



ISSN 23939729

CLAWS

No. **139**

2026

MANEKSHAW PAPER

Evolution of Modern Warfare Frameworks (1990–2026)

**KTG Krishnan
Ravroop Singh**

CENTRE FOR LAND WARFARE STUDIES

Field Marshal Sam Hormusji Framji Jamshedji Manekshaw, better known as Sam “Bahadur”, was the 8th Chief of the Army Staff (COAS). It was under his command that the Indian forces achieved a spectacular victory in the Indo-Pakistan War of 1971. Starting from 1932, when he joined the first batch at the Indian Military Academy (IMA), his distinguished military career spanned over four decades and five wars, including World War II. He was the first of only two Field Marshals in the Indian Army. Sam Manekshaw’s contributions to the Indian Army are legendary. He was a soldier’s soldier and a General’s General. He was outspoken and stood by his convictions. He was immensely popular within the Services and among civilians of all ages. Boyish charm, wit and humour were other notable qualities of independent India’s best known soldier. Apart from hardcore military affairs, the Field Marshal took immense interest in strategic studies and national security issues. Owing to this unique blend of qualities, a grateful nation honoured him with the Padma Bhushan and Padma Vibhushan in 1968 and 1972 respectively.



Field Marshal SHFJ Manekshaw, MC
1914-2008

CLAWS Occasional Papers are dedicated to the memory of Field Marshal Sam Manekshaw

Evolution of Modern Warfare Frameworks (1990–2026)

**KTG Krishnan
Ravroop Singh**



Centre for Land Warfare Studies
New Delhi



Editorial Team : CLAWS

ISSN: 23939729



Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone +91-11-25691308 Fax: +91-11-25692347
Email: landwarfare@gmail.com, website: www.claws.co.in
CLAWS Army No.33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributions aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

© 2026, Centre for Land Warfare Studies (CLAWS), New Delhi.

Disclaimer: The contents of this paper are based on the analysis of materials accessed from open sources and are the personal views of the author. The contents, therefore may not be quoted or cited as representing the views or policy of Government of India, or the Ministry of Defence (MoD), or the Centre for Land Warfare Studies.

Published in Bharat by



Sabre & Quill Publishers, New Delhi, India
www.sabreandquill.com/sabreandquill@gmail.com

Contents

• Abstract.....	5
• Introduction	5
• Revolution in Military Affairs (RMA) – 1990s	7
• Fourth-Generation Warfare (4GW): 1980s–2000s.....	9
• Network-Centric Warfare (NCW): 1990s–2000s	11
• Unrestricted Warfare (1999–Present)	13
• New Wars (1990s–Present)	15
• Hybrid Warfare (Mid-2000s–Present).....	17
• Gerasimov Doctrine / New Generation Warfare (2010s)	19
• Grey Zone Strategies (2010s–Present)	20
• Multi-Domain Operations (MDO) (2010s–Present).....	22
• Intelligentised Warfare (2010s–Present).....	24
• Cognitive Warfare (2010s–Present)	25
• Beyond the Kinetic / Socio-Technical-Cognitive Battlespace (STCB) (2026).....	27
• The Trajectory and Transformation of Warfare Thought.....	28
• STCB and Theaterised C2 Structures	33
• Evolution of Warfare Frameworks: From Kinetic to Cognitive–Systemic Conflict.....	35
• References	36

Evolution of Modern Warfare Frameworks (1990–2026)

Abstract

This article examines the evolution of character of modern warfare from the 1990s to 2026, shifting from technology-centric conventional operations to multidimensional competition spanning military, informational, Cyber, societal, and cognitive domains. Beginning with the Revolution in Military Affairs and Network-Centric Warfare, it covers how the thought process post Cold War emphasized precision strike, information superiority, and networked C2 structures, but later seemed insufficient for insurgent, and hybrid conflicts. The paper covers the progress of modern warfare to the Socio-Technical-Cognitive Battlespace (STCB) in 2026 identifying an intellectual shift from platform- and network-centric warfare towards frameworks emphasizing information, Cyber capabilities, artificial intelligence, societal resilience, and cognitive influence. The STCB framework emerges as the most comprehensive synthesis, integrating these dimensions into a unified understanding of modern conflict. The article concludes that STCB represents a major paradigm shift because it treats society, technology, and cognition as the core battlespace, not merely as support to kinetic force. In light of theaterisation, it honestly describes India's building of this doctrine with strategic clarity on a framework native to the battlespace it already inhabits.

Introduction

Over the past three decades, the character of warfare has evolved significantly in response to technological changes, operational

experiences, and strategic competition. In the immediate post-Cold War period, the Revolution in Military Affairs (RMA) advanced a technology-centric vision of conflict, emphasising precision strike, information superiority, and networked command and control. This approach was soon challenged by irregular and insurgent conflicts, leading to the articulation of Fourth-Generation Warfare (4GW), which highlighted the growing role of non-state actors, legitimacy, and population-centric struggle. As digital connectivity matured, Network-Centric Warfare (NCW) translated information superiority into operational concepts built around C4ISR integration. By the early 2000s, warfare theory expanded beyond purely military domains. Chinese strategists proposed Unrestricted Warfare, arguing that conflict now spans economic, legal, informational, and societal instruments of power. In parallel, the 'New Wars' thesis reframed contemporary violence as identity-driven and transnational. These perspectives were consolidated into the concept of Hybrid Warfare, which captures the deliberate blending of conventional forces, irregular tactics, cyber operations, and information campaigns. Russian strategic practice, often described as New Generation Warfare or the Gerasimov construct, further demonstrated the systematic use of non-kinetic means to achieve political objectives below the threshold of open war.

At the same time, defense planners confronted sustained competition in the grey zone, characterised by ambiguity and deniability. In response to renewed great-power rivalry, Western militaries developed Multi-Domain Operations (MDO) to synchronise effects across land, sea, air, space, cyber, and the electromagnetic spectrum. Looking ahead, Chinese writings on Intelligentised Warfare envisage conflicts shaped by artificial intelligence and autonomous systems, while Cognitive Warfare emphasises the contest for perception, decision-making, and societal resilience. In early 2026, Indian strategists introduced

Beyond the Kinetic, conceptualised as a Socio-Technical-Cognitive Battlespace (STCB), which integrates societal, technological, and cognitive dimensions into a unified understanding of conflict.

This article traces the evolution of these major warfare frameworks in a chronological sequence. For each, it examines origins, core propositions, influence, and critiques, and situates the framework in relation to its predecessors and successors. Each section concludes with a structured comparative assessment across originality, comprehensiveness, empirical grounding, doctrinal implementation, academic and policy influence, future relevance, and ontological depth. Collectively, the analysis demonstrates a clear trajectory from technologically enabled force-on-force warfare toward an expanded conception of conflict in which military power, information, society, and cognition are inseparably linked. This trajectory underscores how contemporary warfare thought has progressively expanded the very boundaries of what constitutes conflict in the twenty-first century

Revolution in Military Affairs (RMA) – 1990s

The concept of the Revolution in Military Affairs (RMA) emerged in the early post-Cold War period as a powerful proposition that advances in military technology and organisational innovation could fundamentally transform the nature and conduct of warfare. Its intellectual roots lay partly in Soviet military thought, most notably Marshal Nikolai Ogarkov's¹ use of the term 'revolution in military affairs' in the late 1970s, and partly in U.S. defence analysis, particularly within Andrew Marshall's Office of Net Assessment². By the early 1990s, RMA had become a central theme in U.S. strategic thinking. Prominent advocates, including Admiral William Owens,

Vice Admiral Arthur Cebrowski³ and analyst Thomas Barnett argued that precision-guided munitions, stealth platforms, satellite

systems, and advanced command, control, communications, and intelligence (C4I) architectures could deliver a decisive military advantage. The 1991 Gulf War appeared to confirm these claims. GPS-guided weapons, real-time intelligence, and networked command structures enabled coalition forces to defeat Iraqi forces rapidly and decisively, with minimal casualties. RMA theorists concluded that information superiority and networked forces could compress decision cycles, improve coordination, and shorten wars.

These assumptions soon found doctrinal expression. During the 1990s, the U.S. Army and other services pursued digitised force structures. The Army's Force XXI experiments aimed to integrate digital networks across formations, while the Joint Chiefs of Staff articulated Full Spectrum Dominance, grounded in information supremacy across domains. NATO and allied militaries invested heavily in reconnaissance satellites, networked communications, precision-guided munitions, and early cyber infrastructure. The U.S. Air Force advanced RMA principles through its Global Strike vision, while the U.S. Navy emphasised Operational Manoeuvre from the Sea. Proponents likened RMA to earlier military revolutions, such as gunpowder, mechanisation, and nuclear weapons, predicting that future wars would be decided increasingly by sensors, networks, and algorithms rather than massed firepower.

By the late 1990s and early 2000s, RMA faced growing skepticism. Critics argued that the Gulf War was fought under unusually permissive conditions against a technologically inferior adversary. Subsequent insurgencies and low-intensity conflicts exposed the limits of a techno-centric approach where advanced weapons and networks alone could not secure political legitimacy, control populations, or defeat decentralised guerrilla forces. Scholars such as Stephen Biddle emphasised the enduring

importance of effective force employment and conventional tactics⁴. Others noted that RMA privileged high-intensity interstate war while neglecting peacekeeping, stabilisation, and counterinsurgency. The US-led campaigns in Afghanistan and Iraq reinforced these critiques, as expensive and complex systems proved ill-suited to counter protracted irregular warfare, raising concerns over affordability and scalability.

Comparative Evaluation (RMA). In its historical context, RMA was highly original, offering a bold, technology-driven narrative of military transformation. It was moderately comprehensive, privileging advanced weapons and information networks while downplaying the political and human dimensions of war. Its empirical validity was a mixed bag; early success in the Gulf War contrasted with later limitations. RMA achieved high uptake within the US military establishment and its allies and exerted a lasting influence on defence planning. Its long-term relevance, however, remains contested. While many RMA-enabled technologies are now standard, later frameworks such as hybrid, grey-zone, and cognitive warfare have challenged its assumptions.

Fourth-Generation Warfare (4GW): 1980s–2000s

As the Revolution in Military Affairs gained prominence, an alternative framework emerged that described a form of conflict almost antithetical to RMA's techno-centric assumptions. In 1989, U.S. analysts led by William S. Lind introduced the concept of Fourth-Generation Warfare (4GW). Lind and his collaborators traced a sequence of four "generations" of warfare starting from Napoleonic line infantry (first generation), through industrial-era firepower and attrition (second generation), to manoeuvre warfare and blitzkrieg (third generation). Fourth-generation warfare, they argued, marked a qualitative shift in which non-state actors and the blurring of war and politics became defining features⁵. In 4GW,

conflict was no longer primarily waged by massed armies but was instead fought “among the people,” through networks rather than hierarchies. Terrorist organisations, guerrilla movements, insurgent groups, and even criminal networks replaced state militaries as the principal actors. Lind and his colleagues contended that the nation-state no longer held a monopoly on organised violence. Through decentralised cells and protracted struggle, relatively weak actors could impose strategic costs by eroding legitimacy, shaping perceptions, and prolonging conflict rather than by defeating enemy forces on the battlefield. Ideology, religion, economics, and information became integral components of battlespace.

The concept gained traction within parts of the US military, particularly the US Marine Corps, and was further developed by Thomas X Hammes in his book “The Sling and the Stone” (2006)⁶, which examined how insurgent groups adapt to technological superiority by avoiding conventional engagements. Fourth-generation conflict was said to include terrorism, propaganda, subversion, cyber activities, and psychological operations, alongside selective kinetic violence. Historical and contemporary examples cited by proponents included Vietnamese and Pashtun insurgents, Chechen fighters, Hezbollah, and later jihadist networks. In practice, however, 4GW functioned as an analytical lens rather than a formal doctrine. It shaped interpretations of conflicts in Vietnam, Afghanistan, and Iraq, where success depended less on battlefield dominance than on control of populations, narratives, and political legitimacy. During the Iraq War, some US officers referenced 4GW to explain insurgent use of improvised explosive devices⁷, media manipulation and the limits of conventional superiority. Nevertheless, 4GW was never adopted as official doctrine and remained largely within academic and professional military debate. Critics argued that it repackaged well-

established concepts of insurgency and terrorism, while supporters credited it with capturing important post-Cold War trends.

Comparative Evaluation (4GW). Fourth-Generation Warfare was highly original in foregrounding the strategic significance of non-state actors and irregular conflict at a time when conventional, technology-driven models dominated Western thinking. Its analytical scope was moderately comprehensive, integrating the political and psychological dimensions of war, though it often treated ideology and identity in broad terms⁸. Empirically, 4GW demonstrated strong descriptive validity, accurately reflecting the conduct of numerous conflicts, but it offered limited predictive precision. Doctrinal uptake was low to moderate, while influential in counterinsurgency debates⁹, 4GW never achieved formal doctrinal status. Its impact on academic and policy discourse has been significant, particularly in shaping discussions on terrorism and insurgency. Its future relevance remains substantial, though later frameworks, such as hybrid and grey-zone warfare, have absorbed many of its insights.

Network-Centric Warfare (NCW): 1990s–2000s

As the Revolution in Military Affairs matured, a more focused and operationally specific concept emerged, which came to be known as Network-Centric Warfare (NCW). Coined in the late 1990s by U.S. naval thinkers, most prominently by Admiral Arthur Cebrowski¹⁰ and John Garstka, in a 1998 Proceedings article, emphasised the proposition that connecting sensors, shooters, and commanders through real-time digital networks could generate a decisive military advantage. Building on earlier ideas advanced by Admiral William Owens and the US Joint Vision statements¹¹, NCW proponents argued that an information advantage could be translated into a competitive advantage by improving situational awareness and accelerating decision-making. At its core, NCW

hypothesised that increasing network centricity, quality, speed, and reach of connectivity among military forces would disproportionately enhance combat effectiveness. In practical terms, this meant heavy investment in C4ISR systems (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance). Examples included Blue Force Tracker systems for friendly force awareness, unmanned aerial vehicles providing live video feeds, satellite communications enabling near real-time data exchange, and digital systems designed to integrate information down to the tactical edge¹². NCW also envisioned a partial flattening of command hierarchies through the principle of “power to the edge,” allowing frontline units to access shared information directly rather than relying solely on centralised orders.

NCW drew explicit inspiration from the civilian information revolution. Scholars such as David Alberts and his collaborators argued that networked business practices, such as just-in-time logistics and distributed decision-making, offered useful analogies for military operations. Their work framed warfare as an information-centric contest, in which shared awareness and rapid coordination could substitute for mass and attrition. Doctrinally, NCW gained significant traction within U.S. and allied militaries during the 2000s. It influenced U.S. Army and Marine Corps planning for digital infantry systems, while the U.S. Air Force pursued net-centric concepts that linked aircraft to space-based sensors and command nodes. United States Military Joint Vision 2010 and Joint Vision 2020¹³ explicitly incorporated NCW principles, and NATO’s transformation initiatives emphasised interoperability and network integration. Early operations, such as precision strikes supported by networked ISR in Afghanistan, were often cited as evidence of NCW’s effectiveness. However, its relevance remained largely confined to conventional, high-

intensity warfare, fitting comfortably within the broader RMA paradigm. Critics highlighted several vulnerabilities. Networks could be jammed, hacked, degraded, or saturated, and adversaries without comparable systems could evade detection or exploit overreliance on technology.

In Iraq and Afghanistan¹⁴, Insurgents frequently operated in dense urban environments where NCW advantages were muted. Concerns were also raised about information overload, as increased data flows did not always translate into better human decision-making.

Comparative Evaluation (NCW). Network-Centric Warfare was analytically significant in formalising the network paradigm for modern combat. Its scope was technologically comprehensive, particularly in its treatment of C4ISR¹⁵, but comparatively limited in addressing social, political, and cultural dimensions of conflict. Empirically, its explanatory power was moderate: it accounted well for success in conventional high-technology operations but was less effective against irregular adversaries. Doctrinal uptake was high within U.S. and allied forces, though its pure form often remained aspirational. NCW exerted substantial influence in academic and policy debates and continues to shape contemporary initiatives such as Joint All-Domain Command and Control (JADC2).

Unrestricted Warfare (1999–Present)

In parallel with Western debates on the Revolution in Military Affairs, a markedly different conceptual framework emerged in China. In 1999, People's Liberation Army Colonels Qiao Liang and Wang Xiangsui published *Unrestricted Warfare*¹⁶, arguing that future conflict would no longer be confined to the military domain. Their central claim was that war had expanded beyond the battlefield, encompassing economic, legal, political, informational,

and cultural instruments. In this view, governments, corporations, and societies themselves could become combatants, and anything capable of harming an adversary's interests could serve as a weapon, from financial manipulation and cyberattacks to media influence and legal action. The authors contended that traditional distinctions between war and peace, soldier and civilian, and military and non-military action were becoming obsolete. They argued that conventional battlefields were being supplanted by continuous, multidimensional competition, in which weaker actors could offset military inferiority by exploiting globalisation and interdependence. Examples offered included currency attacks, cyber sabotage, media propaganda, and the use of international legal mechanisms to constrain adversaries. Crucially, the authors asserted that war was no longer restricted by existing norms or legal frameworks, including the Geneva Conventions.

Unrestricted Warfare diverged sharply from both RMA and Fourth Generation Warfare (4GW). While RMA focused on technological transformation and NCW emphasised information dominance within conventional operations, Unrestricted Warfare rejected the notion of bounded warfare altogether. It took the logic of asymmetric conflict to its extreme, asserting that victory could be achieved through "all means, in all dimensions." Drawing on China's experiences with economic sanctions, diplomatic pressure, and perceived Western coercion, the authors argued that major powers were already practising unrestricted forms of warfare, thereby obliging China and other states to respond in kind. The book generated significant attention in Western policy circles, where it was often interpreted as evidence of a Chinese strategy of "Total War"¹⁷. However, it is important to note that Unrestricted Warfare was never formally adopted as PLA doctrine, and its direct influence on Chinese operational planning remains contested. Instead, it reflected a broader strategic culture that later found

expression in concepts such as the ‘Three Warfares’ (psychological, media, and legal warfare) and in China’s growing emphasis on cyber, economic, and information operations. Analytically, the strength of Unrestricted Warfare lies in its anticipation of how globalisation enables conflict to spill into finance, law, and culture. Its weakness is its lack of doctrinal coherence, many of its proposals were provocative rather than operational, and some methods were neither novel nor easily actionable.

Comparative Evaluation (Unrestricted Warfare). Unrestricted Warfare is highly original in its borderless conception of conflict, offering exceptional conceptual breadth but limited structure. Its empirical testability is low, relying more on illustrative examples than systematic evidence. Doctrinal uptake was minimal, yet its influence on academic and policy discourse has been substantial, particularly in interpretations of Chinese strategy¹⁸. Its future relevance is high, as cyber operations, economic coercion, and information warfare have become central to great-power competition.

New Wars (1990s–Present)

Concurrently, a distinct and more sociologically grounded framework emerged in Europe. Mary Kaldor, a scholar at the London School of Economics, advanced the concept of “New Wars”, most notably in her 1999 book “New and Old Wars”. Kaldor argued that globalisation and identity politics had produced a characteristic form of conflict fundamentally different from Cold War era interstate wars¹⁹. These conflicts were marked by violence among states, warlords, militias, criminal networks, and diasporas, rather than between uniformed national armies. According to Kaldor, New Wars were driven less by ideology and more by identity politics, i.e. ethnic, religious, or nationalist claims, and were financed through predatory and transnational means,

including smuggling, ransom, and diaspora funding. Violence was not primarily directed at defeating enemy forces but at controlling civilian populations through fear, displacement, and intimidation²⁰. She identified cases such as the Balkans, Sierra Leone, Afghanistan, and parts of the Middle East as emblematic of this pattern, highlighting blurred distinctions between combatants and criminals.

A central contribution of the New Wars thesis was its emphasis on non-state networks and the erosion of state authority. Kaldor famously described these conflicts as wars ‘among the people’, arguing that traditional military solutions were insufficient. Instead, effective responses required integrated approaches combining security, humanitarian assistance, governance reform, and international cooperation. Unlike RMA or NCW, New Wars was explicitly normative, advocating changes in how the international community intervened rather than prescribing military doctrine. The framework overlapped with 4GW and later Hybrid Warfare concepts in its focus on irregular actors and non-traditional methods. However, Kaldor placed greater weight on economic incentives, globalisation, and state failure, rather than ideology or military innovation. The New Wars thesis resonated strongly with European policymakers, NGOs, and international organisations, influencing EU and UN approaches that emphasised human security and civilian protection. Critics argued that New Wars overstated its novelty, noting that many features, such as irregular violence, civilian suffering, and war economies, had existed historically²¹. Scholars such as Martin van Creveld contended that war had not fundamentally changed but rather returned to older patterns.

Comparative Evaluation (New Wars). New Wars is original in framing conflict as an identity and economy-driven social phenomenon. It is analytically broad and socially comprehensive,

though sometimes lacking precision. Its empirical power is moderate, fitting many post-Cold War conflicts but offering limited predictive capacity. While it has achieved little in terms of doctrinal uptake, its policy and academic influence have been strong, particularly in peace operations and development discourse.

Hybrid Warfare (Mid-2000s–Present)

By the mid-2000s, strategists increasingly recognised that contemporary adversaries rarely conformed to the binary categories of “conventional” or “irregular” warfare. In response, U.S. Marine Corps Colonel Frank G. Hoffman articulated the concept of Hybrid Warfare²², most prominently in his 2007 article “Conflict in the 21st Century: The Rise of Hybrid Wars.” Hoffman argued that future conflicts would involve the deliberate fusion of conventional military capabilities with irregular tactics, terrorism, criminal activity, cyber operations, and information warfare, conducted simultaneously within a single campaign. The defining feature of Hybrid Warfare is its combinatorial logic. Adversaries are not constrained to one mode of conflict, instead, they dynamically select from a full spectrum of tools to exploit an opponent’s vulnerabilities. A state or non-state actor might deploy regular forces and advanced weapons while simultaneously sponsoring proxy militias, conducting disinformation campaigns, engaging in cyber-attacks, and applying economic or legal pressure²³. This blending complicates attribution, blurs escalation thresholds, and renders traditional declarations of war increasingly irrelevant.

Hoffman drew particular attention to Hezbollah’s 2006 conflict with Israel, which combined guerrilla tactics, precision-guided rockets, fortified defences, and sophisticated media messaging. Similar patterns were later observed in conflicts involving state

sponsorship of militias, terrorist-criminal convergence, and digitally enabled influence operations. Hybrid Warfare thus synthesised elements of RMA (precision and technology), 4GW (irregular actors and legitimacy contests), and Cold War proxy warfare, while rejecting the assumption that these modes occur sequentially or separately. The concept diffused rapidly in Western defence discourse. NATO and US strategy documents began referencing “hybrid threats,” particularly after Russia’s actions in Georgia (2008) and Ukraine (post-2014)²⁴. Militaries emphasised resilience, civil-military coordination, legal preparedness, and whole-of-government responses. However, Hybrid Warfare did not mature into a single coherent doctrine but functioned as a descriptive and planning framework, informing exercises, threat assessments, and capability development. Hybrid Warfare’s principal strength lies in its descriptive accuracy as it captures the complexity of many contemporary conflicts more effectively than earlier paradigms. Its principal weakness is conceptual inflation. As critics note, if all conflicts are “hybrid,” the term risks losing analytic precision²⁵. Nonetheless, hybrid thinking reflects a decisive intellectual shift away from Cold War clarity toward strategic ambiguity and multi-domain competition, paving the way for subsequent Grey Zone concepts.

Comparative Evaluation (Hybrid Warfare). Hybrid Warfare is original in its integrative framing of diverse modes of conflict. Its comprehensiveness is high, though this breadth introduces ambiguity. Empirically, it is strong in describing modern conflicts but weaker in predictive precision. Doctrinal uptake has been moderate, and it is widely cited but loosely codified. Its academic and policy influence has been substantial since 2010, particularly within NATO and strategic studies. Its future relevance remains high as adversaries continue to innovate below and above the threshold of war.

Gerasimov Doctrine / New Generation Warfare (2010s)

19

MANEKSHAW PAPER NO. 139, 2026

Parallel to Western debates on hybrid threats, analysts increasingly focused on Russian strategic thought, particularly following a 2013 article by General Valery Gerasimov²⁶, Chief of the Russian General Staff. In a speech later published in *Military-Industrial Courier*, Gerasimov observed that modern conflicts increasingly begin with non-military measures i.e. political, economic, informational, and psychological, before transitioning to open combat. Western commentators subsequently labelled this approach the “Gerasimov Doctrine,” though the term itself remains contested. Gerasimov argued that the distinction between war and peace was eroding, and that political objectives could often be achieved through indirect means without large-scale conventional operations. He highlighted the growing role of information operations, cyber activities, economic pressure, special operations forces, and proxy actors, noting that these methods could shape outcomes before traditional military force was employed. In this sense, “New Generation Warfare” emphasised pre-conflict shaping and continuous competition, rather than decisive battlefield engagements alone.

Key elements associated with this framework include maskirovka (strategic deception), persistent information confrontation, exploitation of social and political fractures, and the coordinated use of military and non-military instruments under centralised state direction²⁷. Gerasimov cited events such as the Arab Spring and Ukraine as examples of conflicts where non-military means played a decisive role²⁶. Importantly, Russian theorists framed such methods as defensive responses to Western hybrid strategies, rather than as novel inventions. In practice, Russia’s actions in Crimea and Eastern Ukraine (2014 onward) appeared to reflect many of these ideas, including the use of unmarked forces, cyber-attacks on infrastructure, legal and

political manipulation, and sustained disinformation campaigns²⁸. While some Western analysts overstated the coherence of a single “doctrine,” the concept nonetheless became a powerful shorthand for Russia’s integrated, state-directed approach to multi-domain conflict. Conceptually, New Generation Warfare closely resembles Hybrid Warfare but is distinguished by its explicit linkage to state policy and national strategy, rooted in longstanding Russian traditions of deception and active measures²⁹. Its strength lies in systematising hybrid methods within a strategic narrative, whereas its limitation lies in the Western tendency to reify it as a formal doctrine rather than an evolving set of observations.

Comparative Evaluation (Gerasimov / New Generation Warfare). The Gerasimov framework is moderately original, reframing hybrid concepts through a distinctly Russian doctrinal lens. Its comprehensiveness is high, encompassing political, economic, informational, and military tools. Empirical grounding appears strong given its application in Ukraine and Syria. Doctrinal uptake within Russia has been substantial, while abroad it functions primarily as an analytical construct. Its influence on Western policy and military planning has been significant, particularly in counter-hybrid defence.

Grey Zone Strategies (2010s–Present)

By the late 2010s, strategists increasingly sought a concept to describe hostile competition below the threshold of declared war. The term Grey Zone emerged to capture actions that are coercive and aggressive yet deliberately calibrated to avoid triggering conventional military retaliation. The concept gained prominence following Russia’s annexation of Crimea (2014) and China’s assertive behaviour in the South China Sea, though related practices predated these events. Grey Zone activities include cyber intrusions against civilian infrastructure, disinformation

campaigns, economic coercion, covert deployment of special forces or mercenaries, and legal manipulation (lawfare) to alter facts on the ground³⁰. The strategic logic is to achieve political or territorial objectives while maintaining ambiguity and deniability. Conceptually, Grey Zone strategies synthesise earlier frameworks such as Hybrid Warfare, Unrestricted Warfare, and New Generation Warfare, but place particular emphasis on intentional ambiguity. The Grey Zone is defined less by specific tools than by posture where actors operate in the shadow between peace and war, exploiting legal, political, and normative constraints on adversaries. Tactics such as the use of unmarked troops, gradual territorial encroachment (salami slicing), influence operations, and calibrated economic pressure are characteristic examples. Western policy documents, including NATO strategies and U.S. National Defence Strategy reviews, increasingly warn of adversaries operating persistently in this space. While the term appeared sporadically in U.S. defence discussions earlier, it became central only after 2014³¹.

Empirically, Grey Zone competition is now pervasive. China's incremental militarisation of disputed maritime features, Russia's election interference and energy coercion, and the use of non-state proxies by regional powers such as Iran are frequently cited cases. The concept has encouraged governments to rethink escalation thresholds, deterrence mechanisms, and whole-of-government responses. However, its breadth also invites criticism by encompassing activities ranging from propaganda to covert action; the Grey Zone risks becoming analytically diffuse. Compared with Hybrid Warfare, the Grey Zone is less a distinct mode of fighting than a strategic lens emphasising coercion short of war³². It reflects an acceptance that nuclear deterrence and international norms have raised the costs of direct great-power conflict, incentivising competition through incremental and ambiguous means. For

democratic states in particular, Grey Zone strategies highlight vulnerabilities inherent in open societies and the challenge of responding proportionately without escalating.

Comparative Evaluation Grey Zone. Grey Zone strategies are highly original, as a conceptual label capturing contemporary strategic competition. Their comprehensiveness is broad, though at the cost of definitional precision. Empirical relevance is strong, as many recent events fit the model, even if similar dynamics existed historically. Doctrinal uptake has been low as a standalone framework, but policy and strategic influence have been substantial since 2014. Future relevance is high, given persistent great-power rivalry under escalation constraints.

Multi-Domain Operations (MDO) (2010s–Present)

In parallel with Grey Zone debates, the United States military formalised a distinctly operational response to peer competition and christened it as Multi-Domain Operations (MDO). Emerging in the late 2010s, initially as Multi-Domain Battle (MDO) was designed to counter adversaries equipped with anti-access/ area-denial (A2/AD) systems. Tracing its lineage to Cold War concepts such as Air Land Battle, MDO posits that success in future conflicts will require simultaneous and integrated operations across land, air, maritime, space, cyber, and the electromagnetic spectrum. In 2018, senior U.S. Army leaders described MDO as the foundational approach for future warfighting³³. The core proposition of MDO is operational convergence. Rather than sequential or service-specific actions, forces conduct synchronised operations across domains to overwhelm adversary systems³⁴. For example, a kinetic strike might coincide with cyberattacks that disrupt enemy sensors, while space assets provide targeting and missile-warning capabilities. MDO builds directly on RMA and Network-Centric Warfare, relying on advanced sensors, data fusion, and

rapid decision-making, but goes further by institutionalising all-domain integration. Enablers include Joint All-Domain Command and Control (JADC2)³⁵, artificial intelligence assisted decision support, and long-range precision fires.

Doctrinally, MDO has been formally incorporated into U.S. Army field manuals and joint concepts since 2018, shaping modernisation priorities and large-scale exercises. Allied forces have adopted similar ideas, reflecting shared concerns about peer adversaries. Unlike earlier conceptual frameworks, MDO is explicitly doctrinal and programmatic, with published roadmaps and capability requirements. However, critics note that it remains largely kinetic-centric, treating information and cyber primarily as enablers of physical destruction rather than as arenas of political or cognitive contestation. In contrast to Grey Zone and Hybrid frameworks, MDO assumes the onset of open conflict in the form of sub-threshold competition largely as a precursor. As such, MDO represents a reaffirmation of conventional warfighting logic, updated for technological complexity. Its emergence suggests that, after prolonged focus on irregular warfare, the U.S. military has re-centred on preparing for high-intensity conflict with peer competitors³⁶.

Comparative Evaluation (MDO). MDO is innovative in mainstreaming space and cyber as integral warfighting domains. Its technical comprehensiveness is high, though it gives limited attention to political or cognitive dimensions. Empirical validation remains theoretical, relying on exercises and simulations rather than combat experience. Doctrinal uptake is very high within U.S. forces, as MDO constitutes official policy. Academic influence is moderate, with greater traction in professional military literature. Future relevance depends on the character of peer conflict, but MDO addresses a clear operational challenge.

Intelligentised Warfare (2010s–Present)

By the late 2010s, the People's Liberation Army (PLA) began articulating the concept of Intelligentised Warfare (智能化战争), marking a further evolution beyond its earlier focus on 'Informatisation'. Whereas Informatized Warfare emphasised digital networks and precision strikes, Intelligentised Warfare envisions conflict dominated by artificial intelligence, machine autonomy, big data analytics, and algorithmic decision-making. China's 2019 National Defence White Paper explicitly stated that "warfare is evolving toward intelligence," signaling official endorsement of this trajectory³⁷. Chinese military writings describe a future battlespace populated by AI-enabled swarms, autonomous logistics systems, and machine-assisted command structures capable of compressing decision cycles beyond human speed. Distinctively, PLA theorists integrate the cognitive domain into this vision, arguing that intelligent systems should not only optimise weapons employment but also shape enemy perceptions, judgments, and will. In this framework, warfare spans land, sea, air, space, electromagnetic, and cognitive domains, unified by intelligent networks.

Intelligentised Warfare can be understood as a synthesis of Network-Centric Warfare and cognitive warfare, refracted through Chinese strategic culture³⁸. Emerging technologies such as quantum sensing, robotics, neural networks, and digital twins are framed as tools for achieving knowledge dominance and decision superiority. Some Chinese scholars have gone further, speculating about "virtualised" or "metaverse" dimensions of conflict for planning, rehearsal, and influence. A recurring theme is that future war will focus less on destroying forces and more on controlling adversary decision-making processes, potentially through AI-generated disinformation and perception management. Strategically, the concept reflects China's operational environment,

particularly concerns over U.S. technological dominance and regional contingencies such as Taiwan. Proponents argue that Intelligentised Warfare could allow China to offset conventional disadvantages by targeting networks, cognition, and information flows³⁹. The PLA has incorporated these ideas into doctrinal studies, notably the Science of Military Strategy (2020). Western analysts remain divided on whether Intelligentised Warfare represents actionable doctrine or aspirational rhetoric, but it has clearly entered serious policy debate.

Comparative Evaluation (Intelligentised Warfare).

Intelligentised Warfare is highly original as an emerging framework, with no direct Western analogue. Its conceptual comprehensiveness is high, combining technology and cognition, though operational pathways remain underdeveloped. Empirical grounding is speculative, as the concept projects future conflict rather than describing tested practice. Doctrinal uptake within China is growing, while externally it functions mainly as an analytical reference. Its academic and policy influence is moderate but rising.

Cognitive Warfare (2010s–Present)

Underlying many contemporary strategic frameworks is an explicit turn toward the cognitive domain, the realm of human perception, belief, and decision-making. The concept of Cognitive Warfare has gained prominence over the past decade, particularly within NATO and Western strategic discourse⁴⁰. Broadly defined, it refers to the deliberate use of information, psychological techniques, and advanced technologies to influence how individuals and societies perceive reality and make decisions. NATO has described it as a form of conflict aimed at “altering the way people think,” rather than merely what they think. Cognitive warfare builds on earlier practices of propaganda, psychological

operations, and information warfare, but is amplified by digital platforms and AI. Tools such as social media manipulation, algorithmic amplification, deepfakes, and targeted disinformation campaigns enable highly personalised influence operations on a scale. Importantly, cognitive warfare seeks not only to persuade but to disrupt cognitive processes, erode trust, and fragment shared understandings of truth. In this sense, messages, narratives, and algorithms become strategic weapons⁴¹.

The concept aligns closely with Chinese discussions of Intelligentised Warfare and with Western notions of Hybrid and Grey Zone conflict. It also echoes earlier insights from Fourth-Generation Warfare and New Wars, which emphasised ideological struggle and population-centric conflict. What distinguishes cognitive warfare is its explicit reliance on science, data, and technology, including behavioural psychology and AI to operationalise influence at unprecedented depth and speed. Cognitive warfare remains an evolving framework rather than a settled doctrine. Militaries and governments are still grappling with how to defend against it, particularly given the vulnerabilities of open societies. Its analytical strength lies in highlighting perception and morale as decisive terrain, whereas its weakness lies in conceptual overlap with related terms, risking dilution. Nevertheless, cognitive warfare captures a core anxiety of contemporary security that conflicts may be won by controlling meaning rather than territory.

Comparative Evaluation (Cognitive Warfare). Cognitive Warfare is highly original in explicitly defining the human mind as the primary battlespace. Its scope is broad, encompassing psychology, media, AI, and narrative, though this breadth complicates precision. Empirical relevance is strong in contemporary conflicts, even if effects are difficult to measure. Doctrinal uptake remains nascent, but academic and policy interest

is growing rapidly. Future relevance is very high as societies continue to digitise.

Beyond the Kinetic / Socio-Technical-Cognitive Battlespace (STCB) (2026)

In Jan 2026, Indian strategists Lt. Gen. D.S. Hooda (Retd.) and Lt. Col. Pavithran Rajan (Retd.) introduced the framework Beyond the Kinetic, centred on the Socio-Technical-Cognitive Battlespace (STCB)⁴². The concept argues that modern conflict transcends physical violence and fully integrates society, technology, and cognition into a single battlespace. “Socio-technical” emphasises the interdependence of social systems and digital infrastructure, while “cognitive” highlights contests over perception, identity, and narrative. STCB draws on recent conflicts and India’s strategic concerns, including cyber intrusion, foreign influence operations, data sovereignty, and social cohesion. It proposes that every layer of society, i.e. digital networks, economic systems, cultural narratives, and human cognition, can be both a target and a weapon. Attacks on information infrastructure or social trust are treated as acts of war, not peripheral activities. The framework also emphasises resilience, arguing that security must extend beyond the military to civil institutions and populations.

As a synthesis, Beyond the Kinetic integrates insights from RMA, NCW, Hybrid Warfare, Grey Zone strategies, Cognitive Warfare, and New Wars, but articulates them through an explicitly Indian lens. Its ambition is holistic, wherein war is framed as a systemic contest across all domains of national life. However, the concept remains nascent and faces challenges of operationalisation and institutional uptake.

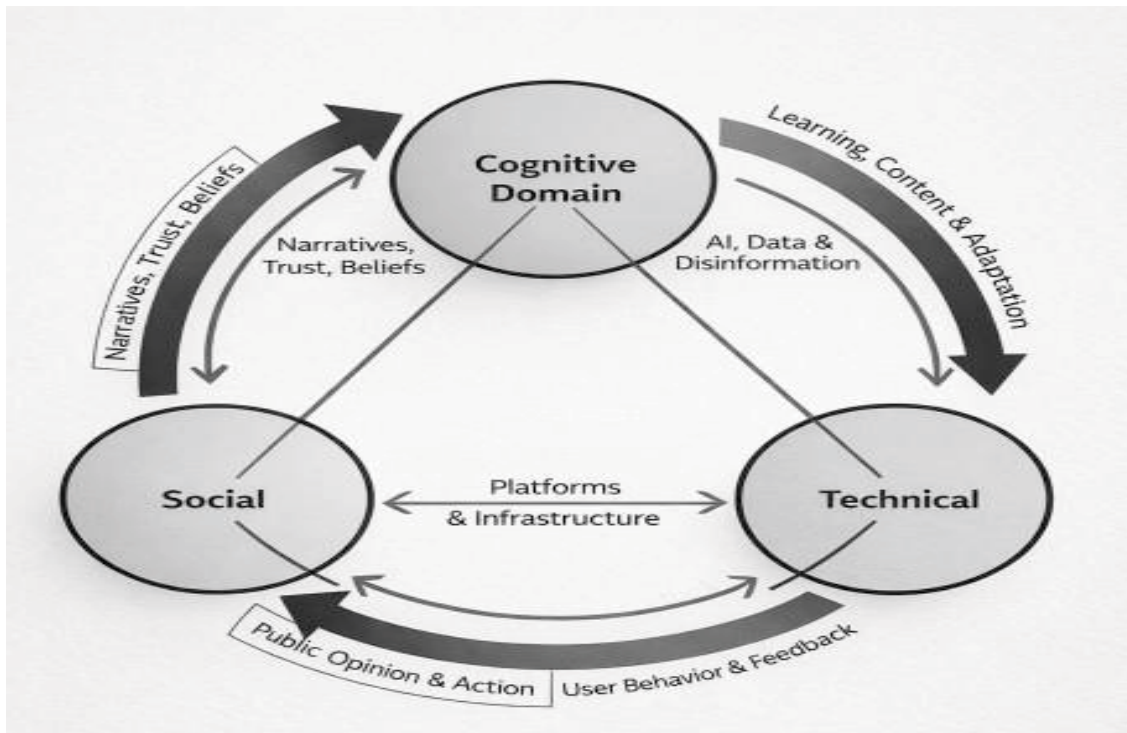


Fig 1: Recursive Feedback Loops – Cognitive Battlespace (STCB)

Comparative Evaluation (Beyond the Kinetic / STCB).

Beyond the Kinetic is highly original in explicitly combining social, technical, and cognitive dimensions within a single battlespace. Its comprehensiveness is very high, though empirical validation is limited due to its recent emergence. Doctrinal uptake is currently minimal, but academic and policy interest is potentially significant. Its future relevance could be substantial as conflicts increasingly target societies rather than armies alone.

The Trajectory and Transformation of Warfare Thought

Taken as a whole, the evolution from the Revolution in Military Affairs (RMA) to the Socio-Technical-Cognitive Battlespace (STCB) represents not merely a succession of doctrinal innovations, but a fundamental transformation in the ontology, epistemology, and practice of warfare. Over the last four decades, warfare thought has shifted from a predominantly material and platform-centric conception to an increasingly immaterial,

systemic, and cognitively mediated understanding of conflict. What began as an effort to optimise kill-chains through information and precision has culminated in frameworks that conceptualise war as a recursive struggle over perception, legitimacy, and the functioning of socio-technical systems. The battlefield has expanded from discrete geographic spaces to encompass networks, narratives, and minds.

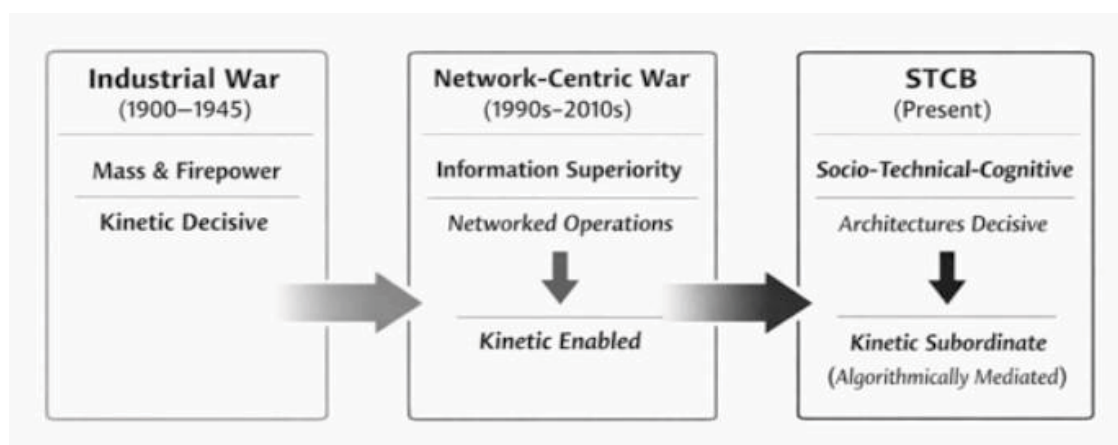


Fig 2: Historical Shift of Strategic Casualty

Early post-Cold War paradigms such as RMA and Network-Centric Warfare were grounded in technological optimism and a belief in informational clarity. They assumed that superior sensing, communication, and precision would yield a decisive advantage, while leaving largely intact the classical, Clausewitzian understanding of war as an instrument of state policy exercised through organised violence⁴³. Although transformative at the level of means, these frameworks did not fundamentally challenge the nature of war itself. By contrast, Fourth-Generation Warfare and New Wars marked a critical inflexion point by foregrounding non-state actors, identity, legitimacy, and the social embeddedness of violence. War was no longer confined to battlefields but increasingly unfolded within populations, institutions, and political narratives⁴⁴.

Hybrid Warfare and Gray Zone competition further destabilised inherited binaries between war and peace, civilian and military, coercion and persuasion. These concepts captured how states and non-state actors increasingly pursue strategic objectives through calibrated combinations of military, informational, economic, and legal tools deliberately employed below the threshold of open war. Gerasimov's synthesis articulated this logic within a Russian strategic idiom, while Western responses, most notably Multi-Domain Operations (MDO) sought to restore operational coherence and deterrence against near-peer competitors by integrating action across physical and non-physical domains. Yet MDO, for all its sophistication, largely reaffirmed a kinetic-centric view of conflict, treating informational and cyber domains primarily as enablers of battlefield success rather than as constitutive arenas of warfare in their own right.

The most recent turn in warfare thought, manifest in Intelligentised Warfare, Cognitive Warfare, and ultimately Beyond the Kinetic, signals a deeper conceptual rupture. Here, warfare is no longer framed primarily as the application of force across multiple domains, but as a socio-technical-cognitive process in which perception, decision-making, and systemic interaction actively constitute the battlespace. Artificial intelligence, data, algorithms, and narratives are not auxiliary tools but central instruments through which power is exercised. Control of meaning, legitimacy, and cognition becomes as strategically consequential as control of territory. In this view, war is not merely fought within information environments; it is fought through them, with reality itself rendered contestable. This evolution should not be interpreted as a linear replacement of ideas, but as a cumulative and adaptive response to changing strategic conditions. Each framework emerged from specific historical experiences and technological contexts: RMA from post-Cold War

unipolarity and precision technologies, 4GW, Unrestricted Warfare, and New Wars from globalization, intrastate conflict, and terrorism, Hybrid and Gray Zone concepts from strategic restraint under nuclear deterrence, MDO from renewed near-peer competition, and cognitive-intelligent paradigms from the data revolution and advances in artificial intelligence. Together, they reflect broader shifts in global power, the diffusion of technology, and the erosion of clear distinctions between military and civilian spheres.

These doctrinal changes also mirror a deeper epistemological transformation. Earlier paradigms presumed that information would reduce uncertainty and enable centralised control. Contemporary frameworks instead assume ambiguity, decentralisation, and the strategic manipulation of knowledge itself. Warfare thought has thus moved away from a centre-of-gravity logic toward a relational and reflexive understanding of conflict, in which actors, systems, and perceptions continuously interact and co-evolve. The central question is no longer only how to destroy enemy capabilities, but how to shape the conditions under which enemies think, decide, and act. The Socio-Technical-Cognitive Battlespace is, by design, a universal framework. Its proposition that modern conflict is waged across the interlocking planes of society, technology, and cognition applies with equal analytical force to any state navigating the ambiguities of twenty-first century competition.

Yet the universality of application does not mean uniformity of fit, and it is here that India's relationship with STCB deserves particular attention. Multi-Domain Operations and Intelligentised Warfare are universal in their own aspirations, too, but both were forged in the specific crucibles of American and Chinese strategic cultures, respectively. The former is oriented toward force-on-force peer competition and breaking A2/AD envelopes, while

the latter is oriented toward AI-enabled decision superiority as an offset to US technological dominance. Neither framework speaks to a state whose primary security challenges include a nuclear-armed border standoff prosecuted through grey-zone and cognitive means, a domestic information environment of unparalleled scale and porosity, a digital public infrastructure (Aadhaar, UPI, ONDC) that is simultaneously a civilisational asset and a systemic vulnerability, and an adversarial calculus that targets social cohesion and cultural identity as deliberately as it targets military hardware. STCB, precisely because it treats society, technology, and cognition as the primary terrain of conflict rather than as enablers of kinetic action, maps onto these conditions with a fidelity that borrowed frameworks cannot match. India need not claim proprietary ownership of a concept whose logic is globally applicable; it only needs to recognise that, among all available warfare frameworks, STCB most honestly describes the battlespace India already inhabits. Building doctrine on a framework native to one's own strategic reality is not intellectual parochialism but strategic clarity.

The STCB framework represents a fundamental rupture in how war is understood: “kinetic action has lost its autonomy as a strategic driver, in STCB, force is an output of information systems,” marking a reversal reminiscent of Hegelian/ Marxist logic in which the traditional base-superstructure relationship is inverted, where classical and industrial-age warfare treated violence as the base and information as superstructure, STCB recasts technical and informational infrastructure as the base, with kinetic violence emerging as an epiphenomenal expression of deeper systemic processes. Philosophically, this aligns with Martin Heidegger’s notion of technology as *Gestell*, yet the STCB formulation goes further by operationalising this insight within strategic theory, arguing that the technical layer does not abolish

but rather internalises and reshapes Carl von Clausewitzian concepts within a new systemic logic.

Seen in this light, Beyond the Kinetic is not a linear doctrinal evolution but a theoretical reframing of war itself, shifting the ontology of conflict from a clash of material forces (an ontology of presence) to the governance of socio-technical-cognitive systems that condition the possibility of force (an ontology of conditioning), wherein material capabilities, technological infrastructures, and human cognition converge into a single analytical plane and kinetic violence becomes only one contingent manifestation of power rather than its defining core. Consequently, whether this framework shapes future doctrine depends less on its internal coherence than on the willingness of military and political institutions to confront the limits of their inherited conceptual models, for if they do, the character of warfare will be defined not merely by control over weapons or domains but by the capacity to understand and shape the systems of meaning, technology, and cognition through which conflict is now waged.

STCB and Theaterised C2 Structures

The Indian Defence Forces are on the cusp of theaterisation, and it is logical to examine STCB through the prism of theaterisation. A close examination reveals that STCB is conceptually aligned with theatreisation because both shift the defence forces from an individual-service-centric approach to integrated, multi-domain warfighting. STCB posits that complex modern conflicts are decided across societal, technological, and cognitive spaces, alongside kinetic tools of warfare, integrating the cognitive and physical battlespaces. Theaterisation creates command-and-control structures that integrate the land, air, maritime, cyber, space, and information domains while leveraging technology more coherently under a single operational framework. STCB

emphasises that outcomes of modern wars emerge from interaction among society, technology, and cognition. That requires military action to be coordinated with cyber, information, intelligence, space, and networked systems. Theaterisation supports exactly this shift by moving toward integrated theatre commands and joint doctrines instead of isolated service responses. STCB, when operationalised in a theaterised structure, integrates the technical layer of information flows, networks and digital systems shaping operational decisions and strategic perception.

The essence of the argument is that if war is socio-technical-cognitive, forces need common doctrines for cyber, amphibious, airborne, logistics, information and special operations.

Theaterisation helps turn STCB from theory into organisation. STCB is primarily a way to understand future wars. STCB provides the intellectual framework and theaterisation provides the command-and-control structure to execute it. Theatre commands are not the end state but the start of broader reforms, including digitisation, data-centricity, and multi-domain integration. It has to be understood that STCB is a larger canvas than theaterisation. Theaterisation mainly reorganises command structures for joint warfighting. STCB goes beyond command arrangements and includes societal resilience, narrative contestation, legitimacy, public morale, and cognitive influence. So theaterisation is necessary but not sufficient for STCB warfare. A military can be theatre-based yet still fall short if it lacks cyber resilience, narrative capability, data fusion, and cognitive preparedness.

Evolution of Warfare Frameworks: From Kinetic to Cognitive–Systemic Conflict

35

MANEKSHAW PAPER NO. 139, 2026

Framework	Era	Core Battlespace	Primary Actors	War–Peace Logic	Strategic Aim	Tech Role	Information Role
Revolution in Military Affairs (RMA)	1990s	High-tech conventional	State militaries	Clear separation	Rapid decisive victory	High	High
4th-Generation Warfare (4GW)	1980s–2000s	Population-centric irregular	Non-state actors	Blurred	Erode legitimacy and will	Low	High
Network-Centric Warfare (NCW)	1990s–2000s	Networked joint ops	State militaries	Clear	Decision speed & precision	High	High
Unrestricted Warfare	1999–present	All instruments (econ, legal, cyber)	State	Abolished	Defeat rivals by any means	Mixed	High
New Wars	1990s–present	Identity & predation conflicts	Mixed actors	Blurred	Control via violence & economics	Medium	High
Hybrid Warfare	2000s–present	Blended kinetic & non-kinetic	States & proxies	Blurred	Wear down the adversary	Medium	High
Gerasimov / New-Generation Warfare	2010s	Integrated political–military	State & proxies	Blurred	Pre-empt war via pressure	Medium	High
Grey Zone Strategies	2010s–present	Below-threshold coercion	States	Deliberately below the war	Achieve aims without escalation	Medium	High
Multi-Domain Operations (MDO)	2010s–present	Land–Air–Sea–Space–Cyber	State joint forces	Clear (peer war)	Break A2/AD systems	High	Embedded

Framework	Era	Core Battlespace	Primary Actors	War-Peace Logic	Strategic Aim	Tech Role	Information Role
Intelligentized Warfare	2019-present	AI-centric cognitive battlespace	AI-capable states	Continuous	Dominate decision loops	Very High	High
Cognitive Warfare	2010s-present	Human perception & cognition	State & non-state	No boundary	Shape beliefs & choices	High	Core
Beyond the Kinetic (STCB)	2026	Socio-technical-cognitive system	Whole-of-society (state)	No threshold	Systemic resilience & sovereignty	High	High

References

- 1 The "Ogarkov Doctrine" and the End of World Bipolarity. A Historical Perspective by Roberto Motta, EJOSS.pdf
- 2 Some Thoughts on Military Revolutions (Office Memo) by Andrew W. Marshall, stacks.stanford.edu.pdf
- 3 "Transforming the Navy," Naval War College Review: Vol. 56 : No. 3, Article 6 by Dombrowski, Peter J. and Ross, Andrew L. (2003) digital-commons.usnwc
- 4 Stephen Biddle on Military Power. *Journal of Strategic Studies*, 28(3), 413–424. By Cohen, E. A. (2005). doi.org
- 5 "The Changing Face of War: Into the Fourth Generation." by Lind, William S., Keith Nightengale, John F. Schmitt, Joseph William Sutton and Gary I. Wilson. *Marine Corps Gazette* (1989)
- 6 *The Sling and the Stone: On War in the 21 st Century* by Thomas X. Hammes, (St Paul, WI: Zenith Press, 2004).
- 7 RAND Studying Iraq Insurgents as First Network-Centric Foes', by Glenn Maffei, 'Inside the Army, 2 May 2005.rand.org
- 8 Fourth-Generation Warfare, Defense and the National Interest Fourth_Generation_Warfare
- 9 The Transformation of War Revisited. *Small Wars & Insurgencies*, 13(2), 3 by Creveld, M.V. (2002). www.tandfonline.com

- 10 Its Origin and Future, Proceedings of the Naval Institute 124 : 1 (Jan 1998), P 28-35 by V.Adm Arthur K Cebrowski, USN and John J Gastka, Network Centric Warfare network-centric-warfare
- 11 Joint Vision 2010: Can It Happen? By Lieutenant General John H. Cushman, USA (Retired) January 1997 Proceedings Volume 123/1/1,127 joint-vision-2010-can-it-happen
- 12 Observations on the Emergence of Network Centric Warfare by Fred P Stein, dtic.mil
- 13 U.S. DoD, Joint Vision 2020 dtic.mil
- 14 Special Report : Al-Qaeda, Janes Intelligence Review, August 2001, pp 42-51
- 15 Information Superiority : Making the Joint Vision, www.c3i.osd.mil/ncw
- 16 Unrestricted Warfare: China's Master Plan to Destroy America by Qiao Liang & Wang Xiangsui
- 17 Unrestricted Warfare: A Chinese doctrine for future warfare? by Major John A. Van Messel, USMC dtic.mil
- 18 Decoding 'Unrestricted Warfare': A Deep Dive into the Revolutionary Chinese Manual on Modern Conflict by Youvan, Douglas. (2023). researchgate_Modern_Conflict
- 19 New and Old Wars by Mary Kaldor
- 20 The Contemporary Mode of Warfare? Mary Kaldor's Theory of New Wars by Shaw, M. (2000). *Review of International Political Economy*, 7(1), 171-180. <http://www.jstor.org/stable/4177336>
- 21 "'New' and 'Old' Civil Wars: A Valid Distinction?" by Kalyvas, Stathis N. *World Politics* 54, no. 1 (2001): 99-118. <https://doi.org/10.1353/wp.2001.0022>.
- 22 Conflict in the 21st Century: Rise of Hybrid Wars by Frank G. Hoffman potomac_hybridwar
- 23 Hybrid Warfare through the Lens of Strategic Theory. Defense and Security Analysis by Caliskan, Murat. (2019). researchgate_Hybrid_Warfare
- 24 A Reminder of Russia's War in Ukraine: "Hybrid Warfare and Presentism" by Murat Çalışkan Navi_Whitepaper
- 25 "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," by Ilmari (2021)
- 26 "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," by

- Valery Gerasimov trans. Robert Coalson, *Military-Industrial Kurier*, 27 February 2013
- 27 "Does Russia Have a Gerasimov Doctrine?," *Parameters* 46, no. 1 (2016) by Roger N. McDermott press.armywarcollege
 - 28 *Hybrid Warfare: Dynamics of Modern-Day Conflict* by Fahim Tahsan bipss.org.bd
 - 29 "'Hybrid Threats': Neither Omnipotent Nor Unbeatable," by Frank G. Hoffman
 - 30 *Mastering the Gray Zone: Understanding a Changing Era of Conflict* by Micheal Mazarr
 - 31 *Gaining Competitive Advantage in the Gray Zone* by Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe www.rand.org
 - 32 *Hybrid Warfare, Grey Zone Conflicts, and the Battle of Narratives: Discourse as a Strategic Weapon.* by Khakwani, Alizeh & Saleem, Muqadas & Malik, Muhammad. (2025)
 - 33 U.S. Army, *Multi-Domain Operations* 2026
 - 34 *Multi-Domain Operations – A New Approach in Warfare?* by János Csengeri University of Public Service, Hungary
 - 35 *Summary of the Joint All-Domain Command and Control (JADC2)*, 2022.media.defense.gov
 - 36 *The Multi-domain Approach to Military Operations and Its Challenges to Intelligence and Intelligence, Surveillance, Reconnaissance* by Ondrej KACMARIK1, Radovan VASI
 - 37 PLA, *Science of Military Strategy* (2020).
 - 38 *Codifying Intelligentized Warfare: The People's Liberation Army's Doctrine's Turn in Science of Military Strategy 2020* by Mayer, Peyton. (2025).
 - 39 *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security* by Allen, G. (2019).www.globalhha.com
 - 40 NATO, *Cognitive Warfare Concept Paper*
 - 41 *Cognitive warfare: a conceptual analysis of the NATO ACT Cognitive Warfare Exploratory Concept* by Deppe C and Schaal GS (2024)
 - 42 *Beyond the Kinetic* (2026) by D.S. Hooda & Pavithran Rajan

- 43 Carl von Clausewitz, On War
- 44 RAND Corporation Future Warfare Studies

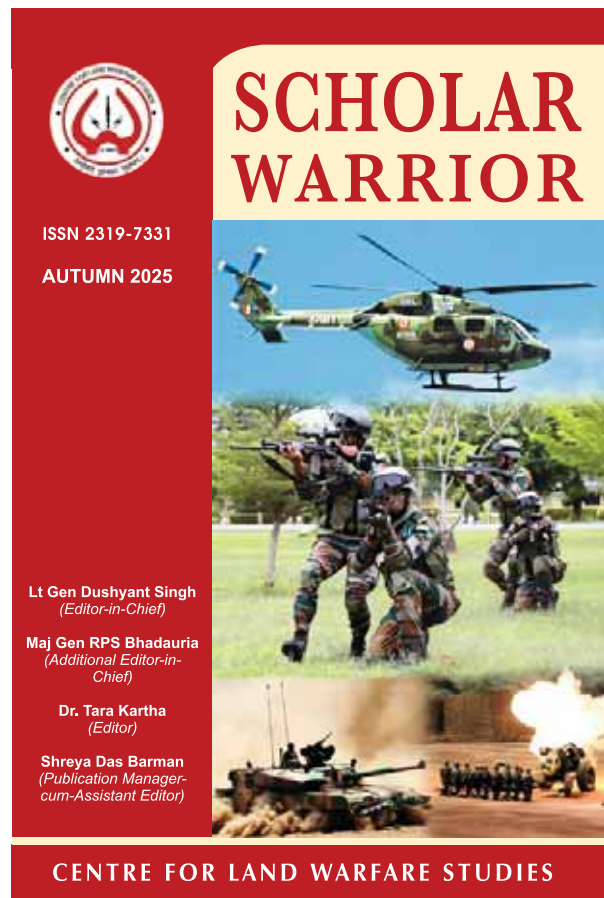
Additional Readings

1. The "Ogarkov Doctrine" and the End of World Bipolarity. A historical perspective by Roberto Motta, EJOSS.pdf
2. Some Thoughts on Military Revolutions (Office Memo) by Andrew W. Marshall, stacks.stanford.edu.pdf
3. "Transforming the Navy," Naval War College Review: Vol. 56: No. 3, Article 6 by Dombrowski, Peter J. and Ross, Andrew L. (2003)digital-commons.usnwc
4. Stephen Biddle on Military Power. Journal of Strategic Studies, 28(3), 413–424. By Cohen, E. A. (2005). doi.org
5. "The Changing Face of War: Into the Fourth Generation," by Lind, William S., Keith Nightengale, John F. Schmitt, Joseph William Sutton and Gary I. Wilson. Marine Corps Gazette (1989)
6. The Sling and the Stone: On War in the 21 st Century by Thomas X. Hammes (St Paul, WI: Zenith Press, 2004).
7. RAND Studying Iraq Insurgents as First Network-Centric Foes', by Glenn Maffei, 'Inside the Army, 2 May 2005.rand.org
8. Fourth-Generation Warfare, Defence and the National Interest fourth_generation_warfare
9. The Transformation of War Revisited. Small Wars & Insurgencies, 13(2), 3 by Crevelde, M. V. (2002). www.tandfonline.com
10. Its Origin and Future, Proceedings of the Naval Institute 124: 1 (Jan 1998), P 28-35 by V.Adm Arthur K Cebrowski, USN and John J Gastka, Network Centric Warfare network-centric-warfare
11. Joint Vision 2010: Can It Happen? By Lieutenant General John H. Cushman, USA (Retired) January 1997 Proceedings Volume 123/1/1,127joint-vision-2010-can-it-happen
12. Observations on the Emergence of NetworkCentricWarfare by Fred P Stein, dtic.mil
13. U.S. DoD, Joint Vision 2020dtic.mil
14. Special Report: Al-Qaeda, Janes Intelligence Review, August 2001, pp 42-51
15. Information Superiority: Making the Joint Vision, www.c3i.osd.mil/ncw

16. Unrestricted Warfare: China's Master Plan to Destroy America by Qiao Liang & Wang Xiangsui
17. Unrestricted Warfare: A Chinese doctrine for future warfare? by Major John A. Van Messel, USMCdtic.mil
18. Decoding 'Unrestricted Warfare': A Deep Dive into the Revolutionary Chinese Manual on Modern Conflict by Youvan, Douglas. (2023).researchgate_Modern_Conflict
19. New and Old Wars by Mary Kaldor
20. The Contemporary Mode of Warfare? Mary Kaldor's Theory of New Wars by Shaw, M. (2000). Review of International Political Economy, 7(1), 171-180. <http://www.jstor.org/stable/4177336>
21. "'New' and 'Old' Civil Wars: A Valid Distinction?" by Kalyvas, Stathis N. World Politics 54, no. 1 (2001): 99-118. <https://doi.org/10.1353/wp.2001.0022>.
22. Conflict in the 21st Century: Rise of Hybrid Wars by Frank G. Hoffman potomac_hybridwar
23. Hybrid Warfare through the Lens of Strategic Theory. Defence and Security Analysis by Caliskan, Murat. (2019).researchgate_Hybrid_Warfare
24. A Reminder of Russia's War in Ukraine: "Hybrid Warfare and Presentism" by Murat Çalışkan Navi_Whitepaper
25. "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," by Ilmari (2021)
26. "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," by Valery Gerasimov, trans. Robert Coalson, Military-Industrial Kurier, 27 February 2013
27. "Does Russia Have a Gerasimov Doctrine?," Parameters 46, no. 1 (2016) by Roger N. McDermott press.armywarcollege
28. Hybrid Warfare: Dynamics of Modern-Day Conflict by Fahim Tahsan bipss.org.bd
29. "'Hybrid Threats': Neither Omnipotent nor Unbeatable," by Frank G. Hoffman
30. Mastering the Grey Zone: Understanding a Changing Era of Conflict by Michael Mazarr

31. Gaining Competitive Advantage in the Grey Zone by Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe www.rand.org
32. Hybrid Warfare, Grey Zone Conflicts, and the Battle of Narratives: Discourse as a Strategic Weapon. by Khakwani, Alizeh & Saleem, Muqadas & Malik, Muhammad. (2025)
33. U.S. Army, Multi-Domain Operations 2026
34. Multi-Domain Operations – A New Approach in Warfare? by János Csengeri, University of Public Service, Hungary
35. Summary of the Joint All-Domain Command and Control (JADC2), 2022.media.defense.gov
36. The Multi-domain Approach to Military Operations and Its Challenges to Intelligence and Intelligence, Surveillance, Reconnaissance by Ondrej KACMARIK1, Radovan VASICEK
37. PLA, Science of Military Strategy (2020).
38. Codifying Intelligentized Warfare: The People's Liberation Army's Doctrine's Turn in Science of Military Strategy 2020 by Mayer, Peyton. (2025).
39. Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security by Allen, G. (2019).www.globalhha.com
40. NATO, Cognitive Warfare Concept Paper
41. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept by Deppe C and Schaal GS (2024)
42. Beyond the Kinetic (2026) by D.S. Hooda & Pavithran Rajan
43. Carl von Clausewitz, On War, RAND Corporation future warfare studies

SUBSCRIBE NOW



SUBSCRIPTION RATES

IN INDIA

☐ Rs.500/- per copy

☐ Rs.1000/- Annual Subscription (2 issues)

SAARC COUNTRIES

☐ US \$ 15 per copy

OTHER COUNTRIES

☐ US \$ 20 per copy

TO SUBSCRIBE SEND YOUR REQUEST TO



Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi - 110010
Tel: +91-11-25691308
• Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com
www.claws.co.in

Over the past three decades, warfare has shifted from technology-centric conventional operations to multidimensional conflict. While various conceptual frameworks attempt to explain this transformation, their overall evolution and interrelations require systematic examination. This article evaluates twelve major warfare frameworks, tracking their progression from the Revolution in Military Affairs (RMA) to the 2026 Socio-Technical-Cognitive Battlespace (STCB). Using a comparative analysis, each framework is assessed based on conceptual originality, comprehensiveness, empirical grounding, doctrinal adoption, academic influence, and future relevance - particularly regarding India's theaterisation efforts. The findings reveal a clear intellectual shift from hardware-heavy systems towards paradigms emphasizing information, cyber capabilities, AI, societal resilience, and cognitive influence. Ultimately, the STCB framework emerges as the most comprehensive synthesis, bringing these dimensions into a unified understanding of modern conflict. It unifies military, technological, societal, and cognitive dimensions, making it an essential tool for 21st-century strategic planning and defense doctrine. Future warfare will be decided by how well we integrate military, technological, societal and cognitive power.

...



Major General KTG Krishnan, SM, VSM is an Infantry Officer who is presently tenanted the appointment of ACIDS (Jt Ops) at HQ IDS. General Officer has extensive operational experience in all terrains.



Major General Ravroop Singh, YSM, SM was commissioned in 18 Jammu and Kashmir Rifles and has done all mandatory courses. The General Officer commanded a unit and Division in Manipur and Brigade having operational role along Northern Borders. He is presently posted as Additional Director General, Staff Duties, Integrated Headquarters of Ministry of Defence (Army).

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributors aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Website: www.claws.co.in

Contact us: landwarfare@gmail.com



MRP: ₹ 100.00 US\$ 5.00