WEB ARTICLE
WA/25/26

CENJOWS

PREPARING INDIA FOR THE NEXT BATTLESPACE: PRIORITIES BEFORE THE CDS DESIGNATE

LT GEN AB SHIVANE (RETD)

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Preparing India for the Next Battlespace: Priorities Before the CDS Designate

Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd) is a former Strike Corps Commander and Director General of Mechanised Forces.

India's next Chief of Defence Staff assumes office at a defining moment in the nation's strategic journey. The character of warfare has evolved faster than the warfighter's ability to adapt. Conflict is no longer confined to the battlefield; it now plays out across cyber networks, space systems, the electromagnetic spectrum, financial channels, supply chains, data networks, and the cognitive domain. This is an era of multidomain battlespace. In this environment, the real contest is about information advantage, faster decisions, technological adaptability, industrial strength, and national resilience. The national security agenda must therefore move beyond conventional force modernisation towards an integrated, multidomain national security architecture.

The era of isolated platforms and linear kill chains is ending. Future wars will be shaped by "kill webs"[1] in which satellites, drones, missiles, cyber systems, sensors, and commanders operate as a single, seamless, real-time network. The future demands precise mass; resilient Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR); autonomous systems; non-kinetic capabilities; and a decentralised warfighting architecture that can withstand saturation and strike first.

The kinetic and non-kinetic threats to national security are escalating sharply across both external and internal domains. China continues to exert sustained friction below the conflict threshold along the Northern borders while expanding its hold on the Indian economy. On the Western Front, Pakistan fuels the proxy warfare calibrated below the

escalation threshold. The collusive challenge posed by territorial coercion, cyber intrusions, proxy warfare, information manipulation, and grey-zone operations demands a fundamentally different approach to deterrence and preparedness.

The deterrence construct should also move from a defensive, ground-holding posture to one based on deterrence through denial and domination[2]. The equipment philosophy also needs to shift from a threat-cum-capability to a capability-cum-opportunity approach. Finally, this must result in a doctrinal shift in the Indian Armed Forces from cold start to cold strike. Military modernisation must therefore be integrated with enhanced combat capabilities, doctrinal reform, and infrastructure upgrades. The approach has to shift from a platform-centric to an integrated system-centric one.

Time and technological asymmetry are not on India's side. Strategic hesitation will only widen operational vulnerabilities. Nor can the nation rest on the laurels of past wars. The next war will be different in both character and challenge. The key remains a whole-of-nation approach to future threats. Future threats no longer remain confined to borders or battlefields. They now penetrate financial systems, digital infrastructure, public perception, and even social cohesion.

The foremost requirement is a clearly articulated National Security Strategy rooted in an "India First" framework[3]. India cannot continue to rely on standalone doctrines and informal strategic presumptions. The security of the nation depends on the unity of political will, military strength, economic stability, technological preference, diplomacy, and internal security. A proactive and preventive approach must replace reactive crisis management.

Equally important is the long-pending establishment of a National Defence University. The absence of an institutional ecosystem for higher defence management and strategic learning remains a serious national deficit. The Rashtra Raksha University cannot be a substitute, given its differing aims and agendas.

The CDS designate must also address the central weakness in India's defence ecosystem, namely, institutional tempo. Modern conflicts have shown that technology cycles have outpaced legacy procurement cycles. Disruptive technologies are creating a new paradigm in the battlespace. The problem is no longer the absence of ideas or technological talent. It is the inability to convert concepts into operational capability at

the desired tempo due to legacy technology-insensitive processes and a silo-based culture. The CDS will be required to develop a de novo model in which high-technology combat requirements are based on CGOE (Capability Guidelines and Operational Employment) rather than draconian General Staff Qualitative Requirements/ Provisional Staff Qualitative Requirements (GSQR/PSQR). Break the shackles and mindsets to adopt a collaborative, time-sensitive model that bypasses the 'Kill Chain' of bureaucracy.

Self-reliance in defence is a strategic imperative[4] that will shape India's Surakshit Bharat dream by strengthening indigenous capacity and capability. The drivers of this mission will rest on sustained, deep research funding for emerging and disruptive technologies, including data sovereignty, artificial intelligence, hypersonics, directed-energy weapons, quantum systems, and robotics. The nation must move from indigenisation to indigenous capabilities, from Make in India to the Made by India construct. This requires India to rethink its defence architecture, break down silos, involve the private sector, empower academia and startups, and foster an innovation culture aligned with civil and military objectives. Deterrence today is not merely about force levels and equipment. It's reflected in political will, economic resilience, diplomatic acumen, multidomain battlespace dominance, and narrative control.

Regarding tri-service integration structures, functional commands must lay the groundwork to empower theatre commands. The push towards Theatre Commands should not come at the expense of capability gaps in Cyber, Space, Air Defence, and C5ISR Commands. Structural reforms without interoperable networks, a common data architecture, and integrated operational processes will remain cosmetic. Empowerment and upgraded capabilities must precede optimisation through theatreisation.

In the internal security domain, new challenges have emerged of radicalisation, institutional subversion, and lone-wolf attacks, which will need to be addressed. Non-state actors are increasingly exploiting social media networks, digital financing, coordinated information campaigns, and encrypted communications. To ensure a proactive, pre-emptive approach, intelligence fusion, predictive analysis, and integrated responses must be institutionalised.

In today’s security environment, society is both a physical and psychological battleground and the first line of defence. Before a military battle is fought, disinformation, cyber manipulation, sleeper networks, and psychological warfare can be used to exploit social vulnerabilities. To resist both kinetic and non-kinetic threats, India needs a national citizens' security culture in which all sections of society are aware, resilient, responsible, and prepared to face them.

In a future conflict, the first strike will not be at a border post. It could target India’s data backbone. The ability to control, protect, and recover critical data will shape strategic decision-making as surely as firepower once did. Data sovereignty is no longer a technical debate. It must be a national security mission.[5] Any compromise of the access, integrity, and survivability of digital systems weakens command. Data infrastructure must therefore be treated as a battlespace for India, not a utility. Architectural resilience, distributed redundancy, a local distributed cloud, and a professional digital warfighting force are as important as missiles, aircraft, and armour in achieving decision superiority in a crisis.

Future wars will demand techno-thought leadership capable of joint, technological, and strategic thinking across multiple domains. The challenge is not only for accomplished war fighters but also for military techno leaders who can think strategically, display creativity, and maintain a proactive disposition in ambiguous conditions within an integrated, multidomain operational environment. PME must, therefore, shift from career-linked instructional routines to continuous strategic learning, joint war-gaming, civil-military academic integration, and technology-oriented operational thought.[6] A military that modernises equipment without modernising minds risks carrying yesterday’s thinking into tomorrow’s battlefield.

At the end of the day, the CDS Designate’s task will not be just about military coordination but also about preparing the armed forces and India’s national security architecture for the age of multidomain competition, compressed timelines, and proactive dispensation. The real test will be the ability to predict, adapt, integrate, and respond faster than the enemy. In that context, institutional lag, legacy structures, traditional capabilities, and peacetime procedures can be a strategic liability.

The priority, therefore, is clear: build capacity before a crisis, create notional commands before theatreisation, and develop a national security architecture that

remains resilient under stress. The future will favour nations that prepare in time, not those that react after the event.

While heading the DMA, the CDS must be elevated in both stature and responsibility, serving as the direct interface with the Prime Minister on matters of national security, not just national defence. India cannot operate in silos, separating external and internal threats, which are merging. The CDS office must reflect this change, and the impact of creating the CDS must be more visible at both the national level and in future battlespaces.

The CDS Designate is a grounded soldier of exceptional professional repute, impeccable integrity, and vast experience, best suited to address the nation's challenge and shape its trajectory. The real challenge before him will not be merely managing structures or integrating services, but preparing the nation for threats to its national security that may arise more quickly, spread more widely, and unfold in disruptive ways.

DISCLAIMER

ENDNOTES

[1] Wenlin Liu, Zishuang Pan. Construction of kill webs with heterogeneous UAV swarms in dynamic contested environments, Nov 2024, https://link.springer.com/article/10.1007/s40747-024-01644-4

[2] Shivane AB, 'Deterrence in the 21st Century Needs A Strategic Reconstruct', CENJOWS, Apr, 2024, https://cenjows.in/wp-content/uploads/2025/12/Lt_Gen_AB_Shivane_IB_Apr_24_CENJOWS.pdf

[3] Arzan Tarapore, 'India Needs the Anchor of a National Security Strategy', SCRIBD, https://www.scribd.com/document/790909621/3

[4] Shivane AB, 'Defence Self-Reliance Is India's Strategic Insurance in an Unstable World', CSC, Apr 2026, https://www.csconversations.in/defence-self-reliance-is-indias-strategic-insurance-in-an-unstable-world/

[5] Shivane AB, 'Reclaiming The Data Battlespace: Data Sovereignty, Security, And Survivability In The Digital Age', CENJOWS, May6, 2026, https://cenjows.in/publications/reclaiming-the-data-battlespace-data-sovereignty-security-and-survivability-in-the-digital-age/

[6] Kharbanda S, 'Professional Military Education—A Force Multiplier?: Conceptual Construct to Lifelong Learning', USI, Jun 2025, https://usiofindia.org/pdf/Professional_Military_Education_A_Force_Multiplier.pdf