Issue Brief

August 2025
No : 454

War Without Borders: Redefining India's Battlefield Geometry in the Age of Digital Disruption

Lt Gen A B Shivane,
PVSM, AVSM, VSM (Retd)

War Without Borders: Redefining India's Battlefield Geometry in the Age of Digital Disruption

Lt Gen A B Shivane, PVSM, AVSM, VSM (Retd)

Digital war is the new frontline; those who control the code will cripple the command. India must strike first in this invisible domain where the silent battles begin

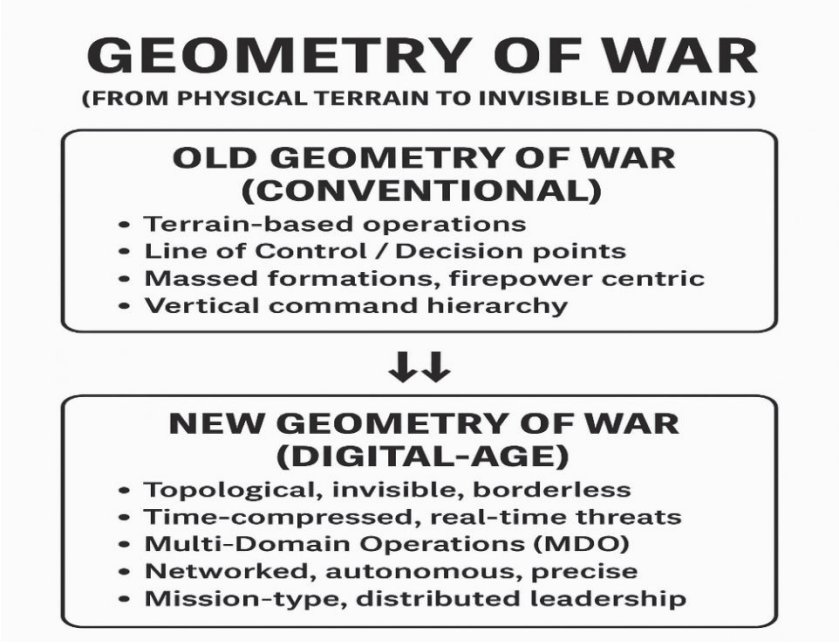
Introduction: Wars are Changing, So Must the Military

India's future wars will not begin with a declaration nor wait for tanks to cross a border— the next conflict could start with a power grid failure in a border town, a blackout in a command centre, or a swarm of drones overwhelming radar cover over Northern or Western borders. As cyber attacks, autonomous systems, and precision munitions rewrite the playbook, India must confront a hard truth: our conventional notions of warfighting, built around physical mass and geographic lines, are dangerously outdated. In this digital and multi-domain era, the very idea of "battlefield geometry", once defined by terrain, contact lines, and manoeuvre corridors, is being reshaped. The warzone is no longer defined by geography; it is fluid, invisible, dispersed and highly time-specific. A threat can attack in milliseconds but disappear in microseconds. In such a dynamic battlespace, size and firepower will do less to provide survivability and superiority than will resilience, redundancy and speed of recovery.

India stands at a strategic decision point— it cannot afford to be doctrinally reactive or technologically indifferent. To fight and win tomorrow's wars, the Indian defence forces must reimagine combat through the lens of invisible geometry, precision disruption, and mission continuity under digital siege.

The Collapse of Conventional Geometry

For decades, Indian operational art, be it in plains warfare or mountain combat, has been guided by physical terrain. Lines of control, decision points, IPB, threat corridors, and depth areas have dictated how formations are structured, deployed, and tasked. But this physicality no longer guarantees dominance.



The digitalisation of warfare enabled by networks, sensors, space assets, and cyber tools has unhinged the geometry of combat. The enemy can now strike deeply without entering our territory. An attack on a satellite uplink, a drone-based intrusion, or a malware implant in logistics software can degrade an entire corps-level formation without firing a bullet. Time, not terrain, has become the key variable. The physical boundaries of three-dimensional warfare no longer exists in an era of integrated multi-domain warfare (Allardice, R. and Topic, G., 2017).

More critically, the concept of "flash to bang", the time between detecting a threat and absorbing its impact, has compressed to such an extent that traditional command hierarchies struggle to respond in real time. If the adversary can compromise a battlefield management system or jam our communications at a critical moment, our combat superiority becomes irrelevant (Allardice, R. and Topic, G., 2017).

From Firepower to Precise Disruption

India's military structure and acquisition priorities have long been built around the idea of mass— more infantry, more tanks, more artillery and more platforms. But the 'era of mass' is giving way to the 'era of precision'. A small, intelligent, low-cost swarm of drones can now do what a regiment of artillery did two decades ago. A loitering munition launched from 100 kilometres away can take out a hardened target with zero troop movement or a manned airstrike (Horowitz, M.C., 2024).

Precision, not size, now defines lethality. In future battles, whichever side can detect, decide, and strike faster at the right node in the adversary's system, will have the edge. This does not mean India must abandon conventional firepower— it means that precision strike capabilities, supported by real-time intelligence and autonomous assets, must be elevated to equal doctrinal importance. Boots and tracks will matter till India has the challenges of disputed borders, but non-contact warfare (NCW) has taken an ascent which must be recognised.

⚔ Shifts in Combat Doctrine

From...	To...
Massed firepower	Precise disruption
Cold Start	Cold Strike
Theatre Command debate	Functional Domain Commands
Connectivity obsession	Survivability under denial
Linear warfare	Adaptive, modular combat units

What matters now is not how much steel you have, but how quickly you can shift from sensing to striking. ***Not a cold start but a cold strike***. This precision mindset must be hardwired into our warfighting doctrine, especially in the plains and deserts wherein open terrain favours drone warfare, and in the mountains where surgical, non-contact engagements could be game-changers (Horowitz, M.C., 2024).

Digital Vulnerability and the Myth of Connectivity

India's increasing emphasis on integrated commands, digitised networks, and high-speed communication systems is both necessary and risky. The need is more for an Indian model of integrated functional commands cyber, space, cognitive, deep strike, C5ISR, than theatre commands when physical geometry does not matter. The more connected the force, the more vulnerable it becomes to digital disruption. Every new link, whether it is a satellite

terminal, a battlefield LAN, or a GPS-fed platform, creates a new target (Allardice, R. and Topic, G., 2017).

Imagine an adversary who does not aim to destroy your tank, but disables its navigation, jams its communication, and corrupts its targeting data. The asset survives, but the mission fails. This is the nature of digital warfare—India's current approach, which still treats cyber and information warfare as adjuncts rather than core components, is inadequate (Allardice, R. and Topic, G., 2017).

The illusion that technology equals superiority is dangerous. Unless Indian forces build redundancy, rehearse fallback systems, and institutionalise recovery protocols, our most advanced systems will become our greatest weaknesses. The focus must shift from seamless connectivity to survivable networks. Fragility cannot be the default setting of India's warfighting machinery (Allardice, R. and Topic, G., 2017).

Operational Resilience: The Six Pillars of Success

In future battlespace to survive and prevail, India needs to have operational resilience and survivability. Operational planning, training, and force structure must incorporate the six practices at their most fundamental levels.

- ***Digital Immunology:*** Negligence is the root cause of most of the digital breaches: people have poor passwords, they do not update systems, and access management is lacking. In the Indian context, where cyber discipline is hardly uniform across units and services, digital hygiene comes down to the responsibility of the leadership (Allardice, R. and Topic, G., 2017).
- ***Redundancy:*** True resilience lies in not depending on any single node but multiple pathways under severe attack. Backup communications, alternate command chains, and fallback targeting protocols must be field-tested. Manual overrides and paper-based systems must be mission-certified, not ceremonial (Allardice, R. and Topic, G., 2017).
- ***Backup Practices:*** Warfighting must be rehearsed in degraded conditions with a non-cyber dependent backup process. What happens when IRNSS is denied over Ladakh? Can a brigade in the desert continue its mission with lost radio contact? Can artillery revert to manual fire calculations if digital systems fail? These are not theoretical

questions; they are operational imperatives to be put into combat training (Allardice, R. and Topic, G., 2017).

- ***Passive Denial:*** India must invest in threat simulation teams that actively test vulnerabilities of its systems. Understanding how the adversary views our digital footprints and identifying the nodes most likely to be attacked must become a standard practice (Horowitz, M.C., 2024).
- ***Digital Domination:*** Offensive cyber, space and electronic warfare units must be empowered and integrated with conventional forces. Whether disrupting enemy sensors, disabling satellites or corrupting their battlefield communication, these actions must be planned, rehearsed, and executed in real time, not just in cyber cells far from the battlefield (Horowitz, M.C., 2024).
- ***Empower the Human Terrain:*** In the digital age, knowledge is power, and Professional Military Education (PME) is the means. The PME transformation has not kept pace with future operational construct. The need is to review, rebalance and reorient PME objectives, curriculum and methodology to dynamically adapt to the era of multi-domain digital threats that the nation faces to its national security today and in the foreseeable future. The armed forces training academies and staff colleges must prepare officers not only for command and leadership, but also for multi-domain operations, technology integration, and cognitive warfare. Warfare is no longer linear. Leadership must be anticipatory, creative, strategic, agile, and intellectually aggressive (Shivane, A.B., 2025).

Reorganising for Topological War

In a topological battlefield, victory does not lie in holding ground— it lies in disrupting relationships. A battalion that loses IRNSS and satellite feed but continues to operate with internal coherence and can outperform a digitally blind brigade. Thus, the organisation of combat elements must favour smaller, modular, mission-autonomous units like the 'Integrated Multidomain Battle Group viz. Rudra', capable of self-direction and rapid decision-making (Hindustan Times, 2025).

This implies a shift from vertical control to distributed command. Mission-type tactics, where intent is clear but execution is flexible, must replace rigid directives. India's higher

defence leadership must trust tactical leaders to make rapid calls under digital fog. This requires both cultural and institutional transformation.

Moreover, India must now look at force multipliers like loitering drones, AI-assisted surveillance, electromagnetic hardening, and adaptive camouflage as core investments, not experimental luxuries. The future will reward those who out-adapt, not outnumber (Horowitz, M.C., 2024).

Strategic Realignment: National Implications

At the national level, integration of military and civilian infrastructure is inevitable. But it also creates interdependence. If a war breaks out tomorrow, the Indian military will be heavily reliant on civilian satellite networks, telecom grids, defence manufacturing assets, and private data centres. Unless protected and prioritised during conflict, these can become critical liabilities (Horowitz, M.C., 2024).

Thus, a national resilience strategy must encompass:

- Dual-use infrastructure hardened for wartime operation.
- Cyber reserves from the private sector that can support military needs.
- Legal frameworks enabling rapid transition from peacetime to full-spectrum information warfare.
- Command and control doctrine that accounts for zero-connectivity situations.
- A tri-service digital warfighting institution focused on multi-domain integration, simulation, and AI-led planning.

India's adversaries are already investing in hybrid warfare, information operations, and cyber sabotage. Hence, India must not wait for a crisis to realise the cost of doctrinal inertia.

A National Security Strategy for the Multi-Domain Digital Era

A national security strategy remains a void, and thus, an absence of understanding of the battlespace geometry in a multi-domain digital era. The strategy must comprehend doctrine, resilience in a digital age— civil-military interagency fusion beyond just a 'whole of nation' to a 'whole of society' to develop a comprehensive and proactive digital age security strategy.

Recommendations: An Operational Philosophy that Walks the Talk

- Establish digital mission assurance units across formations to identify, audit, and plug systemic vulnerabilities.
- Conduct joint annual degraded-mode exercises that simulate war under total digital denial.
- Mandate cyber readiness certification for all operational units before field deployment.
- Accelerate indigenous R&D in counter-drone, anti-jamming and modular digital infrastructure with military-grade protection.
- Establish a joint cognitive warfare command with dedicated IW, cyber, psychological operations, and electronic warfare brigades
- Invest in funding for autonomous and UAS, like loitering munitions, swarms, and AI-enabled ISR platforms. Balance manned and unmanned, as well as kinetic and non-kinetic domains, for defence procurement.
- Institute mission-type tactical training across arms and services to foster adaptive thought leadership under ambiguity and disruption.

Conclusion: India Must Own its Battlespace

The character and geometry of warfare is fast evolving. The threats have expanded beyond geography, and the autonomous weapons, narratives and digital warfare think faster than humans. For India, a nation surrounded by active threats and unstable theatres, there is no margin for error.

We must now build a military force not just of might, but of mind. A force that can lose connectivity but not coherence. A force that can absorb digital blows and strike back smarter. A force that does not wait for the fog of war to clear but moves confidently within it. A force that does not go begging for funds or get crumpled by archival procedures and bureaucratic control.

In the age of invisible geometry and precise mass, only those who adapt without delay will survive and prevail without loss.

Works Cited

Allardice, R. and Topic, G. (2017, December 21). Battlefield Geometry in Our Digital Age: From Flash to Bang in 22 Milliseconds. *NDU*, 7 (2) https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983758/battlefield-geometry-in-our-digital-age-from-flash-to-bang-in-22-milliseconds/.

All about Indian Army's new Rudra brigade and Bhairav Commando Units. Hindustan Times. 2025, July 27. https://www.hindustantimes.com/india-news/all-about-indian-armys-new-rudra-brigade-and-bhairav-commando-units-101753585802213.html.

Michael C. Horowitz, M.C. (2024, October 22). Battles of Precise Mass: Technology Is Remaking War—and America Must Adapt. *Foreign Affairs*. https://www.scribd.com/document/865598314/Battles-of-Precise-Mass-Technology-Is-Remaking-War-and-America-Must-Adapt.

Shivane, A.B. (2025, July 10). Rearming the Indian Military: A National Defence Reset for Being Future Ready.*CLAWS.* https://claws.co.in/rearming-the-indian-military-a-national-defence-reset-for-being-future-ready/.

About the Author

Lieutenant General A B Shivane, is an NDA alumnus and a decorated Armoured Corps officer with over 39 years of distinguished military service. He is the former Strike Corps Commander and Director General of Mechanised Forces. As a scholar warrior, he has authored over 200 publications on national security and matters defence, besides 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 COAS Chair of Excellence at the Centre for Land Warfare Studies 2021-2022. He is also the Senior Strategic Advisor Board Member to several organisations and Think Tanks.