MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Technology, Armoured Forces and Future of Warfare

Karanbir Singh Brar

November 20, 2025

Summary

Every network-centric force is made up of platforms, but not every platform-centric force is networked. The transition is not merely technical—it is doctrinal, cultural and organisational. The shift from isolated excellence to connected intelligence defines the true evolution of military power in the information age.

Introduction

The advent of rapid technological advancements and autonomous systems has significantly impacted warfare in a short period, as evidenced by recent conflicts. The widely shared videos (as part of Information Warfare) of drones destroying tanks in recent conflicts have led to many rushed conclusions about the changing nature of war. These 'lessons', however, need to be understood in a proper tactical and operational context.

The analysis is skewed, given that it is 'net-centricity' which is destroying the 'tanks' and not the 'drones' per se. Those who have operated drone/UAV systems know that, even with AI, the best drones in an average tactical battle area of approx. 30 km x 30 km will find it very difficult on their own, even to locate a tank, let alone destroy it. Only 'drones' connected with the surveillance grid, operating in a net-centric environment with prior intelligence of 'tanks' narrowing down to a km square area or so, can Observe–Orient–Decide and Act (kill) tanks.

The 'tanks', which were generally destroyed in this, were not part of a net-centric environment. The corollary is, if the tanks were part of a net-centric environment, the mere information of a drone attack would have enabled tanks to take countermeasures, even manual countermeasures (not mentioning Air Defence, counter UAS or Active Protection Systems, etc.) like activating anti-aircraft, anti-IR, anti-laser smoke, etc., which would have reduced casualties drastically. Amongst the hype of tank losses, one of the major lessons of Russia–Ukraine conflict gets obfuscated, i.e., the Russians land forces largely led by Armoured captured a very large portion of land and even now hold approx. 20 per cent of the territory, whilst Ukraine devoid of any substantial armoured force cannot regain lost territory.[1]

Future Warfare

Future warfare, defined by Multi-Domain Operations (MDOs) and net-centricity, is not focused on individual platforms but on ensuring that all platforms (organisations/forces, even individual soldiers) are networked. Networked platforms will remain combat-effective, while non-networked platforms (or even organisations/forces) will face adverse effects. Hence, the larger discourse should focus on the impact of technology on the conduct of warfighting and, thereafter, on executing transformations across every arm/service and weapon system to remain combat-efficient in current and future warfighting scenarios.

Platform-centric approach is generally understood to be referring to ships, aircraft and tanks, which is not correct. A platform-centric approach applies to all kinds of

[1] **"Trump Now Says Ukraine Can Win Back All Territory Lost to Russia"**, *Reuters*, 24 September 2025.

weapons (ships, aircraft, tanks), equipment (radar, missile launchers, etc.), companies, squadrons, batteries, or even drones when they are not connected and operate in their own silos. Networks are meaningless unless there are applications on these networks that coordinate the combat and operational functions of forces, weapons systems, and equipment connected to them. A net-centric approach, therefore, does not just refer to networks, computers and data centres.

Therefore, the modernisation of Armoured (or for that matter any arm or service) to future warfighting has to be executed under two heads. It will require creating a net-centric environment and making the force MDO-enabled. This is a larger tri-service issue that requires significant effort. Army Chief General Upendra Dwivedi has mentioned that the year 2026–27 will be 'Year of Network and Data Centricity'.[2] Countries like the USA and China, which have started these efforts many years or decades ago, plan to be fully net-centric and MDO-enabled forces only by 2028 and 2035,[3] respectively.

Secondly, armoured force/weapon systems have to adapt to these changed warfare dynamics, which include new threats such as drones and autonomous systems, an operating combat environment with battlefield transparency, and more non-contact, kinetic, precision-guided warfare, as well as non-contact, non-kinetic, but equally devastating Electronic Warfare (EW) and Cyber Warfare. This would not only require newer or upgraded weapons/equipment but also changes in the type of command, operational and tactical procedures, training, etc.

Beyond Platforms: Understanding Network-centric Warfare

In modern military discussions, the phrase 'network-centric warfare' is often used as shorthand for technological sophistication—AI-enabled drones, smart weapons and advanced sensors. Yet this interpretation misses the essence of what network-centricity truly means. The difference between a platform-centric and a network-centric force is not in the type or generation of technology used, but in how information and decision-making are distributed across the force.

A platform-centric force exemplifies isolated intelligence, built around the power and autonomy of individual systems—tanks, aircraft, ships, satellites, or even AI-driven drones. Each platform is designed to detect, decide and act primarily within its own boundaries. It may use advanced sensors, algorithms and weapons, but its operational picture is limited to what its own systems can perceive and process. In

[2] **"Working on Designating 2026-27 as Year of Networking and Data Centricity: Army Chief"**, *The Economic Times*, 11 November 2025.

[3] **"China's Latest Military Reorganization Terminates the PLA SSF & Launches Three New Arm Forces Based on it: Strategic Implications of the PLA's Latest Reforms and Structural Changes"**, USANAS Foundation, 26 April 2024.

such a set-up, every platform fights its own battle. The commander of a ship or the operator of a drone acts on locally available data. This approach values individual performance—the sophistication of each machine—but often lacks collective intelligence. Even when platforms possess deep technology, without real-time data sharing or coordinated command links, they remain operationally siloed.

A network-centric force, by contrast, is built on the principle of information integration and exemplifies connected intelligence. Every platform, sensor and command node becomes part of a shared network that allows seamless data exchange and collaborative decision-making. Here, information itself becomes the decisive weapon. A sensor in one location can feed data to a shooter elsewhere; a satellite can cue a missile battery hundreds of kilometres away; a drone swarm can be orchestrated dynamically from a command centre based on live intelligence from multiple domains. The focus shifts from 'power of the platform' to 'power of the network'. The advantage no longer lies in who has the most advanced system, but who has the most connected and adaptive force. A fourth-generation fighter linked through a secure data grid may be more lethal in a networked battlespace than a fifth-generation jet fighting in isolation.

AI (and the latest technology like quantum, blockchain, etc.) is not the same as networking. Artificial intelligence is often conflated with network-centricity. While AI can enhance autonomy and speed within individual platforms, or quantum can provide secure, jam-proof communication, these technologies do not automatically create a networked force. An AI-enabled drone that identifies and engages a target autonomously is still platform-centric if it operates without connectivity to other assets. Conversely, a conventional Tank Squadron linked to a real-time command-and-control network that integrates satellite imagery, UAV reconnaissance, and radar tracking is part of a network-centric architecture. This Tank Force will be much more combat-effective than any high-tech operating in isolation. Thus, network-centricity is about shared awareness and coordinated action, not merely about advanced onboard processing.

In a platform-centric force, the decision loop—observe, orient, decide, act—happens within the platform. In a network-centric environment, this loop is distributed across multiple systems. A UAV may observe, a satellite may confirm, a command node may decide, and a naval unit may act. This distributed cognition allows faster, more precise and synchronised responses across domains and is the essence of MDOs.

Indian Solution for MDO/ Net-centricity

All MDOs and net-centric projects in the West, especially in the USA, are being executed in mission mode, with funds earmarked. Replicating the Western MDO architecture is not the answer; we need Indian solutions, but we must follow their

execution procedures.[4] Western MDO and net-centric architecture envisages centralised control across the globe and is massive and monolithic. Whilst we require smaller, customised solutions for our operational context, akin to what Ukraine has done, which are mainly start-up-driven. Decision support systems and battlefield management systems projects which require a fleet of vehicles are passé. Technology (AI/ML, edge computing, sensors, autonomous systems, etc.) and implementation of net-centricity will subsume all operational applications. There is in-house capacity and talent for execution, and we need similar mission-mode projects beyond our procurement procedures.

Armoured Forces and Future Warfare

Land Forces and Tank

Two critical caveats that define the Land Forces in the current (tech) warfare environment are, firstly, that the capture (or loss) of land is the victory marker in any battle. Secondly, due to tech advancements, anything static or unprotected on land will be destroyed even if it is not in a frontline or contact battle.

The first caveat is that Tank remains the key weapon system for conducting operations on Land, with no alternative. The launch of an offensive operation within or across borders requires armour to lead, and no other service or arm can do so. For defence, in the current ISR-enabled precision warfare, static defences will be destroyed by the adversary by targeted fire due to battlefield transparency and "mobile defences" will have to be adopted, in which the 'Tank' would again be the key element. Mostly, the adversary would also bypass static defences, even in mountainous and high-altitude areas (HAAs), hence again requiring mobile defence or a mobile weapon system.

For the second caveat, on land, the Tank is the only land weapon system which is both mobile and the most protected. However, it needs solutions to counter the significant threat posed by drones through complex and soft-kill systems, changes in tactical procedures, and, of course, the enablement of net-centricity, which, in any case, would be a combat enhancer.

Main Battle Tank MBT—The Heavy Tank

For most of the past century, the tank was designed primarily to fight its mirror image. The dominant threat to a tank was another tank. Its form, armour layout and operational philosophy evolved around defeating another tank firing a kinetic energy (KE) round. Aerial and artillery threats existed, but their actual lethality—when measured in probability, precision and cost—never justified major redesigns of the

[4] Lt Gen Karanbir Brar (Retd), **"Is Multi-Domain Operations (MDO) the Answer to the Ongoing Theaterisation Debate?"**, *Bharat Shakti*, 7 November 2025.

tank. The mitigation for air threats, therefore, came not from redesigning tanks but from integrating an Air Defence (AD) component into the combined arms team. Anti-tank guided missiles (ATGMs) did pose a real threat, but the missile operator was equally exposed to return fire. The exchange ratio did not compel doctrinal disruption.

And the only system capable of firing a high-velocity KE penetrator—which no amount of reactive or spaced armour can reliably stop—was another tank. This led to heavier platforms with thicker rolled homogeneous armour (RHA), especially on the frontal arc, while the top remained thinnest because top-attack threats were rare and essentially negligible.

Drone Advantage over Tanks: A Paradigm Shift in Armoured Warfare

The arrival of cheap, autonomous and mass-produced drones, of course, working in a net-centric environment, has overturned this logic. While analysts often highlight low cost and autonomy as tactical advantages, the genuine disruptive factor is numerical superiority. A single fighter aircraft's area of responsibility can now be saturated by thousands of drones. Even a modest 5 per cent hit probability across a drone swarm translates into effects far greater than a complete PGM strike package from human-crewed aircraft.

Quantity has become a form of quality. When drones emerged, traditional air defence systems were unprepared. Legacy radars were optimised to detect aircraft, not small, low-RCS, low-speed aerial objects. Moreover, drones appeared in numbers that existing AD batteries were not designed to handle, overwhelming both sensors and shooters. However, this drone advantage has been negated to a considerable extent by counter-drone systems, creating a paradox for the Tank: it now has to cater for the dominant threat of enemy tanks/missiles at ground level and against drones from the air.

The Indigenisation Gap: A Critical Vulnerability in the Drone Era

Tanks are among the longest-life military assets on the battlefield, often serving for 40 years or more. Over such an extended lifespan, their survivability depends not only on armour thickness and firepower, but on the ability to sustain, upgrade and redesign them in synchronisation with evolving threats. This is only possible when the tank's integration architecture, critical sub-systems and technology stack are indigenous.

India's armoured fleet illustrates this challenge. The bulk of the T-series inventory is based on transferred manufacturing technology (ToT), which provides assembly capability but not design authority. The indigenous Arjun MBT, while a significant step forward, still depends on imported critical sub-systems.

The sudden ascent of drones—from quadcopters to loitering munitions to UCAVs—has created an urgent requirement to integrate counter-drone measures onto tanks. However, retrofitting legacy platforms is difficult when the original design, digital architecture and software ecosystem lie outside national control. Minor modifications require foreign concurrence; major redesigns are practically impossible. This lack of design sovereignty directly impacts battlefield survivability.

Integrating Counter-Drone Capabilities into Tanks

Modern armoured warfare now depends on a tank's ability to survive in drone-saturated environments, making integrated counter-drone systems indispensable. Hard-kill layers—APS adapted for low-RCS drones, anti-drone munitions—must be paired with soft-kill suites such as wideband jammers, spoofers and decoys that disrupt drone guidance and targeting. As top-attack loitering munitions dominate the threat landscape, active and passive aerial protection becomes essential, supported by high-elevation, high-rate anti-drone guns, airburst munitions, and fast-reaction kinetic interceptors that act as a shield.

Equally critical is signature management. With drones employing Electro-Optical/Infra-Red (EO/IR) sensors, Radio Frequency (RF) detection and AI-enabled recognition, tanks can no longer rely on static camouflage. They require multispectral, adaptive concealment that suppresses visual, thermal and electronic signatures while enabling greater survivability in contested airspace. For India, achieving future battlefield relevance demands rapid indigenous development and scaling of these advanced counter-drone and signature-reduction technologies.

Making the Tank Network-centric and Counter-Drone Capable

A tank disconnected from the digital battlespace becomes an obsolete, targetable platform in the drone era. The future tank must function as a networked combat node rather than a standalone vehicle. This begins with secure, jam-resistant Software Defined Radios enabling high-bandwidth links with battlefield management systems, drone swarms, ISR grids and sensor networks. It must also withstand and deliver against both kinetic non-contact attacks—long-range fires, loitering munitions, ground-launched ATGMs—and non-kinetic effects such as EW, cyber disruptions and signature spoofing.

To achieve this, next-generation designs must adopt open-architecture electronics, scalable power for EW suites, AI-driven situational awareness, modular active protection systems and advanced signature management. Counter-drone capability—hard-kill, soft-kill and top-attack protection—must be integral to the design from the outset, not added as retrofits. Only such a networked, drone-resilient tank can maintain dominance in future high-tempo, cross-domain operations.

Light Tank: A Departure from Classic Tank Design Logic

The Light Tank (christened ZORAWAR) is not merely a 'light tank'. Still, it represents a clear doctrinal and technological departure from traditional armoured design, as the DRDO followed in its earliest version of the Tank, weighing 36 tons. As DG Armoured Corps, this author changed Qualitative Requirements (QRs). The design logic[5] is centred around the weight of 25 tons with multi-functionality as the new baseline, and with the following attributes that the next generation of armoured systems will inevitably require:

- *High-altitude optimised mobility*: Power-to-weight, agility and ability to dominate from higher heights than adversary matter more than as there are no classical 'tank vs tank battles'.
- *Air-portable and rapidly deployable*: This will allow massing of armour in High Altitude Areas (HAA) where heavy MBTs are logistically constrained.
- *Anti-drone capable*: This will be enabled by integrating sensors, soft-kill and hard-kill systems, and high-elevation weapons.
- *Autonomous or semi-autonomous operation*
- *Amphibious capability*: This is critical for riverine, marshland and obstacle-rich terrain. Also, as part of Amphibious Task Forces.
- *Swarm-drone compatibility*: The ability to launch, control, or integrate with friendly drone swarms for ISR and precision strike.

Future Tank: The Tank as a Nerve Centre of the Battlefield

The future tank will no longer be defined merely by armour thickness or gun calibre; its decisive value will lie in its ability to control the fight rather than only participate in it. In drone-saturated, sensor-rich battlefields, the tank's primary role is shifting from delivering firepower to orchestrating it. It must become a command-capable node that fuses inputs from UAVs, EW sensors, ISR grids and dispersed combat units, converting raw data into actionable targeting and survivability decisions at the edge. This makes connectivity, data fusion and electromagnetic resilience as essential as mobility and armour protection. Autonomous variants of the future tank would be a natural outcome.

Future combat will compress kinetic and non-kinetic effects into a single engagement space. Tanks must therefore be built to survive and contribute to both. Kinetically,

[5] **"Accelerating Self-Reliance: The Success Story Behind Zorawar's High-Altitude Trials"**, *Bharat Shakti*, 24 December 2024.

they must be able to cue long-range vectors, direct loitering munitions, coordinate fires across artillery and air-delivered systems, and fight through top-attack and swarm-drone threats. Non-kinetically, they must withstand EW attacks, spoofing, cyber interference and signature-based targeting, while simultaneously deploying their own jamming, deception and electronic countermeasures. The tank becomes a dual-domain system—firing rounds and algorithms, armour and electrons—operating simultaneously across physical and electromagnetic terrain.

The relevance of future armour depends entirely on how deeply it is embedded in the broader sensor-shooter grid. Drones have erased battlefield anonymity, precision munitions have collapsed standoff distances, and EW/cyber actions blur the line between contact and non-contact warfare. Multi-domain operations now require land, air, space and information assets to act in synchrony. Therefore, six elements must be tightly networked: tanks and combat vehicles; drones and loitering munitions; artillery and long-range vectors; ISR assets across all domains; EW/cyber capabilities; and integrated air and missile defence nodes to ensure MDO superiority.

Conclusion

Armoured formations, over the years and across various conflicts, have always been a significant factor in battle-winning and a strength for India, serving as a deterrent to our adversaries. Even during the Chinese standoff in 2020, the then Northern Army Commander, Lt Gen YK Joshi, commented that 'Tanks at Rechin La brought PLA for Talks'.[6] Network-centricity remains a work in progress for us—but it is already a force multiplier for India's adversaries.

In a collusive setting, Indian armed forces should not disregard its strength (the Tank). It does not require much military professional expertise to realise that there is a reason that all weapons systems, missiles, rocket launchers, landmines, UCAVs, Drones, Attack Helicopters and even Fighter Aircraft are designed to defeat the 'Tank'. This should not be facilitated.

Every network-centric force is made up of platforms, but not every platform-centric force is networked. The transition is not merely technical—it is doctrinal, cultural and organisational. The shift from isolated excellence to connected intelligence defines the true evolution of military power in the information age. The weapon of the future is not a missile or a drone or an arm—it is the network that binds them together.

[6] Nirupama Subramanian, **"Northern Army Commander Lt General Y K Joshi Interview: 'Tanks at Rechin La, Rezang La Turned Tables on PLA, Brought Them to Talks'"**, *The Indian Express*, 18 February 2021.

About the Author

Lt Gen Karanbir Singh Brar, PVSM, AVSM (Retd), is a former DG Armoured Corps and GOC Dakshin Bharat Area. Presently, he is a Distinguished Strategic Advisor with IIT Madras PRAVARTAK (Tech Innovation Hub of IITM).

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses