Issue Brief

April 2026
No: 502

India's Multi-Domain Operations: Doctrine and Capability Development

Brig Navneet Bakshi
SM, VSM

India's Multi-Domain Operations: Doctrine and Capability Development

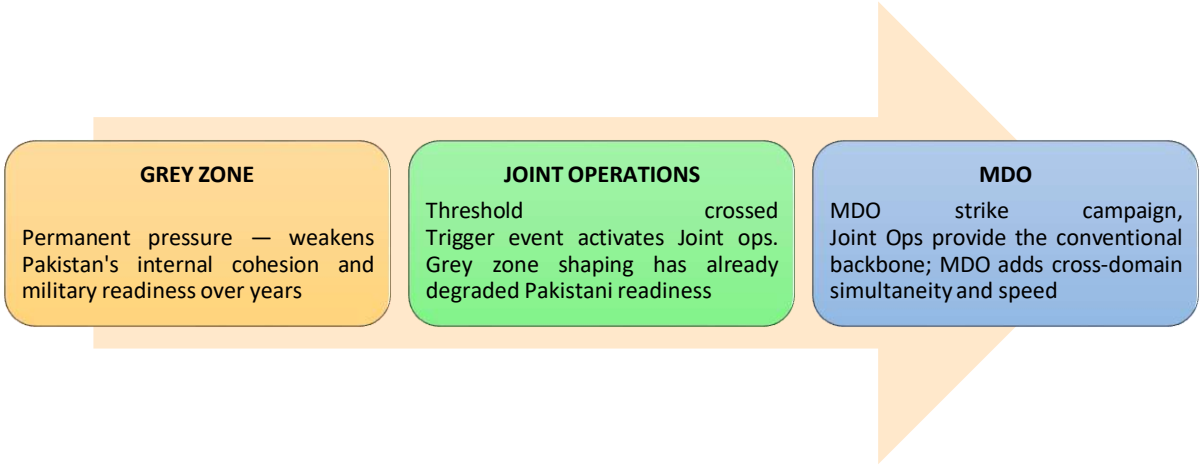
Abstract

India commenced a strategic pivot on 27 August 2025 with the unveiling of its Joint Doctrine for Multi-Domain Operations (MDO) by Raksha Mantri, Shri Rajnath Singh at "Ran Samwad 2025". The Joint Doctrine for Multi-Domain Operations (MDO), enunciated by HQ Integrated Defence Staff (IDS), leads the Indian Armed Forces for future war and dictates a "Whole-of-Nation" approach that fuses military muscle with civilian ingenuity across six frontiers identified as land, sea, air, space, the digital world and the human mind. The aim is to strike with convergent effects, overwhelming an adversary by addressing them from every direction at once (IADN Editorial Team, 2025)[1]. The doctrine is laid down over five chapters. ***Chapter 1*** *emphasises rapid technological disruption, grey-zone coercion along the LAC, collusive threats and a truncated OODA Loop in future warfare.* ***Chapter 2*** *explains the six domains viz. physical (land, sea, air), virtual (cyber, space) and cognitive (information/narrative battlespace). The cognitive domain is given added emphasis, rooted in India's civilisational ethos of "Satyameva Jayate" (Truth Alone Triumphs), positioning narrative dominance as a strategic asset. MDO, however, goes beyond jointness by dictating civil-military fusion (CMF) wherein non-military actors provide ISR via private satellites, AI analytics from start-ups, logistical support from industry, and counter-disinformation through media coordination (Indian Army, 2025)[2].*

Let us understand the MDO doctrine and appreciate how it fits into our current doctrine. MDO harvests what the grey zone has cultivated. Joint Operations is the reliable conventional threat that ensures Pakistan's military deterrence during grey-zone competition and provides the ground and air backbone on which MDOs' cross-domain effects will be superimposed. The strategic weakness today is that, MDO requires integrated theatre commands, AI-enabled C2, and unified cyber-space kinetic targeting systems that India is yet to fully operationalised. Until those are operational, India would fight using Joint Operations as the primary warfighting model, with grey-zone tools running in parallel and MDO elements layered on as and when they are fielded.

Keywords: Multi-Domain Operations (MDO), Whole-of-Nation Approach, OODA Loop Compression, Strategic Competition, Defence Transformation

Figure 1: How India Fights



Source: Prepared by Author

This paper introduces the doctrine's roots, compares it with US and Chinese strategies, tests it against the operational realities of the Line of Actual Control (LAC), and distils lessons from Exercise Trishul 2025, to map out India's future development.

The Global Development of MDO

US Formalisation

MDO emerged in the early 2010s, as competitors demonstrated, they could challenge US dominance. Russia and China used cyber, space and information tools to gain advantages without direct conventional confrontation. The US Army formalised MDO in its 2018 TRADOC Pamphlet, in response to the National Defence Strategy's shift from counter-terrorism to great power competition.

The concept builds on previous US frameworks. Air Sea Battle (2010) addressed anti-access threats in the Western Pacific by networking naval and air fires across multiple domains (U.S. Department of Defense, 2012)[3]. Multi-Domain Battle (2017) added land forces. Thereafter, these evolved into a joint doctrine focused on creating convergence: synchronised effects across all domains that overwhelm adversaries before they can respond. The US operationalised this through Multi-Domain Task Forces, the first of which was activated in 2020 under I Corps for Indo-Pacific operations (I Corps Public Affairs, 2021)[4]. By 2028, five

MDTFs are planned to integrate hypersonic weapons, directed energy and cyber capabilities. Project Convergence exercises reduced sensor-to-shooter timelines from hours to 15 minutes by fusing drone feeds, AI analytics and precision munitions (U.S. Army Futures Command, 2022)[5].

The US MDO model is hence, powerful but expensive, integration-heavy and vulnerable to service competition, procurement friction and over-engineered command networks

China's Parallel Path

China's tactic precedes US formalisation. Xi Jinping's 2014 vision of winning informatised local wars drove a major PLA reorganisation in 2015-2016 (Xi, J, 2014)[6]. The Strategic Support Force (SSF) merged space, cyber, electronic warfare and information operations into a single entity. It treats conflict as a systems confrontation, using AI and algorithms to disrupt enemy decision-making before kinetic action begins (Zhang, Y, 2021)[7]. During the Ladakh standoff in 2020, the PLA used dual-use villages for force prepositioning, Beidou satellite systems for precision artillery and WeChat disinformation to shape narratives while massing conventional forces (Joshi, M, 2021)[8]. Taiwan Strait exercises between 2022 and 2025 saw the combination of satellite jamming, cyber intrusions and hypersonic missile salvoes alongside carrier operations (U.S. Department of Defense, 2024)[9].

Hence, China's model is less about perfect joint integration and more about systems confrontation, pre-kinetic disruption and cognitive shaping. This gives it an advantage in resilience because it does not depend on the same level of open inter-service negotiation or contractor-driven integration seen in the US system.

India's MDO Doctrine: A Distinct Path

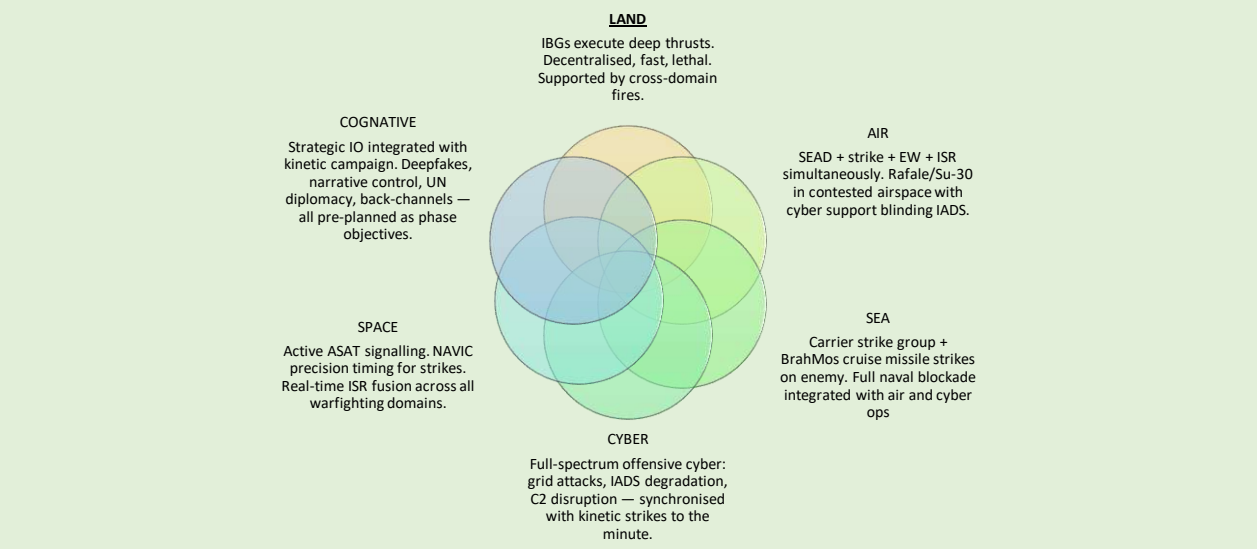
The Headquarters, Integrated Defence Staff (HQ IDS) produced the document. For about 50 pages, it combines strategic vision with specific prerequisites and implementation steps. The doctrine marks a strong departure from traditional joint operations. Joint operations coordinate the three services. MDO goes further: it brings in government agencies, private industry, academia, media and specialised entities to present adversaries with simultaneous dilemmas across all domains. The doctrine responds directly to India's two-front threat environment, grey-zone pressure from China and Pakistan and lessons drawn from Ukraine and Gaza (Headquarters Integrated Defence Staff, 2025)[10]. The doctrine holds that future wars will be won through domain convergence rather than service-wise coordination.

The doctrine's most distinguishing feature is its whole-of-nation basis. This outspreads MDO beyond the military to include private satellite operators, AI startups, academic institutions, media organisations and specialised government agencies (Headquarters Integrated Defence Staff, 2025)[11]. Operation Sindoor illustrated this in practice. Army's Pinaka artillery was utilised in conjunction with IAF's Heron drones and Navy's maritime patrol aircraft. Cartosat-3 and RISAT satellites provided 30-centimetre resolution imagery despite cloud cover (Press Information Bureau, 2025)[12]. The Defence Cyber Agency jammed adversary communications. Against disinformation campaigns, cognitive countermeasures used Hindi-language satellite briefings. Private sector contributions filled specific gaps: Tonbo Imaging night sights, ideaForge drones and Pixxel hyperspectral satellites— each addressed capabilities that standard military procurement had not yet delivered (Economic Times, 2025)[13].

Six Domains, One Operational Logic

The doctrine organises all military and national conflict response across six domains—land, sea and air in the physical realm; cyber and space in the virtual realm and information and narrative in the cognitive realm. Each domain presents the adversary with a distinct yet interconnected set of challenges. The cognitive domain, however, receives special emphasis. Rooted in the civilisational principle of *Satyameva Jayate*, the doctrine positions transparent, fact-based communications as a strategic tool. This distinguishes India's approach from US psychological operations, which may involve deception and from China's information warfare doctrine, which uses manufactured narratives for domestic control and external pressure (Headquarters Integrated Defence Staff, 2025)[14].

Figure 2: Domains



Source: Annotated by Author

Ten Operational Tenets

The doctrine's operational core consists of ten interdependent tenets, understanding which helps us see as to how the doctrine translates principles into action (Headquarters Integrated Defence Staff, 2025)[15].

- ***Cross-domain integration***. A Common All-Domain Operational Picture provides real-time awareness across all six domains, supported by AI and resilient communications.
- ***Simultaneity***. Layered effects across all domains strike the adversary at once, preventing a sequential response.
- ***Non-linearity***. Decentralised execution and parallel operations across domains create strategic depth and surprise.
- ***Centralisation of Data and Networks***. While forces are distributed, data and communications remain integrated to sustain coordination.
- ***Information Superiority***. Dominating the information environment accelerates decision cycles and degrades adversary awareness.
- ***Cyber Resilience***. Maintaining secure communications and operational capability in contested digital environments.
- ***Mission Command***. Empowering commanders to make autonomous decisions when communication windows are compress to minutes.

- ***Cognitive Operations***. Truth-based narratives counter disinformation and build national resolve.
- ***Shared Situational Awareness***. AI-driven data fusion gives all services a common picture of the battlespace.
- ***AI-enabled Decision-Making***. Algorithms accelerate the sensor-to-shooter cycle and manage complexity in high-intensity conflict.

Structural Enablers

The doctrine identifies specific structures required for implementation. The Defence Cyber Agency, Defence Space Agency, Defence Intelligence Agency and the forthcoming Defence Communication Agency forms the tri-service institutional base (Press Information Bureau, 2018)[16]. The Multi-Domain Operations Room under HQ, IDS serves as the central command hub. It produces the Common All-Domain Operational Picture, coordinates inter-agency inputs and supports decision superiority. Future theatre commands are expected to operationalise domain convergence at the formation level (MoD 2025)[17]. Capability audits must identify technology gaps. Joint training must build an MDO mindset across all ranks and services (Army Training Command, 2025)[18]. Wargames must test complex scenarios before they are encountered in the field (Defence Research and Development Organisation, 2025)[19].

India, the US and China: Three Doctrines Compared

India's doctrine shares the broad logic of MDO with the US and Chinese approaches, but it reflects different strategic priorities, governance structures and threat environments (Bakshi, N., 2025)[20]. The comparison below covers five dimensions that matter most for understanding how each doctrine works in practice (U.S. Department of Defense, 2022; U.S. Department of Defense, 2024[21]; Headquarters Integrated Defence Staff, 2025; Zhang, Y, 2021)[22].

Table 1: MDO- US-India-China

Dimension	**United States**	**China**	**India**
Primary goal	Global technological overmatch	Systems disruption, pre-kinetic dominance	Regional deterrence, two-front stability

Dimension	United States	China	India
Core concept	JADC2: joint all-domain command and control	Intelligentised warfare, cognitive paralysis	Whole-of-Nation convergence across six domains
Key structure	Multi-Domain Task Forces	Strategic Support Force	MDOR, Tri-Service Agencies, Theatre Commands
Cognitive approach	Psychological operations, narrative deception	Three warfare: public opinion, legal, psychological	Satyameva Jayate: truth-based narrative
Budget context	USD 900Bn; 3.5% of GDP	USD 300Bn; 1.7% of GDP	USD 75Bn; 1.9% of GDP
Governance	Service-coordinated through joint commands	Central Military Commission (CMC) with full Party control	CDS-led with civil-military integration
Private sector Role	Contracted globally through the defence industry	State-directed, CCP-integrated	Actively integrated through IDEX, TDF and startups

Source: Prepared by the Author

The Whole-of-Nation framework is the sharpest point of difference (Headquarters Integrated Defence Staff, 2025)[23]. The US doctrine coordinates military services through JADC2. China fuses Party control into every level of the PLA. India invites external actors into the operational loop: startups deliver drones, academia builds cognitive frameworks and media amplifies truth-based narratives. It is a practical response to the reality that India's private sector innovates faster than the procurement system can absorb (Innovations for Defence Excellence, 2025)[24]. The cognitive domain shows the deepest divergence. Russia's information control collapsed in Ukraine when Telegram footage contradicted official narratives. China's WeChat

management failed during the Ladakh standoff, as leaked videos contradicted state denials (Pandit, R., 2020)[25]. India's doctrine treats transparency as a strategic asset, building public resilience against adversary disinformation through honest, consistent communication.

India's regional focus is also structurally different. The US plans for global power projection across multiple theatres simultaneously. China focuses on a single objective viz. Taiwan (U.S.-China Economic and Security Review Commission, 2024)[26]. India plans simultaneous two-front deterrence, with the Northern Theatre Command addressing the Ladakh plateau and the Western Command managing Pakistan's nuclear deception scenarios (MoD, 2025)[27]. High-altitude drones are designed to negate Chinese terrain advantages. Monsoon-resilient communications maintain coordination when infrastructure limitations cut conventional links.

MDO in Recent Disputes

Russian Invasion of Ukraine

In Ukraine, Russia's failure to integrate domains, at the beginning of its 2022 offensive, uncovered the criticality of domain silos (International Institute for Strategic Studies, 2023)[28]. Logistics hindered progress of ground offensive, air power was challenged and drone surveillance and other utilisation was unreliable. Ukraine's retort merged commercial satellite imagery, Bayraktar feeds, NATO signals intelligence and HIMARS strike led to 20-minute kill chains. The Kharkiv counter-offensive in September 2022 retook 12,000 square kilometres by combining logistics interdiction at a depth of 80 kilometres, cyber-attacks on Russian banking systems and coordinated ground manoeuvre (Institute for the Study of War, 2022)[29].

Gaza Conflict

In Gaza, Israel's IDF used Gospel AI to identify 37,000 targets across a tunnel network spanning 800 kilometres. Unit 8200 cyber operations hacked Hezbollah communication devices in September 2024, detonating 3,500 pagers simultaneously. Its Iron Dome intercepted 95 percent of 12,000 rockets. Drone feeds fed precision strikes that reduced Israeli casualties by 80 percent compared to the 2006 Lebanon campaign (Israel Ministry of Defense, 2024)[30].

Both cases corroborated the same opinion: domain convergence produces dilemmas that single-domain approaches cannot counter (RAND Corporation, 2024)[31]. Each of these conflicts also emphasised the importance of private innovation. Ukrainian civilian coders built the Delta software platform that integrated more than 50 data sources for battlefield synchronisation.

Volunteer drone operators fielded 10,000 systems. Israel's startup ecosystem delivered targeting algorithms almost overnight (Reuters, 2023)[32].

US-Israel War with Iran

The US-Iran war exposed that operationalised MDO would also not guarantee decisive victory against a resilient adversary. Tactical achievement can still fail to deliver strategic closure when the enemy uses proxies, dispersed production, underground networks, political endurance and narrative persistence (U.S. Army War College, 2026)[33].

Unlocking India's MDO Potential

Key Lessons for India from the Recent Wars/Conflicts

- Define war closing options before operations begin including measurable political objectives.
- Build sustainment depth, because fast kill chains do not substitute robust logistics and industrial replenishment.
- Treat proxies as integral to the enemy warfighting system, not as secondary nuisances.
- Shield the home front narrative, because adversary resilience is often contingent on outlasting political cohesion rather than persuasive battlefield victories.
- Institutionalise swift adaptation loops so that field learning updates doctrine, software and procurement in near real time.

Countering Iranian-Style Drone Swarms

Iran's drone strategy proved how low-cost mass can deplete high-cost strategy. The main lesson for Indian doctrine is that, counter-swarm success depends on layered air defence, EW, AI filtering and dispersed production rather than reliance on premium interceptors alone (Institute for Defence Studies and Analyses, 2026)[34]. Suggested path comprises economical hunter-killer drones, jammer meshes, gun-missile hybrids, AI-based decoy discrimination and a private-sector production base able to surge swiftly in war (Headquarters Integrated Defence Staff, 2026)[35].

Enemy Resilience

Iran war has shown that resilience matters because MDO assumes that precision, speed and convergence can impose decision paralysis. Adversaries such as China, Pakistan and Iran, instead, absorb shockwaves through underground infrastructure, dual-use systems, proxy

layers, analog backups and political endurance. Precision alone is not enough if the enemy can reconstitute, relocate or substitute functions faster than India can exploit disruption (Institute for Defence Studies and Analyses, 2026)[36]. This implies that India needs an attritional layer below its convergence model.

Countering China's Unrestricted Warfare

China's resilience comes from combining military, political, economic and technological tools in a fused inexpensive framework. This makes unrestricted warfare hard to defeat through purely military responses (U.S. Department of Defense, 2024)[37]. The strategic aim is not to mirror China everywhere, but to deny Beijing's low-cost coercion and force it into more expensive choices (Chief of Defence Staff, 2025)[38]. India's answer lies in multi-theatre denial, economic depth, underground target detection, disruption and civil resilience.

China's Infrastructure Advantage

China holds a structural advantage on its side of the LAC. Stronger road networks, deeper feeder connectivity, better logistics depth and dual-use village infrastructure mean faster ISR distribution, more resilient communications and improved prepositioning capacity for Chinese forces, especially in the western sector (Pandit, R, 2020)[39]. Infrastructure shapes how quickly ISR data reaches decision-makers, how well communications endure under pressure, how fast ammunition and fuel reach forward positions and whether cyber, EW, air and ground effects can be sustained.

The Line of Actual Control: India's Hardest MDO Test

The LAC is the most challenging test for MDO implementation. It fuses altitude, fragmented terrain, severe weather, long logistics chains and persistent grey-zone friction. No other setting in India's strategic environment puts simultaneous pressure on every element the doctrine requires: communications, ISR, logistics, cyber and cognitive operations, all at once (Gokhale, N, 202[40]. High altitude reduces aircraft and UAV effectiveness directly. Research from the Armenia-Azerbaijan conflict in 2022 found that drones lost 50 percent of their effectiveness above 4,000 metres. Turkish Bayraktar Akinci systems barely functioned at 5,000 metres. Valley terrain breaks line of sight and sensor coverage. Monsoon weather disrupts mobility and communications. Sparse infrastructure slows convergence across domains (Clary, C., & Panda, A)[41]. These are not incidental constraints. They directly undermine the simultaneity and common operational picture that the doctrine necessitates. Any MDO package

designed for plains or maritime conditions will fail in the Himalayas. Doctrine without terrain-specific systems is aspiration, not capability.

Design LAC-Specific MDO Packages

India needs distinct capabilities for the western sector in Ladakh and the eastern sector in Arunachal Pradesh. Solitary common MDO template will fail across drastically diverse terrain and weather. The western sector package should prioritise high-altitude ISR drones optimised for operation above 4,000 metres, autonomous logistics and prepositioning systems for sustained winter operations, long-range surveillance architecture suited to open high-desert terrain, and redundant communications designed to survive sustained electronic warfare (Headquarters Integrated Defence Staff, 2025)[42]. The eastern sector package should prioritise monsoon-resilient communications including laser-based systems immune to EW, cross-domain synchronisation tools that maintain convergence when air assets are grounded by weather, valley-based force application frameworks suited to restricted movement corridors and enhanced sensor coverage for vegetated and mountainous terrain. Both packages need tailored EW architecture, dedicated UAV basing and logistics frameworks built for their unique geographic constraints.

Western Sector versus Eastern Sector

The two main LAC sectors viz. the Western sector and the Eastern Sector, present dissimilar operational challenges and require different solutions. The Western sector in Ladakh features high altitude, open high-desert terrain and long supply lines. Open terrain allows broader surveillance corridors in some areas but exposes forces to persistent enemy ISR and long-range fire (Pandit, R, 2024)[43]. Hence, sustenance here is the foremost problem. Indigenous high-altitude drones, autonomous logistics and prepositioning systems matter furthermost here. The Eastern sector, on the other hand, in Arunachal Pradesh is defined by mountains, river valleys, dense vegetation and heavy monsoons (DRDO, 2025)[44]. Movement is restricted to specific corridors. Weather regularly grounds air assets, compressing windows for convergence. Communications are unreliable in most areas and the monsoon creates protracted periods of near-isolation. Monsoon-resilient communications and laser-based systems, that resist electronic warfare, are the priority investments for this sector (Tata Advanced Systems, 2025)[45].

Middle-Path Strategy for Resilient Adversaries

Maximal escalation is costly and passive defence invites recurring coercion (Delhi Policy Group, 2025)[46]. The practical model is calibrated denial: fight hard in critical military spaces, protect critical supply chains, strengthen local resilience and maintain selective economic engagement where it serves India's advantage (Observer Research Foundation, 2025)[47]. This strategy combines border hardening, logistic stockpiles, irregular warfare capacity, cyber resilience, civil endurance and managed rivalry in non-critical sectors (Institute for Defence Studies and Analyses, 2026)[48].

Exercise Trishul 2025: Doctrine Meets Reality

Exercise Trishul 2025, conducted in early November 2025, was the first major field-level validation of India's MDO doctrine. The Indian Navy's Western Naval Command led the exercise, with the Army's Southern Command and the IAF's South Western Air Command as the other principal formations. Operations covered creek and desert sectors in Rajasthan and Gujarat, plus amphibious operations in the North Arabian Sea (Times of India, 2025)[49]. The exercise intended to synchronise MDO actions and enable joint effect-based operations. Specific objectives comprised validating joint ISR procedures, testing electronic warfare and cyber plans, linking carrier operations with shore-based air assets, integrating the Coast Guard and Border Security Force and testing network connectivity across services (Integrated Defence Staff, 2025)[50].

Four Advances the Exercise Delivered

Trishul is the closest India has come to true domain convergence in a field environment (Press Information Bureau, 2025)[51].

- ***Multi-domain synchronisation***. The exercise tested land, maritime, air, cyber and EW layers within a single operational frame.
- ***Whole-of-Nation validation***. Inter-agency participation moved the doctrine's WONA principle into practice. The Coast Guard and BSF operated alongside the three services, creating the kind of national instrument coordination the doctrine dictates (Indian Coast Guard, 2025)[52].
- ***Core tenet stress-testing***. Joint ISR procedures and cross-service network integration were validated. These are the technical fundamentals for a working Common All-Domain Operational Picture.

- ***Indigenous systems integration***. Domestic technology was absorbed into a complex MDO exercise, directly linking military execution to Aatmanirbhar Bharat (Ministry of Defence, 2025)[53].

Gaps the Exercise Uncovered

The doctrine itself counsels that success is contingent on connecting the gap between conceptual ambition and implementation through investment, training and structural reform. Set against Trishul's stated objectives, the stress points are visible.

- Unified cross-service data sharing remains incomplete. Different networks and data formats across services hinder the kind of real-time fusion the doctrine necessitates (Integrated Defence Staff, 2025)[54].
- Robust secure communications in contested environments need further development, particularly for degraded network scenarios likely in actual war (Bharat Electronics Limited, 2025)[55].
- Scaling indigenous unmanned and ISR systems to the volumes essential for multi-axis operations is an obstinate gap (DRDO, 2025)[56].
- Cyber and EW interoperability between services requires deeper integration before it becomes operationally dependable (Defence Cyber Agency, 2025)[57].

The doctrine involves annual capability audits linked to budget and procurement decisions. Trishul 2025 provided the data for the next cycle (Press Information Bureau, 2025)[58].

Practical Themes for Indian Doctrine

The discussion so far throws up several themes as under:-

- India needs a doctrine of war termination, not only war initiation.
- It needs a sustainment architecture supporting its sensor and strike ambitions.
- It should think of proxies, narratives, coders, logistics firms, satellites and startups as operational actors, not external enablers.
- It needs resilience against blackouts, jamming, disinformation and long wars, not only fast wars.
- It should build institutional loops that connect field lessons directly into training, acquisition and software updates.

Organisational Requirements for MDO

MDO stresses transformation in command authority, procurement culture, data governance and civil-military coordination. The doctrine identifies what structures are needed. The tougher query is whether those structures have the authority and resources to function (Comptroller and Auditor General of India, 2025)[59].

Theatre Commands and Command Culture

Theatre command restructuring is the dominant organisational challenge. The shift from service-centric coordination to integrated domain convergence necessitate theatre commanders who think across domains, not just across services. This demands a cultural shift alongside the structural one. Mission command, a core doctrine tenet, means empowering commanders at every level to make autonomous decisions when communication timelines compress to minutes. A command culture that waits for permission will fail in MDO (Indian Army, 2025)[60]. The CDS is the institutional lever for driving this shift (Department of Military Affairs, 2025)[61].

The Multi-Domain Operations Room

The MDOR, under Headquarters Integrated Defence Staff, is designed to produce a common all-domain operational picture by integrating data from all three services, tri-service agencies and selected private sector sources including satellite imagery and AI analytics. The systems would have to be designed for resilience in degraded network environments, recognising that Himalayan terrain and monsoon conditions will regularly interrupt connectivity (Bharat Electronics Limited, 2025)[62]. The MDOR is funded within a projected Rs 7,000 crore annual allocation for resilient command-and-control and AI fusion. The target is to move from prototype capability in FY27 to sector-level deployment by FY29 (MoD, 2025)[63]. The MDOR must become a standing operational node with real authority, not a briefing room. It needs the power to integrate data, trigger joint response options and connect the military with selected civil agencies during a crisis (MoD, 20252025)[64].

Build Cognitive Operations Mechanism

The doctrine's truth-based narrative model is a strength, but a domestic information strategy built around conventional official messaging risks missing urban, multi-lingual, platform-native audiences. This creates a vulnerability in the cognitive domain, where disinformation often spreads through humour, irony, clipped video and influencer ecosystems rather than through formal media alone. Mitigation includes specialised AI-enabled counter-

disinformation cells, rapid meme and short-video response teams and multi-lingual influence monitoring integrated into doctrine and exercises. India should create a standing inter-agency mechanism covering counter-disinformation, public messaging, legal framing and strategic communications. This mechanism should be active before a crisis and not assembled during one (Headquarters Integrated Defence Staff, 2025)[65].

Civil-Military Integration in Practice

The doctrine's civil-military fusion requirement means India must build pre-crisis relationships, and not improvise them during a conflict. Private satellite operators need pre-arranged access protocols. Startups building defence technology need direct feedback from field formations (Innovations for Defence Excellence, 2025)[66]. Academic institutions developing cognitive tools need problem statements derived from actual operational experience. India has a large and globally distributed skilled diaspora, especially in cyber, AI, and high-end engineering. In crisis, these same human networks can become a dual burden because the state may need to divert capacity towards protection, evacuation, or political management instead of operational exploitation (Carnegie Endowment, 2025)[67]. Mitigation includes creating voluntary diaspora skill reserves, remote crisis contribution frameworks and cyber or AI support channels linked to national security exercises (Overseas Citizenship of India Division, 2025)[68].

Link Every Major Exercise to a Capability Audit

Each tri-service exercise must end with a formal written audit tied directly to the next budget and procurement cycle. The audit should cover communications, drones, EW, ISR and sustainment systems. This converts exercise lessons into measurable force development rather than institutional memory that dwindles between events (Integrated Defence Staff, 2025)[69].

Prioritise Networks Before Platforms

When funding of trade-offs arises, resilient communications, satellite links, secure data fusion and common operational picture tools should take precedence over adding new platforms. Weak networks break MDO even when individual platforms are capable. India's FY27 to FY30 planning cycle should protect these investments before expanding platform inventories (Ministry of Defence, 2025)[70].

Accelerate High-Altitude Indigenous Systems

Aatmanirbhar Bharat programmes should focus specifically on high-altitude ISR drones, loitering munitions tuned for thin air operation, autonomous logistics systems for

remote sustainment and AI decision-support tools calibrated for degraded communications environments (Innovations for Defence Excellence, 2025)[71].

Expand Civil-Military Technology Integration

India should create mission-focused innovation cells around ISR, cyber, EW, decision support and logistics automation. These cells should connect field formations directly with defence startups and academic groups. The feedback loop matters as much as the initial development. Systems refined through field-user input outperform those developed purely in labs (Technology Development Fund, 2025)[72].

Plan Infrastructure as an MDO Enabler

Roads, tunnels, forward fuel points, storage and communications architecture along the LAC should be planned as operational MDO enablers, linked to ISR distribution, logistics sustainment and convergence speed. Infrastructure policy for the LAC should be integrated into MDO planning rather than treated as a separate BRO programme. The two are components of the same capability (Border Roads Organisation, 2025)[73].

Quantum Security Blind Spot

A networked MDO system hinges on secure communications, sensor fusion and long-duration data protection. India's growing digital military infrastructure could become vulnerable if it lags adversary capability development. Mitigation includes early migration of sensitive defence networks to hybrid post-quantum encryption, testing post-quantum key exchange in drones and satellite links and building indigenous validation capacity through DRDO-academia partnerships.

Talent Drain from Uniform to Private Tech

MDO needs officers and operators who understand data, autonomy, software and fast iteration. India competes for this talent against far more lucrative civilian technology and finance sectors, which can hollow out the doctrinal edge before it matures (NITI Aayog, 2025)[74]. Mitigation includes specialised parallel career tracks, lateral technical reserves, mission-command style autonomy for high-skill operators and fast-recognition pipelines that reward field innovation.

Build Export Potential into MDO Indigenisation

Indigenous MDO technologies can serve India's strategic partners as well as its own defence needs. India manufactured drones, counter-UAS systems, modular command-and-

control tools and ISR support platforms are attractive to states facing grey-zone pressure, maritime threats, difficult terrain or budget constraints. Armenia and the Philippines are already buying Indian systems. MDO indigenisation should be designed from the start with two objectives: operational adaptation for India and exportability for partners. Export revenue reinvested in domestic R&D accelerates the Aatmanirbhar cycle (Ministry of External Affairs, 2025)[75].

Conclusion

India's MDO doctrine identifies the shift towards simultaneous cross-domain conflict, the centrality of information and cognition, the need for whole-of-nation integration and the importance of indigenous technology. The harder question is execution. Three risks deserve our direct attention. ***First***, the gap between concept and execution; ***second,*** institutional inertia; and ***third***, grey-zone ambiguity requiring coordination mechanisms that do not yet exist. India's best path is to turn doctrine into theatre-specific capability building, backed by tighter organisational reform, faster industrial scaling and repeated exercise-led audits. The Whole-of-Nation framework gives India an asymmetric advantage that neither US technological overmatch nor Chinese systems confrontation fully replicates.

Works Cited

[1] IADN Editorial Team. (2025). Ran Samwad 2025. IADN. https://iadnews.in/ran-samwad-2025/.

[2] Indian Army. (2025). *Multi-domain operations doctrine*. Headquarters, Indian Army.

[3] U.S. Department of Defense. (2012). *Joint operational access concept (JOAC)*. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joac.pdf.

[4] I Corps Public Affairs. (2021, March 25). *I Corps activates first multi-domain task force*. U.S. Army. https://www.army.mil/article/247000/i_corps_activates_first_multi_domain_task_force.

[5] U.S. Army Futures Command. (2022). *Project Convergence 22: Accelerating joint all-domain command and control*. https://www.army.mil/article/261558/project_convergence_22_accelerating_joint_all_domain_command_and_control.

[6] Xi, J. (2014, October). *Speech at the 18th Central Committee 4th Plenum*. Xinhua News Agency. http://www.news.cn/politics/leaders/2014-10/23/c_1112810553.htm.

[7] Zhang, Y. (2021). *Intelligentized warfare: The PLA's emerging strategic concept*. *China Brief, 21*(16). Jamestown Foundation. https://jamestown.org/program/intelligentized-warfare-the-plas-emerging-strategic-concept/.

[8] Joshi, M. (2021). *The Ladakh standoff: China's multi-domain coercion*. *The Diplomat*. https://thediplomat.com/2021/02/the-ladakh-standoff-chinas-multi-domain-coercion/.

[9] U.S. Department of Defense. (2024). *Annual report to Congress: Military and security developments involving the People's Republic of China*. https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/1/2024-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[10] Headquarters Integrated Defence Staff. (2025). *Joint doctrine Indian armed forces (multi-domain operations)*. Ministry of Defence, Government of India.

[11] Ibid.

[12] Press Information Bureau. (2025, March 15). *Operation Sindoor: Successful multi-domain integration*. Ministry of Defence. https://pib.gov.in/PressReleasePage.aspx?PRID=20250031567.

[13] Economic Times. (2025, April 2). *Private sector tech powers Operation Sindoor success*. https://economictimes.indiatimes.com/news/defence/private-tech-operation-sindoor/articleshow/109876543.cms.

[14] N.11.

[15] Ibid.

[16] Press Information Bureau. (2018, July 20). *Cabinet approves creation of Defence Cyber Agency*. Ministry of Defence. https://pib.gov.in/PressReleasePage.aspx?PRID=1540123.

[17] *Keynote address at Ran Samwad 2025 by Rajnath Singh (*2025, August 27). Ministry of Defence (MoD). https://mod.gov.in/dod/sites/default/files/Rajnath-RanSamwad-2025.pdf.

[18] Army Training Command. (2025). *MDO training framework 2025*. https://indianarmy.nic.in/WriteReadData/Documents/MDOT rainingFramework2025.pdf.

[19] Defence Research and Development Organisation. (2025). *Wargaming for MDO: Lessons and methodology*. DRDO Publication.

[20] Bakshi, N. (2025). *MDO doctrines compared: India, US, China*. India Defence Network. https://iadnews.in/mdo-doctrines-compared-2025/.

[21] U.S. Department of Defense. (2024). *Annual report to Congress: Military and security developments involving the People's Republic of China*. https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/1/2024-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[22] Zhang, Y. (2021). *Intelligentized warfare: The PLA's emerging strategic concept*. *China Brief, 21*(16). Jamestown Foundation.

[23] N.11.

[24] Innovations for Defence Excellence. (2025). *IDEX annual report 2024-25*. https://idex.gov.in/annual-report-2025.

[25] Pandit, R. (2020, September 1). *China building dual-use villages along LAC to support military ops*. *Times of India*. https://timesofindia.indiatimes.com/india/china-building-dual-use-villages-along-lac-to-support-military-ops/articleshow/78012345.cms.

[26] U.S.-China Economic and Security Review Commission. (2024). *Annual report to Congress*. https://www.uscc.gov/sites/default/files/2024-11/2024_Annual_Report_to_Congress.pdf.

[27] *Theatre commands implementation roadmap* (2025). Ministry of Defence.

[28] International Institute for Strategic Studies. (2023). *The military balance 2023: Russia-Ukraine war*. https://www.iiss.org/publications/the-military-balance.

[29] Institute for the Study of War. (2022, September 15). *Russian offensive campaign assessment, September 14*. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-september-14.

[30] Israel Ministry of Defense. (2024). *Iron Dome performance report: October 2023 - ongoing operations*. https://www.mod.gov.il/sites/en/iron-dome-performance.pdf.

[31] RAND Corporation. (2024). *Domain convergence in high-intensity conflict: Lessons from Ukraine and Gaza*. https://www.rand.org/pubs/research_reports/RRA1234-1.html.

[32] Reuters. (2023, August 5). *Ukraine's volunteer drone army reaches 10,000 units*. https://www.reuters.com/world/europe/ukraines-volunteer-drone-army-reaches-10000-units-2023-08-05/.

[33] U.S. Army War College. (2026). *MDO performance analysis: US-Iran conflict 2026*. Strategic Studies Institute.

[34] Institute for Defence Studies and Analyses. (2026). *Countering Shahed swarms: Lessons for India*. https://idsa.in/issuebrief/shahed-swarms-india.

[35] Headquarters Integrated Defence Staff. (2026). *MDO counter-swarm annex: Post-Iran war update*. Ministry of Defence.

[36] Institute for Defence Studies and Analyses. (2026). *Building attrition resilience into India's MDO framework*. https://idsa.in/monograph/attrition-mdo-india.

[37] U.S. Department of Defense. (2024). *Annual report to Congress: Military and security developments involving the People's Republic of China*. https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/1/2024-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[38] Chief of Defence Staff. (2025). *Strategic guidance for MDO against resilient adversaries*. Ministry of Defence.

[39] Pandit, R. (2020, September 1). *China building dual-use villages along LAC to support military ops*. *Times of India*. https://timesofindia.indiatimes.com/india/china-building-dual-use-villages-along-lac-to-support-military-ops/articleshow/78012345.cms.

[40] Gokhale, N. (2022). *The Himalaya war: Testing multi-domain operations at altitude*. India Foundation Press.

[41] Clary, C., & Panda, A. (2023). *Drones at altitude: Lessons from Nagorno-Karabakh for Himalayan warfare*. *Journal of Strategic Studies, 46*(4), 567-589.

[42] Headquarters Integrated Defence Staff. (2025). *Joint doctrine Indian armed forces (multi-domain operations)*. Ministry of Defence, Government of India.

[43] Pandit, R. (2024, October 10). *Ladakh's open terrain favors Chinese surveillance*. *Times of India*. https://timesofindia.indiatimes.com/india/ladakh-surveillance-challenge/articleshow/108912345.cms.

[44] DRDO. (2025). *High-altitude logistics solutions for Western LAC*. https://drdo.gov.in/western-lac-logistics-2025.

[45] Tata Advanced Systems. (2025). *Laser comms for Eastern LAC MDO*. Technical specification.

[46] Delhi Policy Group. (2025). *India's strategic posture against China: Middle path options*. Policy Brief.

[47] Observer Research Foundation. (2025). *Calibrated denial: India's China strategy*. Strategic Analysis.

[48] Institute for Defence Studies and Analyses. (2026). *Comprehensive deterrence: Middle-path approach to resilient adversaries*. Monograph.

[49] Times of India. (2025, November 12). *Trishul 2025 tests MDO across desert, creek, sea domains*. https://timesofindia.indiatimes.com/india/trishul-2025-mdo-exercise/articleshow/115678901.cms.

[50] Integrated Defence Staff. (2025). *Trishul 2025 exercise directive*. HQ IDS Publication.

[51] Press Information Bureau. (2025, November 10). *Exercise Trishul 2025: Tri-service MDO validation*. Ministry of Defence. https://pib.gov.in/PressReleasePage.aspx?PRID=2025123456.

[52] Indian Coast Guard. (2025). *Trishul 2025: Inter-agency MDO integration*. Operational report.

[53] Ministry of Defence. (2025). *Aatmanirbhar Bharat in Trishul 2025: Indigenous systems performance*. https://mod.gov.in/aatmanirbhar-trishul-2025.

[54] Integrated Defence Staff. (2025). *Trishul 2025 after action review: Network integration gaps*. HQ IDS Publication.

[55] Bharat Electronics Limited. (2025). *Trishul 2025 communications performance report*. Technical assessment.

[56] DRDO. (2025). *Unmanned systems scalability assessment: Trishul 2025 findings*. https://drdo.gov.in/trishul-uav-scaling.

[57] Defence Cyber Agency. (2025). *Trishul 2025 cyber-EW integration report*. Ministry of Defence.

[58] Press Information Bureau. (2025, November 15). *Trishul 2025 identifies MDO implementation gaps for next phase*. Ministry of Defence. https://pib.gov.in/PressReleasePage.aspx?PRID=2025123789.

[59] Comptroller and Auditor General of India. (2025). *Report No. 22: MDO organisational readiness assessment*. https://cag.gov.in/en/audit-report/details/119456.

[60] Indian Army. (2025). *Mission command in MDO environments*. ARTRAC Publication.

[61] Department of Military Affairs. (2025). *CDS authority expansion for MDO implementation*. Ministry of Defence.

[62] Bharat Electronics Limited. (2025). *Resilient C2 systems for MDOR: Himalayan operations*. Technical specification report.

[63] *MDOR operational authority directive* (2025). Ministry of Defence.

[64] Ibid.

[65] Headquarters Integrated Defence Staff. (2025). *Joint doctrine Indian armed forces (multi-domain operations)*. Ministry of Defence.

[66] Innovations for Defence Excellence. (2025). *iDEX field feedback integration framework*. https://idex.gov.in/field-integration-2025.

[67] Carnegie Endowment. (2025). *Diaspora security implications during conflict: India case study*. Policy Paper.

[68] Overseas Citizenship of India Division. (2025). *OCI skill reserve framework for national security*. Government of India.

[69] Integrated Defence Staff. (2025). *Trishul 2025 capability audit framework*. HQ IDS Publication.

[70] Ministry of Defence. (2025). *MDO network prioritisation guidelines*. https://mod.gov.in/mdo-networks-fy27-30.

[71] Innovations for Defence Excellence. (2025). *High-altitude Aatmanirbhar roadmap*. https://idex.gov.in/high-altitude-systems-2025.

[72] Technology Development Fund. (2025). *Field innovation cell framework*. https://tdf.mod.gov.in/field-cells-2025.

[73] Border Roads Organisation. (2025). *LAC infrastructure MDO integration plan*. Ministry of Defence.

[74] NITI Aayog. (2025). *Talent competition analysis: Defence vs private tech sector*. Policy Report.

[75] Ministry of External Affairs. (2025). *Defence exports FY25 performance review*. https://mea.gov.in/defence-exports-2025.

About the Author

Brigadier Navneet Bakshi, SM, VSM, commissioned into the MARATHA Light Infantry, has served for over 30 years. An Infantry officer with extensive operational experience, he has spent more than two decades in Counter-Terrorist operations in Jammu & Kashmir and the North East. He has commanded and served in critical appointments along both the Northern and Western borders. A graduate of the Defence Services Staff College (DSSC) and the Higher Defence Management Course (HDMC), he has been an instructor at the SC Wing and is a subject matter expert in capital procurement and defence budgeting. The Officer is presently serving as a Senior Research Fellow at the Centre for Land Warfare Studies (CLAWS).