dr) DK Pandey | 30 July 2025

Source: CAPSS | https://capssindia.org/suparco-gearing-up-strategic-role-against-india/

Image Source: AI Creation by Author

Introduction

"The Space & Upper Atmosphere Research Commission" (SUPARCO) is the national space agency of Pakistan. It was formed in 1961 as a research committee, under the leadership of two Nobel laureates, Abdus Salam and Ishrat Usmani. It was promoted to a federal independent commission in 1981. SUPARCO is based in Karachi. It is responsible for running the National Space Program, handling Pakistan's space activities under the National Command Authority (NCA), and managing its satellite communications and atmospheric research.

Significance of SUPARCO for Pakistan

SUPARCO plays a vital role for Pakistan as it contributes to the social, economic, scientific, and strategic development of Pakistan. In view of its strategic objectives, it is important to understand its functions, advantages, and challenges. SUPARCO operates Earth observation and remote sensing satellites, which include the "Pakistan Remote Sensing System (PRSS-1)," and the domestically developed "Pakistan Technology Evaluation Satellite (PakTES-1A)." These satellites assist in precision agriculture, monitor glacial melt, aid in managing interprovincial water disputes, and support disaster response efforts related to floods and heavy rainfall. SUPARCO's satellites also facilitate monitoring and assessment of risk-related issues along the China-Pakistan Economic Corridor (CPEC).

SUPARCO oversees the "Space Programme 2040," launched in 2011. NCA approved it to accomplish Pakistan's long-term roadmap for strategic objectives. It was renamed "Space Vision 2047," which aims to launch geostationary and low Earth orbit satellites. The first Pakistani astronaut is scheduled to travel to the Tiangong Space Station on the Shenzhou 24 mission in late 2026. Through an agreement between Pakistan and the China Manned Space Agency (CMSA), Pakistani astronauts are receiving advanced training.

In October 2025, Pakistan launched its first hyperspectral imaging satellite, HS-1, from China. This development is likely to enhance Pakistan's capability

in the monitoring and mapping of the environment and natural resources.

Why SUPARCO is in the News?

After almost 60 years of sluggish progress in the space domain, SUPARCO has launched six satellites in just 16 months. This recent surge is not gradual, but rather abrupt, when compared to the number of satellites launched during the past sixty years since the foundation of SUPARCO.

This is not a future scenario that we are facing but a scenario that has happened before. During Operation Sindoor, Pakistan had tapped into the surveillance void between India and China by accessing the Chinese intelligence reports related to Indian deployments. This would have otherwise remained unknown.

The key change, since then, is related to the ownership model. China has already offered surveillance during crisis times to Pakistan in the past. China is now assisting Pakistan in creating its own autonomous surveillance system that can be integrated into the Chinese network and work on its own in real-time. For crisis stability, a distinction is important for sustaining operations. 'Third-party control of surveillance' means that the capability can be pulled at any time; while 'sovereign control of surveillance' means it is under the control of the nation, with the required degree of autonomy.

Strengths and Weaknesses of SUPARCO

SUPARCO began operations with the launch of the Rehbar-I sounding rocket in 1962, making Pakistan the fourth Asian country to go into space. SUPARCO's functioning has suffered for a long time due to a number of institutional challenges. A few of them are.

(a) **Funding Challenges:** SUPARCO is struggling with funding issues, and this has been impacting its operations as well as the progress of various projects. In 2023, for instance, the budget allocation was approximately USD 24 million only for SUPARCO, whereas the budgets for the Indian Space Research Organisation (ISRO) in India, China, and the National Aeronautics and Space Administration (NASA) were approximately more than USD 1.9 billion, USD 20 billion and USD 79 billion, respectively.

(b **Administrative Challenges:** Additionally, SUPARCO has faced many administrative or political hurdles. In the 1980s and even today, political uncertainty, the changing focus of the government and the growing emphasis on missile and nuclear programmes pushed many top scientists from the space programme into missile and nuclear programmes under the control of the Pakistan Atomic Energy Commission (PAEC) and the Khan Research Laboratories (KRL).

(c) **Planning Gaps:** Out of the available

1,800 geostationary orbital slots, 573 slots have been used by satellites, as reported on January 02, 2026. The other slots that feed the main markets have already been filled by countries and private companies for their satellite operations. Satellites are being developed and awaiting deployment for these positions. The failure to meet deadlines and commit adequate funds to build Pakistani satellites caused the loss of critical geostationary orbital slots, like 38°E and 41°E, during the 1990s. Those 38°E and 41°E longitudes are significant as some of the limited fibre-connected regions are the most conflict-prone parts of the world. Countries are given the allotted slots on a 'first come, first served' basis by the International Telecommunication Union (ITU). Once a nation doesn't send a satellite into its assigned slot in the allotted time, it could lose the right to that slot. This drop in position can impact the country's ability to provide sovereign satellite services in its own space and potentially threaten the country's sovereignty and/or position relative to other countries or companies. For Pakistan, this was complicated by the bureaucracy, which made it difficult to progress due to a shortage of financial resources and a major "technological denial" of essential equipment, which severely impacted Pakistan's ability to keep pace with the ITU's tight schedule to deploy.

Disruption of the 38°E longitude would result in the loss of communications for more than 15 countries. A recent series of conflicts in the Middle East has always been accompanied by the employment of cyber-attacks and jamming against these two longitudes. The inability to plan forced Pakistan to look for external assistance.

(d) **Operational Gaps:** The second experimental satellite (Badr-B), which was launched by SUPRACO in the year 2001, was lost in deep space after twenty years, due to communication failures in its operation, despite a five-year designed life. Unlike India, Pakistan does not have any indigenous satellite launch vehicles (SLVs). As a result, it has to rely heavily on other countries, particularly China, for the launching of its satellites.

The Pakistan Space Programme is in dire need to fill these gaps in its operations since it does not have plans for the procurement of corresponding resources and limited know-how.

Implications for Indian Strategic Objectives

The recent expansion of SUPARCO's capabilities, with the support and assistance of China, has significant implications for Indian defence and space strategies, thereby raising strategic importance.

In the military standoff between India and Pakistan, in May 2025 Pakistani forces tried to tailor military operations in real time with the help of inputs from Chinese satellites. But this could not degrade Indian operations. Now Pakistan is trying to bridge

the capacity gaps. Pakistan has fused its satellite intelligence capabilities with Link-17 and other terrestrial communication technologies. Relevant slots are critical for national telecommunications, television broadcasting and crucial military communications for a nation like Pakistan. This may not constrain Pakistan's capabilities in the long run, but warns India to take necessary steps to manage the ill effects of such developments.

The development of Pakistan's space-based capabilities will provide Pakistan more bandwidth to counter Indian military capabilities. Pakistan is trying to develop a "full-spectrum" deterrent approach. China's excellence in space technology and the BeiDou satellite navigation system have improved the high precision of targeting weapons systems, such as Shaheen-III and Babur cruise missiles. China is actively cooperating with SUPARCO, including help for the launch of Pakistan's HS-1 Satellite and astronaut training. From a strategic perspective, the alliance also creates further challenges for India in space and the cyber sphere.

Conclusion

The satellite constellation of Pakistan is relatively small and has both civilian and military applications. SUPRACO is making efforts to enhance space-based capabilities with Chinese launch facilities, design help and real-time data sharing in times of crisis. Operation Sindoor was very much supported by real-time satellite support. Before the next battle, India's challenge is not to catch up with Pakistan's satellite program, but to make its intelligence, surveillance and reconnaissance capabilities state-of-the-art, faster and more resilient. India is on the edge of a turning point. Space continues to be militarised, and massive investments are being made in their offensive and counter-space capabilities.

***

Securing the Cosmic Coastline: Tactically Responsive Space and the IAF in India's Second Space Age

Ms Shrawani Shagun | 24 July 2026

Source: CAPSS | https://capssindia.org/securing-the-cosmic-coastline-tactically-responsive-space-and-the-iaf-in-indias-second-space-age/

Skyroot's Vikram-1 on the Launch Pad at SDSC SHAR, Image Source ISRO

'In future conflicts, the decisive question will not be who launches first, but who can relaunch fastest.'

As modern warfare transitions towards Multi-Domain Operations (MDO), the

foundation of military readiness is dictated by sovereign control over the 'aerospace continuum'. On July 18, 2026, the successful launch of Skyroot Aerospace's Vikram-1 is another feather in India's orbital access. This is a welcome addition to the nation's military architecture. This issue brief argues that the Indian Air Force (IAF) and Defence Space Agency (DSA) must leverage this private sector boom to pioneer an Indian 'Tactically Responsive Space' (TacRS) doctrine. To clarify the adoption path, India must first overcome the bureaucratic friction of the 'absent dialogue,' then establish a private wartime reconstitution reserve, and finally build the rapid-launch resilience required to secure its 'unblinking eye' and dictate the Observe-Orient-Decide-Act (OODA) loop in the next conflict.

The Cosmic Coastline and the July 18 Paradigm Shift

Space is no longer a benign scientific sanctuary; it is a highly contested military domain. Space technology is fundamentally characterised by its military-industrial genesis. Bowen challenges the cliché of space as the 'ultimate high ground'. He argues instead that Earth's orbit must be understood as a vulnerable 'cosmic coastline' that provides vital logistical and intelligence support to terrestrial forces. On the morning of July 18, 2026, India's ability to defend this cosmic coastline strengthened. A four-stage, carbon-composite rocket built by a Hyderabad startup, Skyroot Aerospace, lifted off from Sriharikota and successfully reached a 450-kilometre orbit. While headlines understandably framed Vikram-1 as a commercial milestone for India's unicorn space economy, its true significance is military. A state that can place payloads into orbit through multiple independent domestic providers possesses an operational resilience that a state relying on a single, congested national agency lacks. The Doctrine of the Indian Air Force formally recognises the seamless nature of the 'aerospace continuum.' Within this continuum, Vikram-1 represents a massive leap in national capacity; India must use it to reconstitute a constrained orbital capability, whether reconnaissance, communications, or navigation, on a timeline that matters to a tactical commander rather than to a five-year peacetime procurement cycle.

Operation Sindoor and the 'Unblinking Eye'

Modern military operations are no longer merely enabled by space; they are absolutely dependent upon it. In the mature 'precision-warfare regime,' military dominance relies on a 'reconnaissance-strike complex.' Because space-based Intelligence, Surveillance, and Reconnaissance (ISR) platforms act as the 'unblinking eye' of this complex, adversaries have a massive operational incentive to blind them early in a conflict. India witnessed this absolute dependence first-hand during Operation Sindoor in May 2025, where near-real-time satellite

imagery was central to identifying and striking targets deep inside Pakistani territory. Because of this reliance, India is accelerating the deployment of its constellation of roughly 50 surveillance satellites, with completion by 2029. This expansion incidentally coincides with China's heavy investment in a broad spectrum of counter-space capabilities. As the IAF seeks to compress the OODA loop, the strategic question is no longer just 'how do we protect our satellites?' but 'how quickly can we replace the ones we lose?' If a cyber-attack or kinetic strike blinds the IAF's 'unblinking eye,' India's reconnaissance-strike complex collapses. Therefore, an agile, distributed launch capability is not just an industrial asset; it is a direct component of India's combat power.

Tactically Responsive Space (TacRS) vs The 'Absent Dialogue'

To address this vulnerability, the United States Space Force has spent the last five years pioneering Tactically Responsive Space (TacRS). Its VICTUS NOX demonstration answered a single critical question: if a satellite is destroyed mid-conflict, can a replacement be orbited within days rather than months? During VICTUS NOX, a satellite was readied within 24 hours of notice and was operational within 37 hours of liftoff.

India took a first step in this direction when the Defence Minister released the Joint Military Space Doctrine (JP 2.07) on 16 September 2025, formally recognising space as a warfighting domain alongside land, sea, air, cyber, and the electromagnetic spectrum. That doctrine, however, addresses space-centric warfare and asset protection at a broad, tri-service level; it does not yet specify a tasking chain, contractual mechanism, or authorisation pathway for surging private launch capacity in a crisis. India therefore does not yet have an equivalent to TacRS itself, but it now has the technical foundation for one.

Skyroot has stated that Vikram-1 is designed to be assembled and launched from any compatible site within 24 hours, a specification that could support a military responsive-launch requirement if adopted through the appropriate institutional and operational pathway. However, translating this civilian capability into a military reconstitution reserve requires overcoming severe bureaucratic friction. A structural fracture in Indian civil-military relations exists where tight bureaucratic control frequently isolates operational military expertise from national planning.

Historically, the Ministry of Defence's reliance on defence public-sector monopolies has led to delayed, suboptimal acquisitions. It may be argued that the Indian Space Research Organisation (ISRO) already possesses decades of reliable launch experience. But it is important to understand that no single state agency, crowded with its own scientific and commercial missions, should be asked to

double as India's sole wartime reconstitution reserve. Integrating private players like Skyroot and Agnikul Cosmos generates 'surge capacity,' distributed parallel production, and vital systemic redundancy. If one facility is kinetically targeted or compromised, multiple independent launch pathways ensure India's access to the aerospace continuum is not severed by a single point of failure.

Bridging the Continuum: An Indian 'VICTUS NOX'

To transform private launch capabilities into a strategic force multiplier across all operational domains, the IAF and DSA must pursue integration at three distinct levels:

1. **Institutional Integration:** The DSA, IN-SPACe, and ISRO must establish a clearly defined, pre-authorised tasking chain that includes private launch providers as named parties. This requires IN-SPACe's regulatory mandate to extend beyond peacetime commercial licensing to include fast-tracking emergency wartime authorisations.

2. **Industrial Integration:** The Ministry of Defence must overcome its legacy procurement models by establishing 'standing framework contracts' negotiated in advance with qualified private providers. These cannot be bespoke agreements negotiated after a crisis breaks out. They must include indemnification for the wartime loss of civilian vehicles or personnel, priority-of-service clauses to pre-empt commercial payloads, and the creation of jointly held strategic reserves of propellant and long-lead avionics for India.

3. **Operational Integration:** Responsive launch must be exercised, not merely legislated. The Indian Armed Forces must execute a dedicated tactically responsive space demonstration—an indigenous VICTUS NOX equivalent. By pairing a tactical military satellite with a private launcher on a compressed, previously undisclosed timeline, India can convert a latent commercial capacity into a demonstrated, hard-power capability.

Conclusion

Strategy is the indispensable bridge connecting tactical military tools to ultimate political purposes. A privately built rocket or an advanced satellite bus has no inherent meaning beyond the strategy that directs it. Equally, the demonstration of space capability is a potent diplomatic weapon. States utilise 'rhetorical coercion' and legitimation strategies to achieve narrative dominance. By proactively conducting an Indian responsive-launch drill, the military does for its launch base what Mission Shakti did for its anti-satellite capability: it establishes an undeniable, visible deterrent. Demonstrating this capability publicly frames India as a rule-bound, resilient 'Net Security Provider' in the Indo-Pacific, paralysing adversaries with steep hypocrisy costs if they attempt to disrupt India's defensive aerospace architecture.

The true measure of space power is no longer the ability to reach orbit once, but the ability to sustain military effectiveness in orbit when that capability is under fire. The July 18 launch of Vikram-1 proves India has the technology. By urgently constructing the institutional strategy bridge to harness it, the Indian Armed Forces can secure the cosmic coastline and guarantee decision superiority in tomorrow's conflicts.

***

Two Theories Worth a Cyber Commander's Time

24 July 2026

Source: Arunninghacker | https://arunninghacker.substack.com/p/two-theories-worth-a-cyber-commanders?r=ypuvf&utm_campaign=post&utm_medium=web&triedRedirect=true

Roughly an hour before Russian armoured columns crossed the border on February 24, 2022, an attacker reached into the ground network of a satellite operator and pushed destructive code to tens of thousands of modems across Ukraine and Europe. The Viasat operation knocked out part of the Ukrainian military's satellite communications at the precise moment of invasion. For years afterward it was cited as proof that this would be the first true cyber war.

It was not. I spent that spring, and the years since, on the Ukrainian side of the fight, inside the state cyber defence effort. The striking thing about Russia's cyber campaign was not how unimpressive it turned out to be. It was how badly it matched the war Russia was trying to win. That mismatch is not a curiosity. It is the most useful lesson the war offers anyone who plans, builds, or runs cyber capability for a state.

My argument is simple. Cyber strategy needs theory, not only doctrine and a firehose of threat reports. Two theories are now available for practitioners to use in earnest. And although their authors disagree, commanders should treat the two as complementary rather than choose a camp. One explains why cyberspace rewards continuous competition. The other explains what makes an actor good or bad at it. Between them, they explain what I watched happen to Russia's cyber effort, and what kept Ukraine in the fight.

Why Theory at all

Practitioners are right to be wary of theory. Bad theory is worse than none, and cyberspace moves faster than any literature review. But the instinct to run on common sense alone is a trap, because common sense smuggles in assumptions from the wrong domains. It tells us that cyber operations are "attacks" that ought to be deterred, that a major intrusion is by definition a strategic event, and that escalation is the main risk to manage. Those reflexes come from conventional and nuclear strategy, and in cyberspace they have produced bad predictions for more than a decade.

Good theory tells you when the frame itself is wrong. That is what these two offer. Cyber Persistence Theory sets out to explain state behaviour that deterrence and escalation cannot. Jon Lindsay, arriving from a different direction, argues that cybersecurity is better understood "as an evolution in intelligence affairs than as a revolution in military affairs." Both trade inherited intuition for a frame that fits what actually happens.

Persistence, in Plain Language

The older and more institutionally embedded of the two is Cyber Persistence Theory, developed by Michael Fischerkeller, Emily Goldman, and Richard Harknett. Its core claim is structural. Because everything is interconnected, even in peacetime states are in constant contact with one another's sources of power in a way the conventional and nuclear domains never allowed. Cyberspace, in their phrase, is "macro-resilient (and thus stable) and micro-vulnerable (and thus inherently exploitable)." The system as a whole endures while individual networks stay exploitable, so strategic effect comes not from a single decisive blow than from advantage accumulated over time.

Put those together and the conclusion follows. If states are always in contact, and if the medium rewards patient accumulation rather than decisive battle, then the rational posture is persistence: continuous activity to seize and hold the initiative in setting the terms of security in one's own favour. What emerges from millions of such interactions is what the authors call agreed competition, a tacitly bounded space below the level of armed attack. Nobody negotiated it. It formed out of practice. The uncomfortable consequence for practitioners is that constant competition below the threshold of war is not an anomaly to be deterred away. It is the normal condition.

This caught on because it described what operators were already seeing. It shaped the American turn to "defend forward" and runs through the persistence logic of the US National Cybersecurity Strategy. It traveled, too. The United Kingdom's National Cyber Force describes its own work in strikingly similar terms in Responsible Cyber Power in Practice, adapted to British law and accountability. When two governments independently arrive at the same operational approach, that is about as much as a structural theory can hope to demonstrate.

The Part war Taught me

The same authors are now extending the theory from single operations to whole campaigns, and from peacetime into crisis and war. Their sharper new claim is the one that matters most to me: a cyber campaign is not free-floating. It exists to serve a specific military operational scheme, and misalignment between the two is a primary way the cyber side of a war effort fails. Borrowing from John Mearsheimer and David Galula, they sort military approaches

into four types, attrition, limited aims, blitzkrieg, and insurgency, and argue that each demands a different cyber logic. The cyber support that suits a lightning offensive is not the cyber support that suits an attrition grind.

Their worked example is the war I lived through. In their 2026 analysis, they read Russia's February 2022 invasion as a limited-aims scheme: achieve surprise, envelop Kyiv, decapitate the leadership, and install a friendly government inside a window short enough that the West would have to accept the result instead of restarting hostilities. When surprise failed, the war collapsed into attrition, and attrition is what it has been since. Yet Russia's cyber organisations never ran the campaign that a limited-aims scheme required. Planning appears to have sat largely with the Federal Security Service, the agency that had run the Donbas insurgency since 2014. So the cyber effort aligned with an insurgency: destructive strikes on government and infrastructure, attempts to delegitimise the state, ambient harassment that never changed register when the tanks moved. The Viasat strike on communications is the one operation the authors tie cleanly to the limited-aims scheme. The rest was aimed at a different war.

On defence, alignment is exactly what we tried to practice, and where the theory stops being academic. When you are helping defend a state under invasion, you are not counting the enemy's intrusions. You are asking which of them actually threatens the scheme your own forces are executing, and spending your scarce people there. The theory's authors themselves conclude that Ukraine's efforts to seize the cyber initiative "helped stave off early defeat" in the opening phase of the invasion. The asymmetry that produced that outcome was not in tools. Russia had capable operators and burned through new families of wiper malware at a startling pace. The asymmetry was in alignment.

Performance, in Plain Language

The second theory explains the other half. In Age of Deception, Lindsay argues that cyber operations are best understood not as a new kind of warfare but as the latest form of a very old activity, the organised use of deception by states. Most cyber operations are about access, manipulation, and counter-manipulation rather than destruction, which is why they sit so naturally inside the history of intelligence. It is the same "intelligence contest" framing that has been argued for years.

His positive theory rests on two variables: how vulnerable the target's institutions are, and how well organised and disciplined the attacker is. The popular claim that cyberspace simply makes offence easy is only half right. Skilled attackers succeed against hard targets, and clumsy ones fail against soft ones. If the attacker's skill is half the story, defenders can't spend everything on hardening systems. The frame also unifies espionage, sabotage, and subversion as one activity in different clothes, and it predicts that

the most consequential operations will rarely look decisive. They accumulate quietly, as access and position. That is precisely what we kept seeing.

Where they Meet, and where they Part

The two theories entered the field through different doors, and they share more than their partisans admit. Both reject the "cyber war" framing. Both treat persistent, below-threshold activity as the normal state of affairs rather than a failure of deterrence. Neither asks the practitioner to memorise the latest catalog of techniques; both ask what kind of strategic environment those techniques are deployed inside. And neither accepts "what damage did we do" as the measure of success.

They differ in where they start. Persistence theory begins with the structure of the medium and derives behaviour from it. Intelligence-performance theory begins with the history of secret statecraft and asks how digital tools change its performance. The authors genuinely disagree about which frame is primary, and that disagreement is worth knowing. But for a practitioner the division of labor is clean. Reach for cyber persistence when you need to explain the environment: why competitors are permanently inside your networks, why deterrence is the wrong concept, and why a cyber campaign has to be aligned to the war your conventional forces are actually fighting. Reach for intelligence performance when you need to plan the effort, assess chances of success, and explain a result: why one intrusion succeeded and another failed, and why tradecraft and operational security matter as much as tools and exploits.

What this means for Building a Cyber Force

A few consequences follow for anyone building or running a state cyber capability, and they cut against how most such organisations are still budgeted and judged.

Design for continuity rather than for spikes. The real unit of work is the campaign, not the incident or operation, and a force resourced only to surge around crises will be under-built for the constant contact that is the actual daily condition. That is even more true across the transitions into and out of war, which is where an unprepared force tends to break.

Invest in people and tradecraft, not just tools. If proficiency is half of performance, then the loud, brittle operation is a symptom of an organisation that bought capabilities without building competence. Ukraine's defence held not because our tooling was superior but because our operators, and our partners, were disciplined and kept learning under fire.

Measure the right thing. Neither theory supports damage as the headline metric. Persistence theory points you toward initiative: are you setting conditions, or reacting to someone who is? Intelligence

performance points you toward access: can you gain and keep it while denying the same to your adversary? The campaigning extension adds a third question, the one Russia failed and Ukraine, under fire, mostly answered well. Is your cyber campaign aligned to the operational scheme your conventional forces are executing, or are you fighting the war you trained for while the real war runs differently?

Finally, stop pretending the line between intelligence and military cyber organisations is clean. The joint design of the United Kingdom's National Cyber Force, and the shared leadership of the American cyber and signals-intelligence commands, are not accidents. If cyber operations are continuous campaigns inside an environment saturated with intelligence work, then organisations built around tidy peacetime-and-wartime or intelligence-and-operations boundaries will struggle precisely when it counts.

The war we are Actually Fighting

To me these are not the questions of a conference panel. They are the questions Ukrainian and allied cyber commanders have been living since February 24, 2022, in language a little less academic and a good deal more urgent. Plan for persistence. Build for performance. Align the cyber campaign to the war you are actually fighting, not the one you rehearsed. And stop scoring cyber operations as though they were air strikes.

Space

SpaceX Wins $1.6 Billion Order to Launch Pentagon's New Space-Based Eyes for Tracking Airborne Threats

Aditi | 30 July 2026

Source: Financial express | https://www.financialexpress.com/world-news/us-news/spacex-wins-1-6-billion-order-to-launch-pentagons-new-space-based-eyes-for-tracking-airborne-threats/4306298/

SpaceX Wins $1.6 Billion US Space Force Contract for 18 Falcon 9 Missions

SpaceX has won a $1.6 billion contract from the US Space Force to carry out 18 Falcon 9 rocket launches that will put military satellites into orbit. The satellites will help the US military detect and track airborne threats from space.

The US Space Force announced the deal on Wednesday. According to Reuters, all 18 missions will launch from Vandenberg Space Force Base in California and are expected to be completed by the end of 2027.

Biggest batch of missions under the program

The 18 launches have been divided into two task orders under the National Security Space Launch (NSSL) Phase 3 Lane 1 program. This is the Space Force's main program for buying launch services from private companies.

Under this system, companies compete for each mission instead of being guaranteed a certain number of launches. SpaceX competes with firms such as United Launch Alliance (ULA), Blue Origin and other approved launch providers for these contracts.

According to SpaceNews, this is the largest publicly announced group of missions awarded under the Phase 3 program so far.

What these satellites are meant to do

The satellites launched under this contract will support the Space Force's Space-Based Sensing and Targeting program.

Their job will be to spot, track and share information about airborne threats much faster than before. The satellites are designed to provide near real-time information, helping the military respond more quickly to potential threats.

Space Systems Command announced on July 29 that it will award two task orders to SpaceX for missions using the company's reusable Falcon 9 rocket. Space Force says the deal moved at record speed

Eric Zarybnisky, a Space Force acquisition official, described it as an "unprecedented two-month acquisition timeline," according to a Space Force news release cited by MarketScreener.

The faster process is seen as an important step for the military, which has spent years trying to speed up how it buys satellites and launch services from private companies.

Government support grows even as SpaceX stock struggles

The new Space Force contract comes at a time when SpaceX is facing pressure in the stock market.

The company, which went public in June, has seen its shares lose about 30% from their debut price and more than 50% from their record high of $225.64.

The stock has remained under pressure as investors worry about the upcoming share lock-up period ending in early August. Once the restriction is lifted, hundreds of millions of additional shares could enter the market, something that often raises concerns about selling pressure.

Despite the stock's recent weakness, the Pentagon has continued to place its

trust in SpaceX. Military contracts are awarded based on factors such as a company's launch capabilities, reliability, pricing and its ability to meet mission deadlines, rather than its share price.

SpaceX continues to stand out because its Falcon 9 rocket has built a long track record of successful missions over more than a decade. It is also the only American rocket with the proven experience needed to support the rapid launch schedule required from Vandenberg Space Force Base.

Part of a much bigger Pentagon plan

This latest contract adds to a series of major Pentagon deals that SpaceX has secured this year.

Reuters reported that SpaceX has now received at least $7 billion in Pentagon contracts in 2026. Much of this work is linked to the Trump administration's Golden Dome missile defence project, a long-term program expected to cost around $185 billion, in which SpaceX plays a major role.

The new contract comes after two other large awards connected to the same sensing and targeting mission.

According to MarketScreener, SpaceX first received a $4.16 billion contract to build a network of satellites that can track moving airborne targets. Just three days later, the company was awarded another $2.29 billion contract to develop communication satellites that will quickly send data between missile-warning sensors and missile interceptors.

Questions over SpaceX's growing role

As SpaceX continues to win more Pentagon contracts, some lawmakers in Washington have raised concerns that the U.S. military could become too dependent on a single company.

In response, Space Force officials have said they want to encourage more competition and help more companies take part in national security space missions.

Rivals are dealing with major setbacks

While SpaceX continues to win new work, two of its biggest competitors are facing technical problems.

United Launch Alliance (ULA), the joint venture between Boeing and Lockheed Martin, is currently dealing with a months-long investigation into a faulty booster separation system on its Vulcan rocket. The rocket has been certified to launch Pentagon satellites, but the investigation has created uncertainty around its operations.

Meanwhile, Blue Origin, the space company founded by Jeff Bezos, is investigating why its New Glenn rocket exploded on the launch pad in May before its fourth flight.

The rocket is also part of the Space Force's launch program, but it is expected to remain grounded until at least the end of the year while the investigation continues.

***

Beyond IAF 114-Rafale Deal, Dassault Plans to Leverage India's Manufacturing Base for Global Rafale Exports

Chandresh | 30 July 2026

Source: Defence.in | https://defence.in/threads/beyond-iaf-114-rafale-deal-dassault-plans-to-leverage-indias-manufacturing-base-for-global-rafale-exports.18386/

India's potential acquisition of 114 Rafale fighter jets under the Multi-Role Fighter Aircraft (MRFA) programme is shaping up to be much more than a standard military purchase.

Recent developments suggest that the production facilities established in India could transform into a secondary global manufacturing hub for Dassault Aviation.

If executed as planned, this industrial base would not only fulfill the Indian Air Force (IAF) requirements but also supply advanced Rafale jets to future international clients across the Middle East, Africa, and Asia.

Such an evolution would mark a historic leap for India's domestic aerospace sector. By becoming an assembly and export powerhouse for one of the most prominent 4.5-generation combat aircraft in the world, India would firmly cement its position in the global defence market.

Currently, Dassault Aviation's primary assembly line in Mérignac, France, is managing an expanding production backlog. The company entered 2026 with an order book of over 220 Rafale jets destined for nations like the United Arab Emirates, Egypt, Indonesia, Greece, and Serbia, alongside its commitments to the French military.

With the massive IAF deal advancing—and potential new orders emerging globally—relying exclusively on the French facility to fulfill all deliveries presents severe industrial bottlenecks. To meet these growing international commitments, expanding manufacturing capacity outside of Europe has become an absolute necessity for Dassault.

The foundation for this shift has already been laid. In June 2025, Dassault Aviation finalised critical production transfer agreements with Tata Advanced Systems Limited (TASL). This partnership is establishing a state-of-the-art facility in Hyderabad to manufacture complete fuselage sections for the fighter jet.

Crucially, these components are not restricted to Indian jets.

Set to roll out its first assemblies by 2028, the Hyderabad plant is integrated directly into Dassault's worldwide supply chain. Rather than operating an isolated facility just for India, Dassault is cultivating a vast industrial ecosystem capable of feeding both domestic and international assembly lines.

The proposed structure of India's 114-aircraft deal reflects this pragmatic approach. According to defence ministry clearances granted earlier in 2026, the initial batch of fighters would be delivered in fly-away condition from France to quickly address the IAF's urgent operational needs. Meanwhile, 94 of the remaining aircraft are planned to be manufactured in India with significant indigenous content.

As local infrastructure matures, Indian factories will gradually take on greater responsibilities—moving from basic assembly to advanced systems integration and complex structural component production. Once the IAF's primary needs are satisfied, this fully matured production pipeline is expected to remain active to cater to future global exports.

Establishing a secondary production hub in India offers numerous strategic benefits. It will significantly boost Dassault's annual output, alleviating pressure on the French supply chain while offering greater flexibility to meet international deadlines.

Furthermore, India's geographic location makes it an ideal bridge between Europe, Southeast Asia, the Middle East, and Africa. Manufacturing jets closer to these critical markets will inevitably lower logistics expenses and streamline long-term maintenance support for regional operators.

This massive undertaking will also galvanise the wider Indian defence industry. Major corporations such as Bharat Electronics Limited (BEL), Bharat Dynamics Limited, L&T, and numerous micro, small, and medium enterprises (MSMEs) have been steadily expanding their footprint in global aerospace manufacturing.

Participating in the Rafale's production cycle will embed these companies deeper into the global value chain. The hands-on expertise gained in precision engineering, advanced composites, and supply-chain management will directly benefit India's own indigenous aviation projects, including the Tejas Mk2 and the Advanced Medium Combat Aircraft (AMCA).

Ultimately, India's transformation into a Rafale export hub rests on the successful finalisation of commercial and governmental agreements. The Indian government issued a formal Letter of Request (LoR) to France in mid-2026, and detailed price negotiations are expected to follow shortly.

Any future exports of Indian-built Rafales will naturally remain subject to French export controls and international

defence trade regulations. However, if these diplomatic and industrial milestones are met, India is well on its way to becoming a central pillar in the global production of cutting-edge combat aircraft.

"To conquer the command of the air means victory; to be beaten in the air means defeat and acceptance of whatever terms the enemy may be pleased to impose."

Giulio Douhet

The Centre for Aerospace Power and Strategic Studies (CAPSS) is an independent, non-profit think tank that undertakes and promotes policy-related research, study and discussion on defence and military issues, trends and developments in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Marshal Nagesh Kapoor, SYSM PVSM, AVSM, VM (Retd).

Centre for Aerospace Power and Strategic Studies
P-284 Arjan Path, Subroto Park, New Delhi - 110010
Tel.: +91 - 11 - 25699131/32 Fax: +91 - 11 - 25682533
Email: capsnetdroff@gmail.com
Website: https://capssindia.org/

Advisor : Air Vice Marshal Prashant Mohan VM (Retd)
Editor, Concept & Content : Ms Gowri R

Composed by Mr Rohit Singh
Tel.: +91 9716511091
Email: rohit_singh.1990@hotmail.com