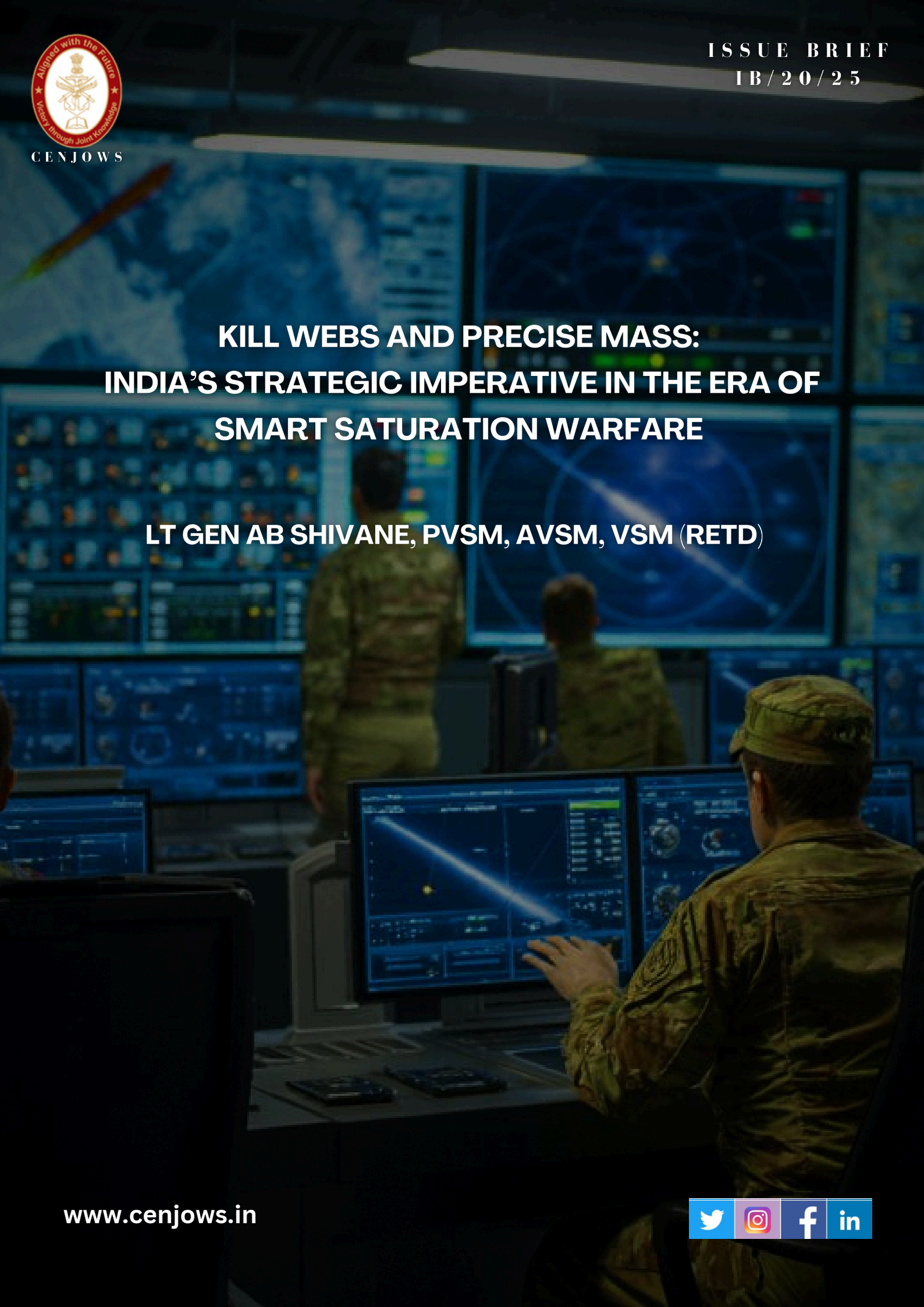
CENJOWS

ISSUE BRIEF
IB/20/25



KILL WEBS AND PRECISE MASS: INDIA'S STRATEGIC IMPERATIVE IN THE ERA OF SMART SATURATION WARFARE

LT GEN AB SHIVANE, PVSM, AVSM, VSM (RETD)

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Kill Webs and Precise Mass: India's Strategic Imperative in the Era of Smart Saturation Warfare

Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd) is the former DG Mechanised Forces and a Strike Corps Commander. Presently, he is the Distinguished Fellow and COAS Chair of Excellence at CLAWS

Introduction: The Emergence of Precise Mass Warfare

The post-Cold War era heralded the dominance of precision-strike warfare enabled by smart bombs, long-range cruise missiles, and highly networked air power. Western doctrines especially favoured the idea that **precision could replace mass**, that fewer, smarter weapons would obviate the need for sheer numerical superiority. But this notion has now collapsed. The wars in Ukraine, Gaza, and Operation Sindoor, as well as China's doctrinal developments, signal a new age where **mass and precision co-exist, magnify each other, and form the foundation of future combat- an era of persistent precision-saturated attacks.**

As highlighted in Horowitz's *Battles of Precise Mass*, warfare has entered a phase where **cheap autonomous weapons, when deployed in large, coordinated volumes, achieve strategic effects once reserved for nuclear or manned airpower**. These systems, guided by artificial intelligence, operate on compressed timelines and often outside the traditional command hierarchy. China's kill web concept is the clearest embodiment of this reality.

A **kill web**, unlike a traditional kill chain, is non-linear and decentralised. This system enables sensors, shooters, and command control centres to communicate in real time laterally and vertically in an interconnected networked environment where real-time, autonomous actions manifest across domains. This results in an overwhelming tempo of operations, difficult to predict and across all domains simultaneously. For India, facing a technologically empowered PLA, the danger of such a kill web being switched on along the LAC, over the Indian Ocean, or even in space isn't just a theory anymore; it's a ground reality.

India's military thought must reclaim the principle of mass, not as an outdated tradition but as a timeless truth reframed for a technological age. Mass was never just about numbers. In Indian strategic culture from Kautilya to Shivaji, it was about applying force with guile, purpose, and economy. Today, mass must be intelligent, multidomain and precise, rooted in strategic autonomy and operational pragmatism.

Threat Assessment: China's Kill Web Capability

1. Network Integration

China's military modernisation is geared toward achieving **sensor-to-shooter integration across platforms and domains**. The PLA has deployed an extensive constellation of satellites (Yaogan, Gaofen), airborne early warning systems (KJ-series), and over-the-horizon radar systems along its coastline. All sensors are fused with strike elements like the rocket force, maritime missile platforms and ground-based missile launchers for a real-time response mechanism.

China's **Beidou satellite navigation system**, combined with quantum communication pilots and state-backed cloud networks, ensures secure, jam-resistant data transmission, allowing China

to effectively **compress its OODA loop** (Observe–Orient–Decide–Act) and execute precision strikes before adversaries can respond.

2. Autonomous Targeting and Decision Superiority

Platforms powered by AI, like loitering munitions and swarms, are becoming increasingly capable of identifying and engaging targets autonomously. There is a paradigm shift from systems that require a human to be actively involved in the targeting process **(human-in-the-loop)**, towards models where humans supervise from the sidelines (**human-on-the-loop**). In these niche technology models, the machines execute based on predefined targeting logic and only seek human input in truly exceptional situations.

This dramatically reduces decision time, forcing adversaries, including India, into **compressed windows of response**, where a failure to act within minutes can result in operational paralysis. These capabilities are also being field-tested in grey-zone engagements—such as in Taiwan's air identification zones and the South China Sea—where simulated saturation attacks are becoming routine.

3. Multi-Domain Saturation Capability

China's Rocket Force is no longer simply a ballistic missile branch; it is now an integrated, domain-spanning strategic arm. A typical PLA saturation strike would involve:

- **Hypersonic Glide Missiles (like DF-17s)** bypassing radar envelopes and independently capable of evasive manoeuvres.
- **AI-armed Drone Swarms and loitering munitions** for saturation attacks, penetrating air defence systems for effective target engagement.
- **Cyberattacks are disabling the communication infrastructure.**
- **ASAT (Anti-Satellite) attacks or jamming attempts** disrupting Indian space-based ISR and navigation.

The goal is not to destroy every asset but to **create operational chaos**, blinding Indian forces, breaking decision coherence.

Vulnerability Matrix: Gaps in India's Current Posture

Despite strides in military modernisation, India remains doctrinally and structurally misaligned to confront precise mass warfare. A breakdown of core vulnerabilities is essential to understand how and where the Indian defence establishment must evolve.

1. Platform-Centric Doctrine

India's current force posture still emphasises traditional high-value platforms, S-400 air defence systems, Rafale fighters, naval destroyers, and static radar infrastructure. While these assets are formidable in conventional contexts, they are poorly suited to survive or adapt under a **kill-web-enabled saturation attack**. A single hypersonic glide vehicle or swarm drone attack can render an airbase inoperable. India's reliance on "silver bullet" platforms exposes it to strategic overmatch when facing adversaries who can **expend and reload faster** with autonomous and cheap assets.

2. Voids in Drone Capabilities

The Indian Armed Forces' current approach to drone capability development reveals structural flaws, an indigenous technology deficit and operational inefficiencies. The present system of assigning platform-based responsibilities to multiple directorates lacks cohesion and a long-term perspective. There is a lack of a centralised Drone Capability Task Force, which must see the capability holistically - technology integration, institutionalised long-term road map, doctrine construct, training, setting up drone hubs and structural changes in legacy organisations for optimal advantage. Further, in an era of 3D printing and precise mass, the need is for a family of drones on a plug-and-play format, versatile and adaptive to multiple missions. The upgrades, MRO and training aggregates must be inbuilt.

The legacy procurement cycle does not match the technology cycle as it is plagued by ***bureaucratic lethargy, lack of accountability, and outdated defence reforms that fail to address contemporary threats***. The present procurement is complex, slow, unwieldy, outdated and misguided by a monolithic GSQR, which actually should be one-page guidelines for the

operational requirement. In an era where drone technology is moving at a fast pace, business as usual will not work. We need to optimise what exists and not what does not exist.

Technology mapping and indigenous content audit, including design, raw materials, sub-components, cost structure, and intellectual property ownership by an independent empowered committee, remains a void, particularly in critical components like the flight controller. The presence of Chinese or foreign parts in critical systems makes them vulnerable to electronic interference and manipulation, thereby compromising national security.

There is presently limited capability in autonomous drone swarming for offensive and defensive operations. The need is to develop and procure UCAVs (Unmanned Combat Aerial Vehicles) with precision-guided munitions, AI enablement, and enhance the integration of drones with manned platforms for coordinated strikes.

Finally, secure cyber-proof resilient communication systems are critical for drone effectiveness. They must be immune to RF interference, cyber-attacks, and jamming and possess High-Speed Data Transfer and increased bandwidth.

India must develop a robust indigenous drone industrial ecosystem (both mass production and AI-enabled technology), enhance acquisition and induction, and foster military adaptation through doctrinal review, adaptive training, and collaboration with start-ups*.* Further, the present threat cum capability building model must give way to a more proactive and perspective capability cum opportunity-based model to be ready and relevant for the future. This will empower a pre-emptive and proactive operational military strategy and also help in adding teeth to a redefined deterrence based on denial and domination.

3. Sensor Fragility and ISR Dependency

India's surveillance and reconnaissance infrastructure is vulnerable across three levels:

- **Terrestrial sensors**, such as radar stations in vulnerable border zones.
- **Space-based ISR platforms** are few and lack orbital redundancy, manoeuvrable coverage and short revisit cycles.

- **Data fusion centres**, which are not fully hardened or mobile.

In a saturation scenario, **jamming, spoofing, or kinetic strikes on satellites** (ASAT) would leave Indian forces blind. Without robust **low-earth orbit (LEO) satellite constellations, a launch on demand capability and sensor fusion** from multi-domain sources, India risks losing decision advantage within minutes of an engagement. The present SBS capability remains fragile and non-resilient.

3. Lack of a Multi-Domain Command and Control (MDC2) Architecture

The current model of command approval, especially in scenarios involving kinetic response, is hierarchical and time-consuming. In a battle environment where the PLA may act and adapt within minutes via AI-managed kill webs, India's need for multi-tiered clearance before launch or manoeuvre becomes a **structural liability**.

Moreover, the lack of **an integrated C6ISR (Command, Control, Communications, Computers, Cyber, Cognitive, Intelligence, Information, Surveillance, and Reconnaissance)** across the services and the lack of a cyber-secure multi-domain command and control (MDC2) system accentuate the challenge. Without seamless data sharing and autonomous capability, India's armed services cannot present a joint, real-time, multi-domain operational picture.

In future, decisions will be made at lightning speed, and where human intelligence is augmented by artificial intelligence, where battlefields can span not just land, sea, and air, but also space, cyberspace and even into the cognitive dimension. It's not just any more about high technology platforms, but really about a **whole new way of looking at command and control (C2).** As military operations become more complex and involve human-machine teams, understanding the cognitive load on personnel, ensuring trust in automated systems, and guarding against cognitive manipulation will be critical aspects of any future command system. **MDC2 can greatly improve operational awareness at all levels, shorten the F2T2EA (Find, Fix, Track, Target, Engage, Assess) 'Kill Chain' and increase combat effectiveness**. However, the biggest vulnerability today lies in the present cyber-compromised MDC2 cloud-based structure.

4. Limited Autonomous Arsenal and Swarm Warfare Doctrine

India's drone capability development programs, while progressing, remain fragmented and behind the technology cycle. Platforms like **Tapas-BH** and the **AURA UCAV** programme are still in testing or development stages. There is also a void of a precise mass or a drone-enabled doctrine for War Fighting.

This shortfall not only limits India's **first-strike and counter-strike options** but also denies it the ability to present a credible cost-imposing threat to adversaries. The need is to mass-produce AI drones under a civil-military fusion institutionalised drone ecosystem.

5. Reactive Deterrence Philosophy

India's deterrence strategy is still reactive, based on retribution and response after provocation. However, precise mass warfare favours **offensive, proactive and pre-emptive initiative**; the side that strikes first and fast can render the opponent's response incoherent. Thus, it mandates a deterrence which is based on denial and domination with a pre-emptive and proactive doctrine. Domination and control of the escalation ladder thus need greater clarity with a proactive deterrence construct.

India's military deterrence must evolve to reflect the logic of precise mass. Traditional deterrence relied on visible thresholds. The new deterrence must be about ambiguity, adaptability, and speed. Deterrence by punishment must be backed by the demonstrated ability to respond faster than the adversary can act. ***Deterrence by denial and domination must be achieved through cognitive overmatch and operational unpredictability.***

Operational Precedents: What the World Has Already Shown

Operation Sindoor (2025)

The central innovation of Operation Sindoor was the demonstration of "precise mass", the deployment of swarms of affordable, semi-autonomous systems delivering effects typically reserved for high-end missiles and aircraft. The strategy is simple: overwhelm defences through numbers, coordination, and resilience.

The lessons from Sindoor resonate far beyond the tactical. India now faces a strategic question: Will this success remain episodic or evolve into an enduring advantage? For that to happen, New Delhi must draw not only from its battlefields but also from international experiences. Ukraine's war against Russia has become a grim proving ground for the power of innovation under fire. China's silent preparations for autonomous, networked combat offer another playbook—one of deliberate, long-term integration. India must now walk a line between these two models: one born out of necessity, the other out of strategic foresight.

Israel-Iran Conflict (2025)

Iran's April 2025 missile and drone offensive against Israel was a watershed moment. Hundreds of Shahed-class drones, combined with cruise missiles and cyber jamming, forced Israel to fire over $1 billion worth of interceptors. Despite Iron Dome and David's Sling systems, significant degradation occurred at airbases and energy infrastructure.

Key takeaways for India:

- **Cheap large-scale swarms** can bleed advanced missile defence dry.
- Fixed-site reliance creates predictable target baskets.
- AI-based tracking and tiered deception are key to preventing defensive exhaustion.

Ukraine Conflict (2022–2025)

The ongoing Ukraine war continues to showcase:

- The massive strategic value of commercial drones and uncrewed platforms for saturating attacks.
- The centrality of space-based reconnaissance and its vulnerability to jamming and cyberattacks.
- The critical role of national willpower, but also **adaptability in fusing irregular and formal forces into kill-chain loops**.

Strategic Recommendations: Rebuilding Deterrence and Resilience

To survive and prevail in the age of kill webs and smart saturation, India must reengineer its strategy along five integrated lines of effort:

Adopt a Decentralised Kill Web Doctrine

India must build a **homegrown kill web** with emphasis on decentralisation, redundancy, and adaptability. This includes:

- **Multi-domain Command and Control System.** Cyber-secure, cloud-based, and adaptive MDC2 system that integrates and shares information between all domains, from sensors to trigger pullers and between all component operations centres, is a necessity.
- **Service-level cloud-based integration** across the Army's missile regiments, the Navy's maritime strike wings, and the Air Force's precision strike units and Space operations with cyber resilience is required.
- **Civilian infrastructure integration**, leveraging ISRO, commercial satellite companies, and private defence firms to ensure resilience.

Such a doctrine must be grounded in the idea of **"mission autonomy"**, where tactical nodes can operate independently under predefined strategic directives even if central command is disrupted.

Mass-Autonomy at Scale

India must invest in **high-volume production of low-cost autonomous precision strike weapon systems**. This requires:

- **Plug and play 3D printable Drones and loitering munitions** with modular payloads (PGMs, EW, ISR).
- **Swarm AI** that enables collaborative targeting, distributed navigation, and adaptive strike coordination.
- **Autonomous uncrewed surface and underwater vessels (USVs and UUVs)** for maritime operations are a requirement.

A PPP model must be capable of deploying **thousands of autonomous units annually**, with high export potential to support the ecosystem. These swarms would serve both defensive (air denial) and offensive (deep strike) roles.

Resilient and Deceptive C5I2SR Systems

India's command and control architecture must move from fixed, high-signature nodes to **mobile, hardened, and deceptive systems** that can operate under saturation and cyber-electromagnetic warfare. Key components include:

- **Mobile Command Posts (MCPs):** These must be rapidly deployable, digitally linked, and EMP-shielded. Static HQs are first-wave targets in a kill web scenario.
- **Spectrum-Efficient Communications:** Adoption of laser communications (satcom alternatives), quantum key distribution pilots, and cognitive radio that can detect and avoid jamming.
- **Passive Sensing and Decoys:** Passive radar, IR heat maps, and radar spoofers can confuse adversary kill webs. AI-generated decoys mimicking Indian missile batteries, airfields, and C4I nodes should saturate the EM battlespace.
- **AI-Enhanced Data Fusion Centres:** Human analysts cannot keep up with the data volume in a kill web battle. India must deploy AI-assisted command software capable of triaging inputs, generating course-of-action options, and pushing alerts up the chain in seconds.

Together, these measures can deny China the coherence it seeks in its first wave of kill web-based targeting.

Launch-on-Warning and Pre-emption Cold Strike Doctrine

The doctrine of delayed retaliation is strategically unsuited for machine-speed warfare. India must establish **launch-on-warning protocols** for its conventional precision strike assets and tactical ISR-based retaliation. This should include:

- **Defined Trigger Indicators:** Satellite jamming, kill web activation (e.g., uplink surges, mass UAV launches), or early hypersonic launch signatures can all form pre-emption thresholds.
- **Legal and Political Clarification:** National security policy must clarify that limited pre-emptive strikes on satellite constellations, missile launchers, or drone hubs are within the scope of India's active defence posture.
- **Empowered Decentralised Command:** Commanders in Ladakh, Eastern Sector, Western Sector, or IOR should have pre-delegated, time-bound strike authority under national war directives. This is key to eliminating lag-induced vulnerabilities.

India must also ensure **public communication preparedness**, so pre-emption is not mischaracterised as escalation but seen as **a deterrence-preserving move.**

Space Domain Integration and Protection

No kill web can function without dominance and survivability in space. India's space strategy must rapidly transition from a support role to an integrated, defensive-offensive capability. The need is for a military space orientation (offensive and defensive) by constituting an Integrated Space Command.

a) Satellite Constellation Resilience

- India currently relies on limited GEO and MEO satellites for ISR and communication, which remain both visible and vulnerable.
- ISRO, in partnership with the private sector, must deploy **LEO-based micro-satellite constellations** with overlapping coverage, autonomous manoeuvring, and spectrum agility.
- The need is for a manoeuvrable orbital path and doctored revisit systems, besides augmentation of short-notice launch on demand capability.
- Onboard AI and quantum encryption protocols must protect data integrity under EW or cyberattack.

b) Counter-Space Capabilities

- India must evolve beyond ASAT demonstrations (as with Mission Shakti) and invest in **co-orbital assets** capable of rendezvous and soft-interdiction missions (e.g., jamming, blinding).
- The establishment of a **Joint Space Command** is overdue, with tri-service integration and operational authority in times of contested satellite environments.

c) Space-Based Surveillance (SBS) and Space Situational Awareness (SSA)

- After defence forces realised the need for more precision surveillance during Operation Sindoor, the Union government has ordered the fast-tracking of the launch of 52 dedicated surveillance satellites, enhancing round-the-clock monitoring of the coastline and land borders. SBS-3 aims to cover much larger areas of China and Pakistan, as well as the IOR region, with reduced revisit time and better sub-metric resolution.
- India must fund its own SSA centres, rather than rely on foreign alerts. It must have the capability to track, predict satellite movements, identify dark periods, and adversarial behaviour in space.
- AI can assist in predicting orbital warfare scenarios and suggest evasive manoeuvres or deception via decoy emissions.

d) Kill-Web Redundancy Through Space Assets

- India's kill web must be space-augmented. ISR feeds, encrypted SATCOM, and early warning systems must remain **multi-nodal and survivable** even under space-based attacks.
- Space-based launch detection, relayed via autonomous drones and AI-linked battlefield clouds, must allow **strike-back within minutes**, regardless of ground disruptions.

In this respect, **space is not just the high ground; it is the backbone** of algorithmic deterrence. India must treat it as a contested warfighting domain, not a passive support sphere.

Drone-Enabled Doctrine for Future Warfighting

The drone-enabled doctrine must focus on three lines of effort: Build the Force Capability, Optimise Force Readiness (effectiveness and preparedness), and Integrate Force Design into the structure. The aim must be to achieve operational flexibility, integrating drones across all warfare levels and domains, while balancing autonomous capabilities with human oversight. It must emphasise multi-domain interoperability, scalability for varied environments, and a family-of-platform approach to streamline logistics and mission adaptability. The doctrine also necessitates reorganising forces for lean, smart warfighting without over-matrixing and addressing ethical and legal considerations to align with global norms, ensuring responsible and effective deployment in modern warfare. Jointness to interdependence must drive this joint force capability.

Policy Imperatives: What India Must Do Now

To internalise lessons and operationalise resilience, India must enact the following policies within a strict timeline:

1. Create a Joint Kill-Web Integration Task Force

- Bring together DRDO, ISRO, armed services, academia, and industry.
- Mandate cross-service integration of sensors, autonomous platforms, and data-sharing protocols.

2. Codify a Multi-Domain Cold Strike Doctrine

Multi-Domain Cold Strike Doctrine is **data-driven, precision-led preemption**. Its objective is not territorial occupation but denial, degradation, disruption, and domination across land, air, sea, cyber, and space, aimed at dominating escalation without crossing nuclear thresholds. It proposes the use of long-range precision vectors, cyber, space, electronic warfare, swarms/ drones and cognitive operations in a synchronised, time-compressed C5ISR force application cycle. Cognitive warfare and narrative dominance remain inbuilt.

3. Expand Public-Private R&D for Autonomous Warfare

- Incentivise startups and research labs to develop swarm AI, autonomous drones, and electronic warfare payloads.
- Establish battlefield testing corridors under MOD supervision.

4. Establish Functional Commands Before Theatre Command

- Fully operationalise a tri-service Defence Space Agency (DSA) into a **Space Command with autonomous planning and operational authority**. Prioritise space asset hardening, quantum-secure data links, cyber proofing and orbital redundancy.
- Establish a **Cyber Command** with offensive and defensive capabilities across all domains.
- Create a **Pan-India Air Defence Command** across the entire Indian peninsular and land mass. The irrelevance of distance has exposed the entire land, air, sea, space and cyber mass.
- Create at each theatre level a **Missile-Drone Strike Force based on a MUM-T architecture** by restructuring and augmenting the Artillery Divisions and other long-distance fire assets.
- Arm the present **Strategic Force Command with more multidomain teeth** and precise strike capabilities.

5. Fund Multi-Layered Defence Transformation

- Shift away from mega-platform purchases to **systems warfare ecosystems**. Balance kinetic versus non-kinetic and contact versus non-contact components of warfighting.
- Develop layered C52SR redundancy and a **cyber-secure MDC2 architecture** to dominate the kill chain.
- Audit all major military infrastructure for **kill web vulnerability**.

Conclusion: A Decade to Survive or Lead

The wars of the future will be won by those who understand that **warfare is no longer about platforms, but about networks**. Precision-guided systems, uncrewed platforms, and deep learning algorithms are reshaping how nations generate combat power. In India's context, the challenge is not simply countering large-scale conventional threats but doing so with an advantage in tempo, precision and intelligence.

In the age of satellite surveillance, drone warfare, and hypersonic strikes, numerical superiority can be rendered irrelevant if it is not combined with superior battlespace awareness and compressed kill chains. China has internalised this logic and is acting on it with urgency. Its kill web strategy is not a threat in the future; it is a threat now.

India's military evolution must respond not only to conventional provocations along its borders but also to a rapidly evolving contemporary battlespace. **Emerging wars are shaped less by numerical strength and more by how smartly, precisely and quickly force can be applied across multiple domains.** The rise of artificial intelligence, machine learning, autonomous platforms, and cognitive warfare is not just transforming doctrines; it is redrawing the battlefield reality for every responsible power, including India.

This is the era of precise mass and kill web. It is a transformation India cannot afford to observe from the sidelines.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

References

1. Horowitz, Michael C. "Battles of Precise Mass: Technology Is Remaking War—and America Must Adapt." *Foreign Affairs*, May/June 2024. https://www.foreignaffairs.com/technology/battles-precise-mass-michael-horowitz .
2. Shivane A B, Lt Gen. "Focused C5isr- A Critical Capability For
3. Turbulent And Disputed Borders" https://cenjows.in/wp-content/uploads/2022/06/C5ISR-A-Critical-Capability-by-Lt-Gen-AB-Shivane-Retd-on-06-Jul-2020.pdf, June 2022.
4. Shivane A B, Lt Gen. *Operation Sindoor and the Future of India's Escalation Dominance Doctrine* https://www.csconversations.in/operation-sindoor-and-the-future-of-indias-escalation-dominance-doctrine , 2025.
5. Aroonabha Ghose. India's Weapons Systems: Op Sindoor, DefStrat, Jun 2025, https://www.defstrat.com/magazine_articles/indias-weapons-systems-op-sindoor/
6. Cohen, Raphael S. *The Future of Warfare in 2030:* RAND Corporation, 2020. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2849z1/RAND_RR2849z1.pdf
7. Marik Kalbarczyk. *Autonomy in defence: systems, weapons, decision-making,* https://eda.europa.eu/webzine/issue14/cover-story/autonomy-in-defence-systems-weapons-decision-making
8. KPMG. "AI in Indian Defence Modernisation, Jun 2025, https://kpmg.com/in/en/blogs/2025/06/artificial-intelligence-in-defence-modernisation.html
9. Vajiram. India's Military Space Doctrine: Preparing for the Final Frontier, Apr 2025, https://vajiramandravi.com/current-affairs/indias-military-space-doctrine-preparing-for-final-frontier/

10. Kill Web: China’s Cyber War in Spotlight | Asianet News, https://www.youtube.com/watch?v=G-wfTrUmxX0
11. Wenlin Liu, Zishuang Pan. Construction of kill webs with heterogeneous UAV swarms in dynamic contested environments, Nov 2024, https://link.springer.com/article/10.1007/s40747-024-01644-4