Issue Brief

June 2026
No: 516

Preparing for the Future Conflict in the Era of Multi-domain Warfare

Lt Gen AB Shivane
PVSM, AVSM, VSM (Retd)

Preparing for the Future Conflict in the Era of Multi-domain Warfare

Abstract

Recent conflicts indicate that warfare is shifting from 'attrition warfare' to 'compressed multi-domain operations' aimed at disrupting the adversary's decision-making system and targeting its critical capabilities. Cyber operations, electromagnetic manoeuvre, space-enabled intelligence, precision strikes, and narrative calibration now constitute a unified operational approach rather than separate capabilities.

This paper examines how these changes are unfolding and what they mean for India's security, particularly along the Western and Northern fronts. It argues that current employment concepts require a doctrinal shift towards a Cold Strike approach that emphasises strategic pre-emption, shorter decision cycles, integrated functional commands, and controlled escalation management. In such a framework, deterrence credibility will depend on the robustness of C5ISR architectures, land dominance, reliable aerospace control, the capacity to project maritime pressure (when necessary), data resilience, and a coordinated political–military decision structure capable of influencing the initiation, conduct, and conclusion of conflicts in a nuclearised environment. At its core, the argument is straightforward: speed of decision will matter more than the size of the force.

Keywords: Multi-domain Warfare, C5ISR, Escalation Management, Land Warfare, Aerospace Dominance, Maritime Domain, Cold Strike Doctrine, Future Wars

Introduction

The past decade has altered the conduct of war more sharply than the previous fifty years. Contemporary conflicts are no longer seen as extended mobilisation followed by sequential battles. Increasingly, they begin with coordinated pressure across multiple domains (IDN, 2025). Cyber penetration, electromagnetic interference, space-enabled surveillance and precision strike are fused to unsettle an adversary's command system before conventional operations visibly commence (Shivane, A.B. 2025). The real contest is now over decision cycles as much as it is over ground.

Cross-domain integration creates operational and strategic dislocation, leading to the enemy's paralysis. The result is systemic disruption across command, tempo, and perception. For India, this is not just an abstract theory of war. These are operational indicators of how the next war might unfold on the Western and/or Northern Front (The Week, 2025).

The next conflict India faces will not be a mirror of the past; it will not begin with traditional mobilisation or massed-force deployment. The shift will be from the Cold Start doctrine to a decisive Cold Strike. It will begin within networks, satellites, supply chains, and perception space, before any troop movement is evident (The Week, 2025). None of this is theoretical anymore; elements of it are already visible in current conflicts.

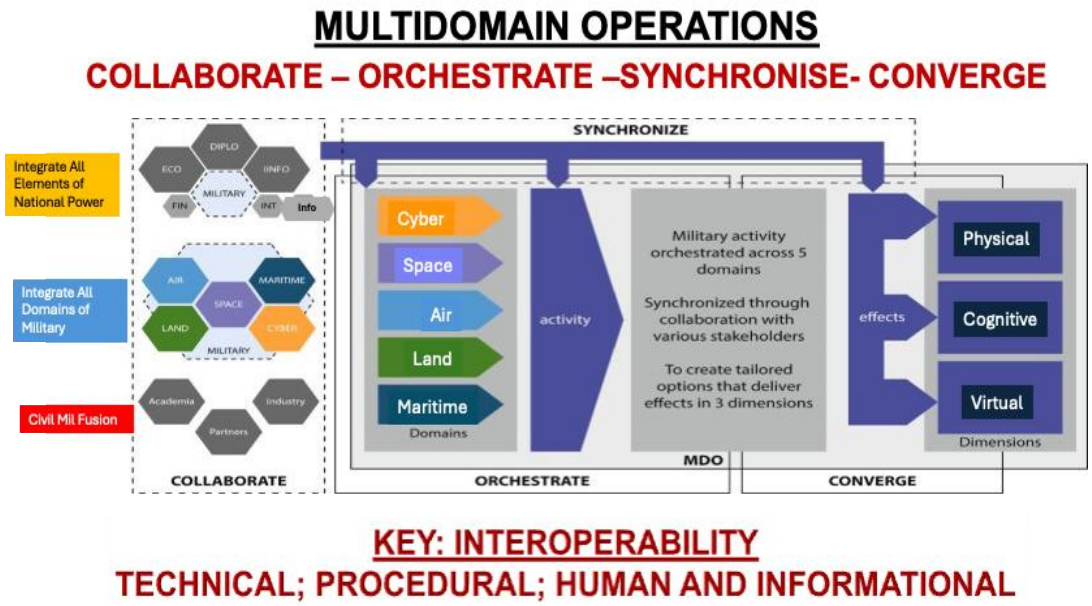
In such a battlespace, the true centre of gravity lies in the integrity of C5ISR architecture. The side that can protect its own information grid, while degrading the adversary's, will influence the tempo and velocity of the conflict. Control of this invisible network will shape the first phase of war long before conventional combat becomes visible in a multi-domain battlespace.

The Multi-domain Battlespace

The domains of warfare are rapidly expanding beyond the traditional focus on land, sea, and air. The nature of conflict has been transformed by the inclusion of cyberspace, space, and the cognitive domain at the forefront of competition. These are no longer conceptual domains. They are already shaping operations. The side that integrates these domains first gains the initiative.

The purpose of MDO is to leverage collaboration, orchestration, and convergence to present the enemy with multiple dilemmas across land, maritime, air, cyber, space, and cognitive domains, overwhelming their ability to respond effectively (The Week, 2025). The information environment is also incorporated, covering all domains.

Figure 1: No Multi-Domain Operations without Interoperability



Source: Democura

The key factor for success in MDO will be information superiority and decision dominance rather than brute force. Therefore, C5ISR will act as the main node, with all other methods and pathways functioning as the lines of effort.

Recent campaigns have demonstrated that the decisive blows often occur outside the visible battlefield. The Russian campaign in Ukraine was not limited to missile salvos and armoured thrusts; it was preceded by cyber disruptions of government servers and followed by persistent disinformation campaigns (Sanger, D. E. 2018).

Decision Dominance: Compressing the Sensor–Shooter Cycle

Recent conflicts indicate that the force capable of compressing the sensor–shooter loop often secures an early operational edge. Speed without clarity carries its own risks. When networks fracture the operational picture, rapid action can easily descend into confusion. Experience shows that months of intelligence preparation were followed by decisive kinetic phases that unfolded within hours rather than weeks. In some cases, air defence systems remained physically intact but proved ineffective because the command networks connecting them were blinded, spoofed, or disrupted in the battlespace.

The key lesson is that C5ISR must become the centre of gravity rather than just a support function. Sensors are not the issue. The system already gathers large amounts of data

from space assets, airborne vehicles, maritime surveillance, and cyber monitoring. The problem is no longer collection. It is making sense of data in time to act. What is needed is a national fusion architecture that converts scattered inputs into a single, continuously updated operational picture (Om, H. Saini, M.L., Kumar, A. and Tyagi, V. 2025).

An effective operational grid must enable commanders across services to observe and interpret the same battlespace simultaneously. While the human authority must not be diluted, AI can greatly assist in fusing, flagging anomalies, correlating patterns and filtering noise at machine speed (TNN, 2026). In a crisis, clarity of the operational picture becomes the difference between initiative and reaction.

Any future crisis will demand streamlining decision processes that normally involve several levels of consultation. Pre-approved escalation paths, regularly practised crisis protocols, and a continuously active multi-domain command structure would significantly reduce the time required for decision-making. Without this, faster systems will only produce faster confusion.

Cyber and the Electromagnetic Spectrum as Opening Salvos

In recent conflicts, the fight often begins before the first missile is fired. Radar displays show false tracks, communication nodes act unpredictably, and military headquarters struggle to distinguish interference from system failure. The invisible realms of cyber networks and the electromagnetic spectrum are no longer just supporting capabilities used alongside conventional forces. They are now tools to shape the battlespace before physical combat begins. Cyber intrusions and electronic warfare can alter radar images, weaken command networks, and disrupt critical infrastructure, creating chaos within an enemy's operational system even before the first kinetic strike occurs (Sanger, D. E. 2018). The overall effect is not just temporary but causes physical and psychological paralysis of the enemy's decision-making system.

India must assume that its networks will be targeted from the outset. Cyber resilience and protection of critical digital infrastructure are vital. Mapping strategic infrastructure, hardening industrial control systems such as SCADA, implementing redundant communication architectures, and providing independent power backups for military nodes are crucial safeguards (US DoD, 2020). These are not enhancements; they are basic survival requirements.

Electronic warfare must also advance from a niche capability to a routine operational skill, both for defensive and offensive actions. Training in a degraded, contested electromagnetic spectrum and a hostile cyber environment is crucial. Future survivability will rely on controlling the contested environment where deception, spectrum management, and cyber intrusion operate simultaneously.

Precision Mass and Saturation Strikes

The geometry of the battlespace is changing. The warzone is no longer defined by physical geography; it becomes fluid, invisible, dispersed, and highly dependent on timing. Targets can be detected and engaged at depth within minutes, often without large force concentrations. In this environment, advantage depends not on the size of formations, but on the ability to identify key nodes in the enemy's system and deliver precise effects swiftly and with coordination.

Precision shapes lethality on the modern battlefield. In future conflicts, advantage will go to the force that can detect, interpret, and strike critical nodes in an adversary's operational system faster than the opponent can respond. Conventional firepower remains essential, but it must now be directed through precision-enabled networks. What matters is how precision capabilities are integrated, not just how many are fielded. In such an environment, the outcome of engagements will rely less on the number of platforms and more on the speed and accuracy with which decisive effects can be achieved.

The recent wars have shown that precision requires volume and simultaneity (Pandey, A. 2025). The key is coordinated precision that uses different domains and their respective energies. Force application with long-range cruise missiles, stealth platforms, drones, and loitering munitions was preceded by suppression of the enemy's combat systems and paired with non-kinetic effects. These were saturation packages of multi-domain warfare that prevented and disrupted the enemy before achieving full-spectrum dominance.

India must develop a doctrine of precise mass. BrahMos variants, Pralay-class systems, extended-range artillery rockets, Fifth Generation strike aircraft packages, hypersonic research, and large-scale drone swarms should be integrated into theatre-level sensor-shooter networks (Shivane, A. B. 2025). Any validated sensor should be able to cue the most suitable shooter within seconds and remain resilient against electronic warfare, regardless of service ownership. The aim is not ground capture alone, but system disruption. Ammunition depots, command

nodes, communication relays, and logistics hubs must be targeted as part of an effect-based strategy that disrupts the adversary's tempo before it stabilises.

SEAD as a Systemic Competence

Suppression of enemy air defence (SEAD) increasingly influences the operational freedom of attacking forces. Once sensors, data links, and command nodes are disrupted, even advanced missile systems struggle to operate coherently. Recent conflicts have shown that layered missile shields failed because they were electronically isolated and kinetically targeted in a coordinated way.

Layered air defence by itself does not ensure survival. Resilience depends on a combination of mobility, deception, strict emission discipline, and redundancy within the network. Systems that remain static or predictable, or that rely too heavily on continuous radar emissions, become vulnerable to both electronic and kinetic attacks.

For India, strengthening the SEAD capabilities must become a key part of joint operational planning. Indigenous anti-radiation missiles, specialised electronic warfare aircraft, and AI-enabled targeting tools should be developed and used in a coordinated way to weaken hostile air defence networks at the start of a crisis (TNN, 2026). Plans along India’s northern and western borders will likely require a quick neutralisation or disruption of enemy missile defences to create the operational space needed for air and ground forces to move with confidence. In effect, survivability shifts from protection to adaptability.

Primacy of Land Warfare in a Contested Border Environment

Despite the growing importance of cyber, space, and aerospace domains, India’s strategic focus remains rooted in land. Both the western and northern borders are characterised by disputed boundaries, unresolved claims, and the constant presence of adversarial forces. Geography still imposes limits that technology cannot remove. For India, territory still visibly shapes deterrence.

The Line of Control and Line of Actual Control remain contested borders with strategic implications. In such a context, land power alone turns military advantage into visible and negotiable control. Aerospace and maritime capabilities expand options and provide protection. Still, they cannot replace the need to hold ground, secure approaches, and support forward troops amid altitude, weather, and infrastructure challenges.

Future confrontation along these borders is unlikely to resemble large-scale manoeuvres across open plains. It will more likely involve sharp, localised engagements, rapid reinforcement under surveillance, contests for key features, precise artillery exchanges, and sustained logistical endurance in tough terrain. Success will depend as much on acclimatisation, engineering support, and redundant supply lines as on firepower.

For India, deterrence through denial and domination is assessed in practical terms: preventing any change to the current ground position. In a contested border environment, that responsibility primarily falls on land forces.

Aerospace Dominance as the Decisive Enabler

Recent conflicts confirm that control of the aerospace domain influences the speed, depth, and direction of modern warfare. Aerospace dominance goes beyond traditional air superiority (Jayakumar, P.B. 2025). It combines air power, space assets, near-space platforms, and missile defence into a unified operational framework that maintains freedom of action while limiting the adversary's options.

Conflicts over the past year have shown that early control of the air and protection of space-based enablers shorten battlespace timelines, enabling operations to proceed at a pace the adversary struggles to match. It also signals intent and capability before conflict escalates. Visible readiness, quick reach, and layered defences enhance deterrence before conflict expands.

Aerospace dominance will be the key factor in deciding whether future forces operate under protection or face ongoing vulnerability. Without secure control of airspace and reliable space-based support, precision operations slow down, and escalation becomes unpredictable.

Maritime Leverage and Undersea Control

Operations in West Asia highlighted the importance of maritime depth and long-range capabilities. For India, geography is a strategic advantage in the Indian Ocean Region. The Andaman and Nicobar Command should develop into a fully equipped joint strategic command with long-range strike abilities, ongoing maritime domain awareness, and distributed logistics.

The undersea domain requires much greater strategic focus. Submarines, seabed surveillance systems, and specialised anti-submarine aviation can influence the speed and freedom of action across the broader maritime theatre. Their value lies as much in uncertainty

as in stealth. In a two-front scenario, the ability to threaten or disrupt sea-based trade and energy routes would provide India with a form of measured pressure that falls short of immediate escalation on the continental front. When used effectively, undersea capabilities enhance strategic choices by allowing maritime influence to shape the conflict environment well before large-scale land operations begin.

India's maritime geography also provides leverage through sea denial and control of key chokepoints. The approaches to the Malacca Strait, Lombok Strait, and other critical sea lanes put the Andaman and Nicobar Command in a position to monitor, influence, and, if necessary, interdict adversary naval movements. In a broader conflict scenario, the ability to create uncertainty around maritime traffic and energy flows through these routes would complicate an adversary's strategic calculations without necessarily escalating the continental front. Permanent dominance is not required; credible disruption is enough.

Functional Commands Before Theatre Optics

Recent conflicts have sharply highlighted a reality often hidden by institutional debates: operational success depends more on 'how well different capabilities work together in real time than on formal command structures'. Interdependence across domains is more important than organisational integration, and integration matters more than the labels assigned to headquarters. The ongoing discussion in India about theatre commands, while necessary, risks becoming fixated on structural changes at the expense of developing functional mechanisms capable of producing decisive cross-domain effects.

The priority should be on functional commands that deliver results, not on structures that look integrated. A Cyber Command must go beyond network defence to include the ability to conduct persistent offensive cyber operations that can disrupt adversary command systems and critical infrastructure during a crisis.

A Space Command also requires a similar change in perspective. Satellites can no longer be seen solely as tools for navigation or communication; they are essential assets supporting surveillance, targeting, and secure connectivity during conflicts. Handling these capabilities needs a command structure that views the space domain as a contested operational environment.

A C5ISR Command must connect every radar, drone, and sensor. A dedicated command structure responsible for this network should ensure that information from all sensors

is fused, analysed, and quickly transmitted to those who need to act on it. Speed of understanding, not just speed of weapons, is what increasingly separates advantage from vulnerability.

Other areas require a similar focus. Long-range fires, delivered via rockets, loitering munitions, and armed drones, are becoming a key tool for applying operational pressure. A specialised Drone and Rocket Force could produce sustained precision strikes deep within enemy territory without the expenses linked to traditional air campaigns.

At the same time, India's air defence system needs deeper integration. An Integrated Air Defence Command would unify the country's sensors, interceptors, and command networks into a single, responsive defensive grid. This architecture would ensure that threats from aircraft, missiles, and unmanned systems are detected early, tracked smoothly, and countered through a coordinated national response rather than by fragmented service actions.

Recent conflicts leave little room for ambiguity. Multi-domain effects, not multi-service symbolism, shape outcomes. Until India achieves functional synergy, theatreisation risks becoming a mere structural change rather than accelerating operations.

Escalation Management as Design, Not Afterthought

The main lessons learnt from recent conflicts are how to control escalation. Successful campaigns are rarely the result of accidental responses that escalate on their own. Instead, they are guided by clear political goals and specific military tasks; occupation, regime change, and endless entanglements are intentionally avoided. In these conflicts, escalation is 'not an accident but a planned outcome, with each increase considered and politically evaluated before new hostilities begin'.

For India, this requires moving beyond an implicit understanding of escalation towards a clearly articulated doctrine. Escalation should not be seen as a simple linear progression from tactical action to strategic crisis. It is better understood as a 'matrix of choices wherein military pressure, diplomatic signalling, information campaigns, and economic measures can be applied in different combinations'. Such a framework enables the state to keep the initiative, adjust pressure across domains, and prevent the adversary from controlling the narrative space.

Operating within a nuclearised environment makes this discipline essential. Every stage of conflict must include an implicit understanding of how and where it is meant to conclude.

Clear termination pathways are as crucial as the initial moves. Operation Sindoor demonstrated the importance of calibrated response and political restraint. A future Sindoor 2.0 would require even closer integration of political guidance and military action, supported by strategic communication that shapes perceptions from the very beginning.

Strategic Communication and the Contest for Narrative

Experience from recent conflicts shows how narratives and perception management can influence strategic space as much as military action (Schake, K. 2022). Press briefings, international outreach, and clear articulation of strategic objectives must shape the narrative space before adversaries can gain ground by distorting it.

Strategic communication must be institutionalised, not improvised. Messaging during crisis should not be ad hoc or scattered across different institutions. A dedicated Director General for Strategic Communication, based near the top security leadership and working closely with the Chief of Defence Staff and the National Security Council, would ensure coherence. Every major operation should be paired with early diplomatic outreach, consistent and timely public messaging, and ongoing efforts to explain India's objectives. In today's information environment, silence is quickly filled by others.

Cognitive resilience within the country is equally important. Adversaries often exploit disinformation, social divisions, and propaganda. Such efforts aim to erode confidence and distract attention when national resolve is most needed. Therefore, preparing for conflict requires an informed public and a National Citizens Security Culture, in which society and citizens become equal partners in the national security strategy.

Data as a National Security Mission

Data now sits at the core of national security, but the real test is not how it is used in normal times; it is 'who holds control when systems are under pressure' (Shivane, A.B. 2025). [16] Data sovereignty, in that sense, is not about legal or policy language. It is about whether critical data remains within reach when networks are disrupted, supply lines are uncertain, and external dependencies begin to fail. That question remains insufficiently addressed.

Critical data must be identified unambiguously, separated from the rest, and stored in systems designed for redundancy and survivability. Data needs to be treated as a strategic asset, and its security as a national mission. Data sovereignty in critical areas must be achieved. Disruption should be built into exercises, not treated as an exception; and policy has to provide

industry with a steady framework to work within, so that capability grows in step with national needs.

Logistics and Industrial Depth

Contemporary wars demand preparation, sustenance, and war endurance. Precision munitions, resilient networks, and trained cadres require ongoing investment. In conflict, availability often outweighs theoretical optimisation. Real-time AI-enabled logistics dashboards, predictive maintenance, and domestic industrial capacity in critical technologies become vital for endurance in modern warfare (TNN, 2026).

Self-reliance in defence production must move beyond intent. India's approach to Atmanirbharta should promote rapid innovation in fields such as artificial intelligence, counter-UAS systems, quantum communications, and autonomous platforms (Michael C. Horowitz, M.C. 2019). An integrated defence ecosystem and a robust defence industrial base will determine the capability and capacity for future conflicts. Readiness will depend on indigenous R&D focused on achieving technological sovereignty, with clear operational delivery timelines.

Possible Contours of Next War

A plausible scenario begins with a high-impact terror event or clear intelligence of imminent cross-border escalation. Within hours, cyber operations degrade adversary communication nodes and power supplies in targeted sectors. Electronic warfare disrupts radar and air defence systems along selected corridors. Simultaneously, precision mass strikes neutralise identified infrastructure across depth. Drone swarms saturate tactical zones. The aerospace domain ensures freedom of manoeuvre and disrupts enemy assets, while maritime assets posture to signal extended reach. Strategic communication frames the action as limited, precise, and defensive. The intent is to impose immediate operational shock while maintaining escalation control.

Escalation ladders are managed through calibrated signalling, diplomatic outreach, and visible readiness without uncontrolled expansion. The objective is 'denial and domination', not occupation. Termination profiles are defined from the outset.

The next conflict is likely to develop through a phased operational approach aimed at 'detecting, disrupting, degrading, and ultimately dominating' the adversary's decision-making system.

Table 1: Phased Operational Framework for Achieving Battlespace Dominance

Phase	Operational Objective	Primary Means	Targeted Effect	Operational Outcome
Phase 1 Detect	Comprehensive Situational Awareness; Identify CoG	Integrated multidomain ISR	Upgrade Target List and Electronic Signatures	Dominant Battlespace Awareness and Decision Superiority
Phase 2: Disrupt	Disrupt situational awareness	Precision strikes, cyber-electronic operations, long-range stand-off systems	Disrupt C5ISR nodes	Fragmented decision cycle and reduced response coordination
Phase 3: Degrade	Exhaust defensive capacity	Sustained multi-vector drone and missile pressure	Force repeated defensive engagements	Reduced interception density and response sustainability
Phase 4: Dominate	Achieve decisive operational dominance	Employment of advanced long-range and high-speed strike systems	Penetration of weakened defensive grid	Strategic ascendancy and cognitive dominance

Source: Prepared by Author

The opening phase aims to achieve clear situational awareness and weaken the enemy's centres of gravity. The goal is to establish clear operational understanding before any kinetic action. This requires integrated multi-domain intelligence, ongoing electronic

signature mapping, and carefully planned cyber intrusions designed to identify vulnerabilities within command networks and critical systems. Information gathered from space assets, airborne surveillance, cyber reconnaissance, and electronic monitoring must be combined into a unified view of the adversary's operational structure. The purpose is not just to observe but to understand how the opponent's command system functions, where decision-making nodes are located, and which dependencies, if disrupted, could cause significant operational consequences.

Once this awareness is established, the **next stage concentrates on disrupting the adversary's situational awareness structure.** Precision strikes, cyber–electronic operations, and interference with system signals target key C5ISR nodes. The goal is not just to cause physical damage but to break the adversary's decision cycle. As information flows are blocked and command links weaken, coordination between sensors and shooters breaks down, and response mechanisms slow.

The following phase aims to weaken the opponent's defensive capacity through sustained pressure. Multi-vector drone and missile attacks force the adversary to repeatedly activate and deplete its defensive resources. As engagements increase, interception density decreases, and the defensive network's resilience begins to decline, gradually reducing the effectiveness of the opponent's response system.

The final phase aims to turn accumulated degradation into clear operational dominance. As the defensive network weakens and response times lengthen, advanced long-range, high-speed strike systems are used to deliver focused, impactful effects. At this point, the goal is to establish overwhelming operational superiority and secure strategic dominance through precision, speed, and concentrated force.

Technological Foundations of a Phased Operational Design

Figure 2: Integrated Multi-Domain Operational Architecture for Future Warfare

Source: Prepared by Author

Phase I – Detect: Building the Picture

The goal is to sustain ongoing situational awareness rather than rely on intermittent surveillance.

Technological Foundation: Ongoing Multi-domain Surveillance and Information Fusion.

Key Technology Capabilities

- Electro-Optical and Synthetic Aperture Radar Satellites for persistent strategic surveillance.
- High-Altitude Long Endurance (HALE) UAVs for continuous wide-area monitoring.
- Airborne Early Warning & Control (AEW&C) aircraft for aerial battlespace visibility.
- Ground-based Over-the-Horizon and Phased-Array Radar Networks.
- Signals Intelligence (SIGINT) and Electronic Support Measures (ESM) for electromagnetic mapping.

- AI-Enabled Sensor Fusion Platforms within Battlefield Management Systems.
- Cyber reconnaissance tools are probing the adversary command networks.

Outcome

- Development of a coherent and continuously updated operational picture.
- Identification of command centres, surveillance infrastructure and logistic corridors.
- Improved situational awareness, hence enabling informed operational planning before kinetic engagement.

Phase II – Disrupting the Adversary's Decision System

The objective of disruption is to undermine the coherence of the adversary's decision-making network.

Technological Foundation: Precision Strike, Electronic Warfare and Cyber Disruption.

Technology Capabilities

- Stand-off precision strike weapons launched from aircraft and ground platforms.
- Electronic warfare aircraft and ground EW systems for radar and communication jamming.
- Satellite communication interference systems targeting adversary data links.
- Cyber intrusion platforms capable of degrading command networks.
- Electronic attack pods on fighter aircraft disrupting sensor systems.
- Decentralised EW brigades operating across the electromagnetic spectrum.

Outcome

- Degradation of the adversary's command, control and surveillance network.
- Disruption of communication pathways between headquarters and field formations.
- Distort the decision cycles and reduce coordination between sensors and weapons.

Phase III – Degradation of Defensive Capacity

Saturation is intended to overwhelm and steadily erode the adversary's defensive capacity.

Technological Foundation: Saturation and Attrition through Autonomous Systems.

Key Technology Capabilities

- Loitering munitions and armed unmanned aerial systems.
- Drone swarm technologies coordinated through autonomous control algorithms.
- Long-range rocket artillery and tactical ballistic missile systems.
- Decoy drones and electronic deception platforms.
- Autonomous navigation and encrypted swarm communication links.
- AI-driven mission planning for distributed attack waves.

Outcome

- Saturation of air defence networks and repeated engagement cycles.
- Gradual depletion of interceptor missile inventories.
- Reduced radar coverage and increased gaps in the defensive network.

Phase IV – Dominate: Converting Advantage into Operational Control

Precision strikes translate systemic degradation into tangible operational control.

Technological Foundation: Precision Strike Integration and Dynamic Targeting.

Key Technology Capabilities

- Long-range precision weapons, including cruise missiles and advanced stand-off munitions.
- Integrated targeting networks combining satellite, UAV, and airborne surveillance feeds.
- Hypersonic or high-speed strike systems capable of rapid engagement of high-value targets.
- Real-time secure data links enabling dynamic retargeting during operations.
- Network-enabled command systems linking ISR with strike platforms.
- AI-assisted targeting and battle damage assessment tools.

Outcome

- Neutralisation of critical command centres and logistic nodes.
- Collapse of coordinated defensive response mechanisms.
- Operational superiority and dominance in the battlespace.

Towards a Cold Strike Doctrine: A Doctrinal Shift to Contemporary Conflicts

The preceding analysis underscores the need for doctrinal adaptation in India's strategic approach. Cold Strike is not an incremental update to the Cold Start concept. The focus shifts from mobilising forces in response to provocation to seizing the critical opening hours of a crisis through integrated ISR, cyber disruption, precision stand-off fires, and carefully managed escalation. It embodies a proactive, calibrated strategy designed to impose an unacceptable cost-benefit equation on an adversary's intent.

Figure 3: Cold Strike Doctrine Architecture

Source: Prepared by Author

The trigger in such a framework could be credible intelligence indicating an imminent threat. This could include the expansion of terrorist infrastructure, heightened proxy activity, or verifiable preparations for an attack. The response would be structured rather than reactive. Readiness levels would be raised as air defence, internal security, and force protection measures

are activated in parallel. Non-kinetic means, such as cyber penetration, electronic warfare, and information operations, would be activated. Precision kinetic options would then follow in defined cycles, focusing on command nodes, launch infrastructure, logistics hubs and critical enemy capabilities.

The stand-off kinetic strikes would aim to overwhelm the adversary's Air Defence System in a strategically planned force application. First, a massive launch of Kamikaze drones that identify and overwhelm the air defence system, followed by deep strikes by ballistic and cruise missiles, and after that, employment of hypersonic systems against critical operational and strategic targets.

Escalation would unfold across domains in cycles of roughly 12 to 24 hours, constantly reassessed under political guidance and executed through military channels. If necessary, non-contact operations could transition to limited ground action through Integrated Battle Groups, although contact warfare would not be the default approach.

The doctrinal shift is fundamentally conceptual. Cold Start sought manoeuvre dominance after a triggering event and was platform-centric. Cold Strike seeks decision dominance and is system-centric. The concept places greater emphasis on manoeuvre-based warfare, with strategic dislocation as the key lever, rather than on attrition and destruction. It also reflects a shift from punitive deterrence to a model based on denial and dominance. Such a shift would require a corresponding structural change within the force.

Table 2: Cold Start to Cold Strike: The Fundamental Difference

Cold Start Doctrine	Cold Strike Doctrine
Mobilisation after provocation	Pre-emptive anticipation
Platform-centric warfare	System-centric warfare
Manoeuvre after trigger	Decision dominance from outset
Punitive retaliation	Deterrence by denial and dominance
Attrition focused	Strategic dislocation focused

Source: Prepared by Author

At the centre of the concept lies strategic pre-emption. Terror networks function through distributed nodes, digital enablers, and deniable proxies. When hostile patterns become clear, and attribution is credible, action must precede impact. This approach is not driven by adventurism but by the need to sustain deterrence credibility. The principle gradually moves from a declaratory equivalence between terror and war towards assured consequences of proactive retribution. In this framework, precision supported by massed effects replaces simple accumulation of platforms.

Escalation management remains critical throughout the process. Each rung must integrate the application of military force with diplomatic signalling, economic leverage, and narrative control. Exit strategies and conflict termination profiles for each stage would be designed at the outset. Conflict termination is shaped, not improvised. Limited war in a nuclear environment would demand orchestration rather than hesitation.

Tri-service net-centricity is therefore indispensable. Theatre commands cannot function through segregated networks or due to resource inadequacy. Functional commands and interdomain interoperability must precede them. A common data architecture, unified encryption protocols, shared spectrum management, and clear lines of accountability are essential. Command authority without control over data flows would remain largely notional.

Cold Strike marks a shift from 'a reactive to an anticipatory deterrence posture in India'. The redefined framework emphasises readiness over mobilisation, anticipation over reaction, integration over aggregation. Cold Strike Doctrine, thus, must become India's strategic message, 'delivered with lethality, precision, and integrated multi-domain synergy' to 'deter, detect, deny, dominate, and defeat future threats'.

Operational Constructs: Sindoor 2.0 and Galwan 2.0

Sindoor 2.0: Systemic Counter-Proxy Limited War

- **Operational Triggers:** Sindoor 2.0 would most likely be triggered by a major terrorist attack that causes significant casualties and is linked to cross-border sponsorship. Other triggers might include credible intelligence indicating preparations for imminent mass-casualty operations by state-backed networks. Such developments would carry substantial political weight and require a calibrated government response to restore deterrence credibility. In the initial hours, clear assurance of retribution would be

crucial. Decisions would rely on integrating evidence from multiple sources, including cyber forensics, technical intelligence, and human sources. They would be supported by AI-assisted analysis that can connect scattered indicators into a coherent operational picture.

- **Threat Analysis:** The threat would be hybrid in nature. It would involve deniable proxy actors, hardened launch and training infrastructure, cyber capabilities targeting Indian networks, and a coordinated information campaign to frame escalation as disproportionate. The adversary's core strength would not lie in traditional force superiority but in resilient proxy networks and international diplomatic strategies designed to limit escalation.
- **Desired End State:** The goal is the restoration of credible deterrence, measurable degradation of proxy operational capacity, demonstrable cost imposition on enabling infrastructure, and controlled termination below nuclear signalling thresholds. The adversary must emerge with reduced operational capability and increased uncertainty about the likelihood of repetition. Escalation should remain calibrated and bounded.
- **Force Orchestration:** Force orchestration would require synchronised multi-domain integration. A National C5ISR architecture would reduce decision cycles and enable real-time target validation. Cyber commands would initiate shaping operations to isolate adversary command hierarchies. Space-based ISR would maintain persistent surveillance and conduct battle damage assessments. Maritime forces would offer flexibility in escalation and protect sea lines without prematurely broadening the scope of the conflict.
- **Force Application:** Force will be calibrated, sequenced, and executed simultaneously. Initial cyber disruption and electromagnetic shaping will degrade defensive coherence. Precision mass strikes using missiles, armed drones, and stand-off air assets will target logistics hubs, training infrastructure, command nodes, and financial enablers. The goal is systemic dislocation rather than symbolic retaliation. Saturation within compressed windows will prevent adaptive recovery.
- **Operational dominance and denial:** Focus on preventing regeneration capacity. Persistent ISR halts the quick reconstitution of proxy networks. Financial disruption and cyber pressure weaken funding channels. Integrated air and missile defence protects India's critical nodes from retaliation. Information dominance enhances legitimacy and limits the adversary's ability to manipulate narratives.

- **Escalation Management:** Escalation management depends on predefined political authorisation matrices and clearly defined thresholds. Horizontal escalation options across cyber and maritime domains offer flexibility without expanding vertically. Nuclear thresholds remain protected through disciplined target selection and control of signalling. Diplomatic engagement occurs alongside operational activities.
- **Conflict Termination Profile:** Termination would be declared upon demonstrable degradation of proxy capacity and the restoration of deterrence credibility. Diplomatic signalling would frame the operation as limited and focused on objectives.

Galwan 2.0: LAC Escalation

- **Operational Triggers:** A stand-off along the disputed LAC could trigger a Galwan 2.0 crisis, leading to confrontation or conflict. The stand-off may result from territorial incursions, aggressive patrolling beyond agreed limits, disputes over border infrastructure, or changes to the status quo ante. Unlike Sindoor 2.0, it could cause direct military friction between two states rather than proxy violence. The outcome would be much faster reaction times, with local actions quickly gaining strategic importance, and a significant reduction in the margin for misjudgement.
- **Threat Analysis:** The threat environment would focus on incremental territorial encroachment, grey-zone coercion, and psychological signalling. The adversary may use rapid mobilisation, layered air defence, cyber probing, and information campaigns to gain a perception advantage. Terrain constraints and limited manoeuvre corridors would increase reliance on ISR dominance and air mobility.
- **Desired End State:** The goal is to restore the status quo ante along the Line of Actual Control, reinforce tactical deterrence, and stabilise escalation without expanding the theatre. The aim is not extensive infrastructure destruction but rather to deny territorial advantage and impose localised tactical costs sufficient to deter repetition.
- **Force Orchestration:** Force orchestration would require an integrated theatre posture that combines land forces, tactical air assets, ISR platforms, and space-enabled surveillance. Rapid reinforcement through air mobility and resilient logistics chains would demonstrate resolve. Integrated air defence and cyber resilience would protect forward formations. Coordination across theatre commands would ensure unity of effort without premature horizontal expansion.

- **Force Application:** Focuses on denial and tactical dominance. Precision fires would target forward logistics nodes and staging areas directly connected to contested sectors. Air-land coordination would establish localised superiority while avoiding deep strategic strikes. ISR saturation would prevent surprise manoeuvres and maintain transparency across the theatre.
- **Operational Dominance and Denial:** Dominance is defined by control of key terrain, surveillance superiority, and sustainment resilience. Denial prevents the consolidation of adversary gains and restricts incremental encroachment. Maritime and long-range strike forces remain levers in any escalation of a deterrent posture.
- **Escalation Management:** Managing escalation in such a situation requires careful signalling, military-to-military talks, and diplomatic engagements. Vertical escalation must be avoided while preserving credible horizontal options to reduce the risk of miscalculation.
- **Conflict Termination Profile:** An end to the confrontation would most likely occur through negotiated disengagement. This could involve withdrawing forces from face-off points, restoring mutually agreed buffer arrangements, and reaffirming border management protocols. The outcome would be stabilisation rather than a dramatic resolution.

Strategic Contrast: Sindoor 2.0 vs Galwan 2.0

Sindoor 2.0 is a targeted proxy campaign designed to impose ongoing costs on hostile networks and restore deterrence credibility. Its focus is on degrading the infrastructure, logistics, and systems that support proxy violence.

Galwan 2.0, in contrast, reflects a theatre-specific confrontation between regular forces in a sensitive border environment. The operational focus in such a situation is on denying territorial advantage, restoring the existing ground position, and achieving early stabilisation before a local clash escalates into a broader crisis.

Both contingencies require quick decision-making, resilient command structures, and careful escalation management. The logic behind each is different. Sindoor 2.0 aims to build a counter-proxy ecosystem. Galwan 2.0 focuses on preventing changes on the ground and restoring tactical stability along the LAC.

In the Indian context, whether during a Sindoor 2.0 counter-proxy operation or a Galwan 2.0 high-altitude confrontation, an adversary would almost certainly try to exploit cost asymmetry against India's air and missile defence network. The initial effort would likely focus on disrupting forward-sensing and command systems. Radar nodes, communication relays, and elements of the air defence command structure could face cyber intrusion, electronic interference, and attacks by expendable drones.

Once disruption begins to take effect, large numbers of inexpensive rockets, loitering munitions, and cruise weapons may be employed. The goal would be less about individual precision strikes and more about exhausting interceptor inventories and stretching defensive coverage across multiple axes.

Only when defensive density starts to weaken would higher-value capabilities be introduced. These could include longer-range precision systems and, in a northern theatre, potentially even hypersonic weapons intended to achieve a decisive tactical or symbolic effect.

For India, the lesson is clear. Effective escalation control in both limited punitive campaigns and high-altitude stand-offs will rely on resilience. Distributed sensors, layered interception, redundant command networks, and indigenous replenishment capacity are essential. They are the fundamental requirements for maintaining deterrence in a conflict environment shaped by saturation and cost pressures.

Conclusion

Future wars will not be decided by numbers alone, but by how well systems are connected and how quickly decisions are made. Modern warfare is about systems and speed, with perception shaping both. India must shift from platform-focused thinking to system-focused integration. Functional Commands should come before the formal symbolism of Theatre Commands. The next war will test not only a nation's structures and platforms but also its networking and interdomain integration.

For India, adopting the Cold Strike doctrine, integrating C5ISR capabilities, and leveraging niche technologies are essential to maintaining credible deterrence in a multi-domain threat environment. Future conflicts will favour the nation that can 'think, decide, and strike faster' than its adversary can understand what is happening. Victory will favour the force

that can ‘understand faster, decide earlier, and act with coherence’. In that sense, much of the next war will be decided before it is visibly fought.

Works Cited

Army Embraces AI (2026, February 25). *The Times of India*. https://timesofindia.indiatimes.com/city/indore/army-embraces-ai-as-maj-gen-shukla-speaks-on-predictive-analytics-at-awc/articleshow/128761541.cms.

Challenges in handling data security in Data analysis (2024, October). *IJCSPUB Vol. 14 (4)*. https://rjpn.org/IJCSPUB/papers/IJCSP24D1033.pdf.

DoD Data Strategy (2020). *US DoD*. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-Data-Strategy.pdf.

Horowitz, M.C. (2019). Quantum Computing and Military Power. *Orbis* 63, no. 2.

Jayakumar, P.B. (2025, September 30). IAF, Army and Navy formed a joint operational backbone during Operation Sindoor. *Fortune India.* https://www.fortuneindia.com/india/iaf-army-and-navy-made-joint-operational-backbone-during-operation-sindoor-rajnath-singh/127139.

Kania, E. and Costello, J. (2018). Quantum Hegemony. *CNAS Report.* https://www.cnas.org/publications/reports/quantum-hegemony.

Mission Sudarshan Chakra. *NDTV*. https://ndtv.com/india-news/sudarshan-chakra-to-protect-our-skies-indias-iron-dome-explained-4283979.

Modern Warfare Is No Longer Linear, But Networked, Deceptive and Indigenous (2025, May 31). Indian Defence News. https://www.indiandefensenews.in/2025/05/modern-warfare-is-no-longer-linear-but.html.

Om, H., Saini, M.L., Kumar, A. and Tyagi, V. (2025, November 5). Leveraging Artificial Intelligence in Modern Defense: Integrating Generative AI, Cybersecurity, and Military Doctrine *Transformation. International Journal of Engineering Research & Technology, 14 (10)*. https://www.ijert.org/leveraging-artificial-intelligence-in-modern-defense-integrating-generative-ai-cybersecurity-and-military-doctrine-transformation.

Operation Sindoor Narrative and Multi-Domain Dynamics (2025, July 16). *The Week*. https://www.theweek.in/news/defence/2025/07/16/self-reliance-in-uav-counter-unmanned-aerial.html.

Pandey, A. (2025, December 29).Operation Sindoor and Beyond: How India Prepared for Future Wars in 2025. *The Times of India*. https://timesofindia.indiatimes.com/india/operation-sindoor-and-beyond-how-india-prepared-for-future-wars-in-2025-year-ender/amp_articleshow/126224785.cms.

Sanger, D.E. *The Perfect Weapon* (New York: Crown, 2018).\

Schake, K. (2022). Civil Resilience in Modern War. *Survival,* 64 (3).

Shivane, A. B. (2025). Operation Sindoor and the Triangular Battlespace: An Assessment of India, Pakistan, and China’s Strategic Construct and Future Strategies. *Faultlines*.

Shivane, A. B. (2025, May 15). India's Bold New Doctrine: Turning 'Act of Terror = Act of War' into Reality. *CENJOWS*. https://cenjows.in/indias-bold-new-doctrine-turning-act-of-terror-act-of-war-into-reality.

Shivane, A.B. (2025, May 21). Op Sindoor 2.0: Why & How India Must Prepare for the Next Round. *CLAWS*. https://claws.co.in/op-sindoor-2-0-why-how-india-must-prepare-for-the-next-round/.

Shivane, A.B. (2025, August). Military Doctrine For Drone Integrated Warfare. *CENJOWS*. https://cenjows.in/wp-content/uploads/2026/01/August-2025-Synergy.pdf#page=119.

About the Author

Lieutenant General AB Shivane PVSM, AVSM, VSM (Retd) is an NDA alumnus and a second-generation decorated Armoured Corps officer with over 39 years of distinguished military service. He is former Strike Corps Commander and Director General of Mechanised Forces. As a scholar-warrior, he has authored over 300 publications on national security, geopolitics, defence technology, doctrines, and related matters, in addition to four books, and is an internationally renowned keynote speaker. The General was a Consultant to the Ministry of Defence (Ordnance Factory Board) post-superannuation. He was the Distinguished Fellow and held the COAS Chair of Excellence at the Centre for Land Warfare Studies (CLAWS) 2021-2022. He was also a key member of the Indian Army Study Team on Technology Induction 2025. He is presently the Strategic Advisor and Board Member to several organisations and Think Tanks.