EMERGING TECHNOLOGIES AND POLICY PROGRAM MAY 2026

# FIGHTING ON BORROWED GROUND

## Multi-Domain Operations and the Socio-Technical-Cognitive Battlespace

*Lt Gen D S Hooda (retd)*
*Lt Col Pavithran Rajan (retd)*

CSDR
COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

**Recommended Citation:**

DS Hooda & Pavithran Rajan. *Fighting on Borrowed Ground: Multi-Domain Operations and the Socio-Technical-Cognitive Battlespace*. New Delhi: Council for Strategic and Defense Research, 2026.

## ABOUT THIS REPORT

This report is a follow-up to an earlier study, "Beyond the Kinetic," by the same authors, which introduced the Socio-Technical-Cognitive Battlespace as a way of understanding modern conflict.
It responds to a specific moment in Indian defense policy. In August 2025, India released its Joint Doctrine for Multi-Domain Operations, a significant step toward integrated warfighting. This report examines what that doctrine assumes and what it leaves unaddressed. Its central claim is that Multi-Domain Operations is an operational layer that functions inside a wider strategic environment, and that India cannot build credible multidomain capability on foundations it does not own. The title captures that warning: a force operating on others' infrastructure is fighting on borrowed ground.
The report combines doctrinal analysis with recent case studies drawn from conflicts in Iran, Ukraine, Gaza, and Venezuela, as well as from China's long-term infrastructure strategy. It concludes with concrete recommendations for Indian doctrine, force design, industrial policy, and military education, followed by an annex addressing five objections to its framework. It is written for military planners, policymakers, and analysts concerned with Indian defense doctrine and national strategy.

## COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

The Council for Strategic and Defense Research (CSDR) is an independent, New Delhi-based think tank providing strategic analysis and policy recommendations to governments, businesses, and institutions. Its expertise spans foreign policy, geopolitical risk, connectivity and geoeconomics, defense and aerospace, strategic technologies, conflict resolution, peacebuilding, climate change, energy security, and technology policy, with a focus on the Indian subcontinent, Eurasia, and the Indo-Pacific.

## EMERGING TECHNOLOGIES AND POLICY PROGRAM

The Emerging Technologies and Policy Program studies the intersection of advanced technologies and their wide-ranging social, economic, and political implications. Its work revolves around two primary dimensions: addressing shortcomings in the existing legal framework and developing policy and technical tools to tackle the multifaceted challenges posed by the rapid growth of the tech sector.

## AUTHORS

Lt Gen D S Hooda (retd) - Co-Founder, CSDR
Lt Col Pavithran Rajan (retd) - Advisor, Centre for National Security Studies, Ramaiah University of Applied Sciences

# EXECUTIVE SUMMARY

India released its Joint Doctrine for Multi-Domain Operations in August 2025. The report, written by DS Hooda and Pavithran Rajan, treats this as a sound and overdue step but argues that MDO alone is not enough to win a modern war.

MDO is a doctrine for integrating military effects. It coordinates land, sea, air, cyber, space, and information operations so a force can act faster and more coherently than its opponent. It does not account for the environment on which those operations depend: reliable data, working networks, secure communications, intact supply chains, and a population willing to bear the costs of conflict. The report calls that environment the Socio-Technical-Cognitive Battlespace, or STCB, made up of social, technical, and cognitive domains, plus the algorithms that now shape how information moves between them.

The report's case is that MDO is incomplete in three respects. It is built for the period from crisis to open conflict, but rivals shape the battlespace for years before that, embedding themselves in supply chains, networks, and platforms. Volt Typhoon and the Digital Silk Road are the examples given. MDO also treats cyber and electronic warfare as domains of maneuver, but does not deal systematically with the social and cognitive domains, where legitimacy and public opinion are decided. And it assumes a battlespace composed of military actors, when in practice, private companies shape the outcome, too. The report points to Elon Musk restricting Starlink over Kherson in 2022 and Microsoft cutting services to Nayara Energy in 2025.

For India, this is a problem of ownership. The United States already dominates the global substrate. China has built a sovereign version of its own. India has done neither. Its information environment runs on American platforms. About 90 percent of its cloud market is held by AWS, Microsoft Azure, and Google. It imports close to 80 percent of its electronic components, has no capacity to fabricate chips below 28 nanometres, and depends on foreign models and compute for AI.

The report does not ask India to drop MDO. It argues that India must first secure its substrate, treating it as a goal on par with territorial defense or nuclear deterrence. The recommendations include a national STCB strategy under the Cabinet Committee on Security, long-term investment in indigenous capability, closer civil-military coordination, social and cognitive resilience, and military training that assumes a degraded environment. An annex answers five objections to the argument.

## INTRODUCTION

In August 2025, the Raksha Mantri, Shri Rajnath Singh, released the Joint Doctrine for Multi-Domain Operation.[1] **Multi-Domain Operations (MDO)** represents an important evolution in military thought. It recognizes that modern war cannot be fought through isolated service domains and that operational success depends on the convergence of effects across multiple domains. As the Indian military proceeds with key reforms like theatre commands, this doctrinal shift toward integrated warfighting is both necessary and timely.

The effectiveness of MDO, however, depends on more than the integration of military capabilities. It depends on the environment within which those capabilities function. MDO presumes trusted data, resilient networks, secure communications, functioning supply chains, and commanders who can act with confidence in the information before them. Behind the military effort, there must be a cohesive society that stands resolute in the face of costs. These are the deeper conditions that allow military power to be generated, directed, sustained, and translated into strategic effect.

Our earlier report, **Beyond the Kinetic: Deconstructing Warfare in the Socio-Technical-Cognitive Battlespace** (STCB), introduced the STCB as a framework for understanding how social structures, technical infrastructure, cognitive processes, and the algorithmic substrate interact to form the true terrain of modern conflict.[2] This report builds on that framework and makes a specific argument that MDO is not a self-sufficient doctrine, but an operational layer that functions within the larger STCB environment.

For India, this distinction matters. The challenge is not whether India should pursue MDO, but whether India can build multidomain capability on foundations that are secure, resilient, and sovereign enough to withstand a crisis.

> MDO is not a self-sufficient doctrine, but an operational layer that functions within the larger STCB environment.

## THE APEX AND LIMITATIONS OF KINETIC ART

MDO is one of the most sophisticated expressions of modern operational art. A doctrine of synchronization seamlessly integrating land, sea, air, cyber, space, and information warfare into a singular, unified military system. Its overarching objective is to compress the

adversary's decision cycle through superior tempo, precision, and interoperability across all domains. A joint force that can strike from multiple domains simultaneously, faster than an adversary can respond in any single one, achieves a decisive advantage that no amount of mass in a single domain can match.

The Indian MDO doctrine calls for fusing innovative structures and technologies to counter kinetic, non-kinetic, and cross-domain threats. It amplifies deterrence by presenting adversaries with simultaneous challenges across land, sea, air, cyber, space, and cognitive fields. This integration of capabilities across these fields presents multiple decision dilemmas for the adversary.[3]

For all its operational brilliance, MDO remains incomplete. Its emphasis is on the employment of military power that is effectively integrated, acts faster, strikes deeper, and converges effects more precisely than the adversary. The limitation of this approach is that it does not fully explain how the underlying conditions that enable such operations are created, protected, degraded, or denied. This is where the STCB framework addresses a broader strategic environment. It argues that the true battlespace lies in the intricate, pervasive socio-technical-cognitive substrate beneath the visible battlefield itself.

> For all its operational brilliance, MDO remains incomplete. Its emphasis is on the employment of military power that is effectively integrated, acts faster, strikes deeper, and converges effects more precisely than the adversary. The limitation of this approach is that it does not fully explain how the underlying conditions that enable such operations are created, protected, degraded, or denied.

## TERRAIN REIMAGINED: THE SUBSTRATE AS ACTIVE BATTLESPACE

If MDO defines the operational art of modern warfare, the STCB defines the strategic terrain on which that art is practiced. In the STCB framework, conflict unfolds within an interconnected system in which society, technology, and cognition are inextricably linked.

These elements are not merely supporting instruments of war. They are the conditions through which war is perceived, organized, and sustained.

**The STCB comprises three interlocking domains bound together by an algorithmic substrate.**

The **social domain** encompasses the structures that bind populations together. These include shared identities, trust networks, collective narratives, institutional legitimacy, and the fault lines that can fracture them. A cohesive society can absorb devastating kinetic strikes and maintain political will, while a fractured one may collapse from within before conventional warfare begins. This domain determines whether military operations receive sustained domestic support and whether an adversary's population can be turned against its own government's war aims.

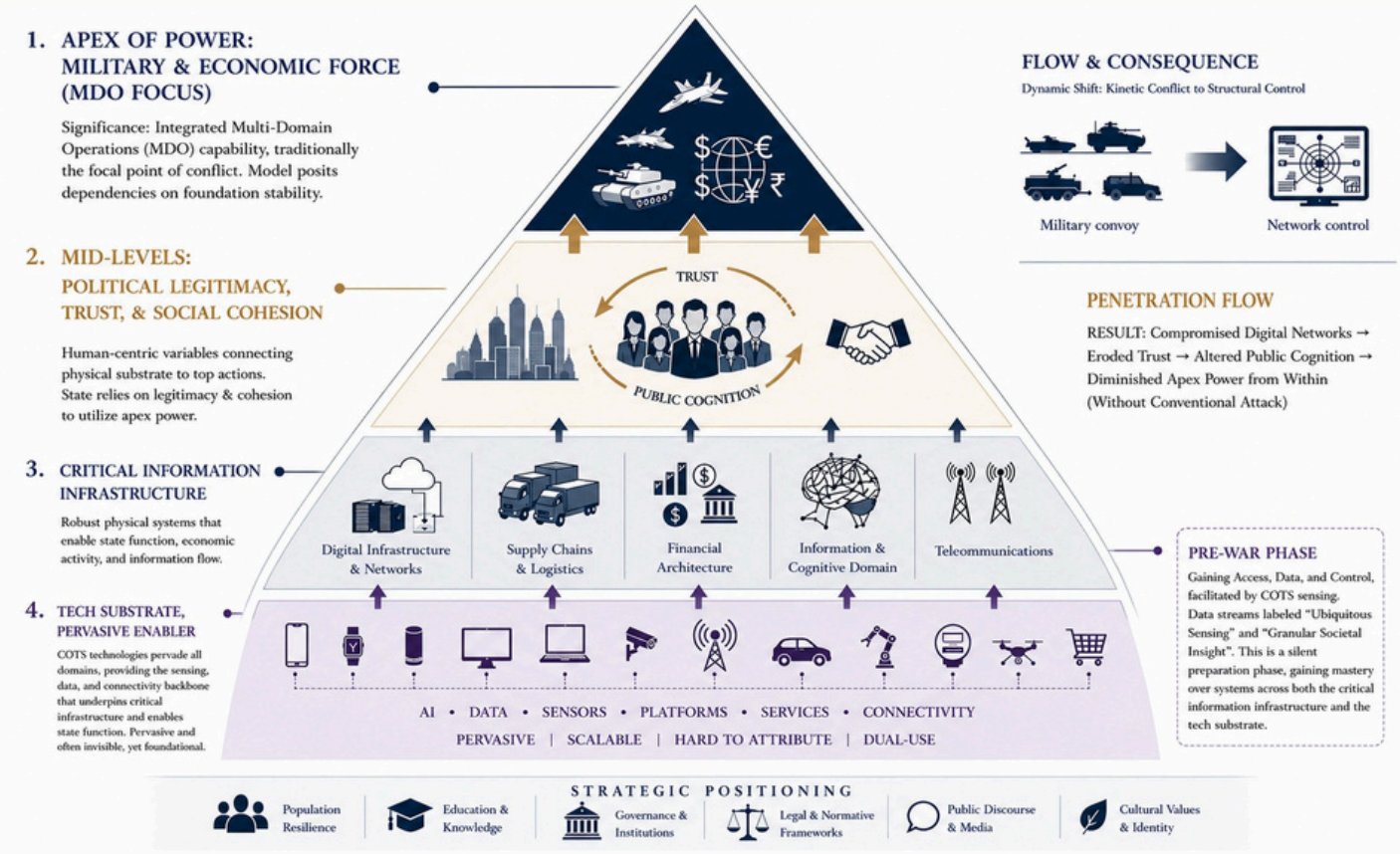
The **technical domain** encompasses the full spectrum of technological systems, including weapon platforms, networks, sensors, satellites, cloud systems, communication grids, financial systems, supply chains, AI models, and data architectures on which contemporary states and militaries depend. In the STCB framework, infrastructure is no longer merely the background of conflict but becomes an active terrain. These systems are often civilian, commercial, and globally distributed. This makes them powerful force multipliers, but also potential channels of strategic vulnerability.

The **cognitive domain** is the center of gravity. It encompasses the mental processes through which individuals and groups perceive reality, form beliefs, construct meaning, and make decisions. The objective is not merely to influence opinions, but to reshape how adversaries, populations, and decision-makers think, reason, and act. Control over this domain can determine whether events produce confidence or confusion, resolve or hesitation, cohesion or fragmentation.

> The algorithmic substrate binds these three domains into a single dynamic system...It mediates every interaction among the three domains. It determines whether cognitive effects amplify or dissipate, whether social movements coalesce or fragment, and whether technical capabilities translate into strategic advantage.

The algorithmic substrate binds these three domains into a single dynamic system. The stack of platforms, models, and control policies that determine who sees what, when, and with what credibility now serves as conductor, amplifier, and gatekeeper of information flows across the STCB. Unlike earlier information environments where human editors curated narratives, today's social reality is increasingly shaped by algorithms embedded in recommendation systems, search engines, and large language models. The algorithmic substrate mediates every interaction among the three domains. It determines whether cognitive effects amplify or dissipate, whether social movements coalesce or fragment, and whether technical capabilities translate into strategic advantage.

**Fig 1 - The STCB conceptual model: a blueprint of national power**




## WHERE MDO FALLS SHORT

The critical question is not what MDO achieves within its scope, but where it leaves the strategic environment insufficiently addressed. The answer lies along three dimensions — time, domain, and actors — each of which has shaped operational outcomes in contemporary conflict but remains underdeveloped in MDO doctrine.

## THE TIME DIMENSION

MDO is most developed as a doctrine for the crisis-to-conflict transition and the conduct of military operations. It is less equipped to theorize decade-long substrate shaping in which commercial platforms, supply chains, social narratives, and technical dependencies are positioned before any military crisis becomes visible.

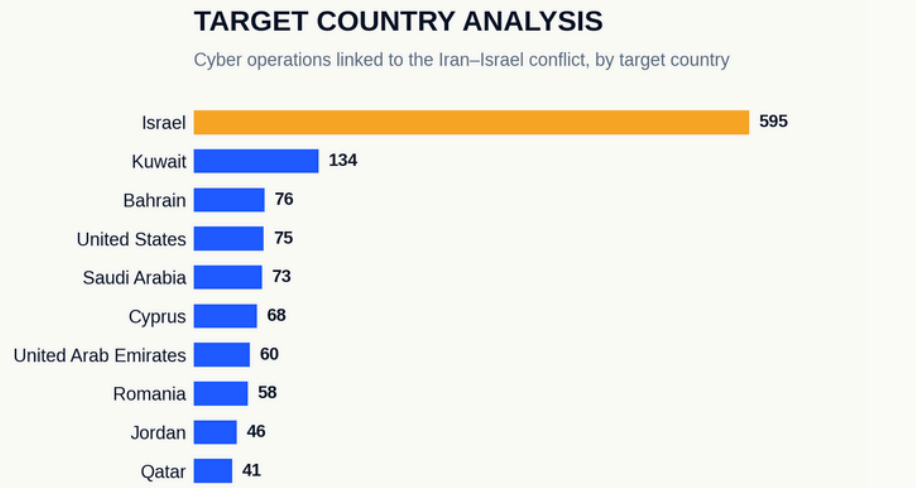
An adversary operating through STCB logic does not wait for declared war. Instead, it engages in proactive penetration, gradually moving through systems over years, cultivating access within defense procurement chains, digital dependencies, telecommunications infrastructure, financial networks, and AI development pipelines. The objective during this phase is never immediate destruction, which would trigger a conventional response, but strategic positioning. By the time a crisis escalates, the target state may appear entirely intact, even as its internal nervous system has already been compromised.

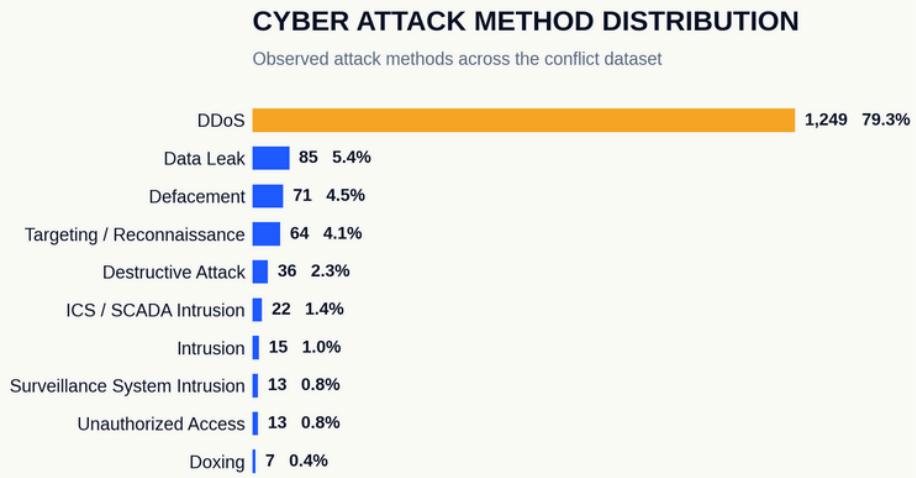
An adversary operating through STCB logic does not wait for declared war. Instead, it engages in proactive penetration, gradually moving through systems over years, cultivating access within defense procurement chains, digital dependencies, telecommunications infrastructure, financial networks, and AI development pipelines.

When US and Israeli forces launched operations against Iran on February 28, 2026, the kinetic campaign was accompanied from its opening hours by a decapitation strike killing Supreme Leader Ayatollah Ali Khamenei and dozens of top security and political officials. This was the culmination of a years-long effort that built a “pattern of life” through social network analysis, algorithmic processing of leadership behavior, hacking Tehran’s traffic cameras, and the compromise of mobile networks.[4]

Within the first hours of the strikes, multiple popular pro-regime Iranian news agencies were simultaneously compromised by fabricated content injected into their front pages. During the second day of strikes, Iranian national television’s Channel 3 satellite streams on IntelSat were hijacked. Viewers were shown video broadcasts of speeches by Donald Trump and Benjamin Netanyahu instead of regular programming. Iran took the unprecedented step of

severing its connection to the global internet.[5] This was a clear example of how substrate domination precedes kinetic strikes.





Source: SOCRadar Iran–Israel Cyber War Dashboard (socradar.io). Figures captured 21 May 2026; dashboard last updated 6 April 2026.

If the Israel-Iran case demonstrates pre-positioned capabilities being activated, China's Volt Typhoon campaign represents the same logic in its preparation phase. In February 2024, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) issued a joint advisory confirming that China-sponsored cyber actors had been embedding themselves inside American critical infrastructure, with particular focus on Guam, a key US military staging base for any Taiwan contingency. This pre-positioning was intended to cause disruptive effects during a future crisis with the United States.[6] FBI Director Christopher Wray called Volt Typhoon "the defining threat of our generation."[7]

China's Digital Silk Road has embedded Chinese-built telecommunications networks, undersea cables, data centers, smart city systems, and surveillance infrastructure across South and Southeast Asia. These are dependencies that can be leveraged in a future crisis, not as military assets but as a substrate through which economic coercion, information control, and cognitive influence can flow. Huawei's presence in national telecommunications networks across dozens of countries represents a pre-positioned technical dependency whose strategic implications would only become visible during a confrontation. These are campaigns measured in decades, not operational planning cycles.

China's Digital Silk Road has embedded Chinese-built telecommunications networks, undersea cables, data centers, smart city systems, and surveillance infrastructure across South and Southeast Asia. These are dependencies that can be leveraged in a future crisis, not as military assets but as a substrate through which economic coercion, information control, and cognitive influence can flow.

## THE DOMAIN DIMENSION

MDO integrates cyber and electronic warfare as domains of maneuver, a genuine advance in how wars would be waged. The STCB brings into view the social domain, the cognitive domain, and the algorithmic substrate. These are domains that MDO does not systematically address.

The social domain, comprising identity, trust, cohesion, and institutional legitimacy, operates as a strategic terrain that determines whether military operations achieve their intended effect. Russia's social-domain tactics succeeded in Crimea in 2014 but failed comprehensively in Kharkiv in 2022, despite the region's significant Russian-speaking population. This was because Ukrainian national identity had consolidated in the intervening years in ways Russian planners did not anticipate.

Israel's military operations in Gaza since October 2023, while achieving operational objectives, generated a social backlash across global audiences that altered diplomatic relationships and constrained political options. In both cases, the social domain shaped strategic outcomes by affecting legitimacy and public support in ways that kinetic operations alone could not control. MDO does not yet provide a sufficiently developed framework for treating social cohesion, legitimacy, and public perception as strategic terrain.

Russia's social-domain tactics succeeded in Crimea in 2014 but failed comprehensively in Kharkiv in 2022, despite the region's significant Russian-speaking population...Israel's military operations in Gaza since October 2023, while achieving operational objectives, generated a social backlash across global audiences... In both cases, the social domain shaped strategic outcomes by affecting legitimacy and public support in ways that kinetic operations alone could not control.

The cognitive domain proved equally decisive in Ukraine. President Volodymyr Zelensky's defiant direct-to-camera wartime communications crystallized international support. The documentation of the Bucha massacre, combining ground-level evidence with commercial satellite imagery, led to punishing US and EU sanctions targeting Russia.[8] These had strategic effects that materially altered the military balance by unlocking resources, strengthening alliance commitments, and sustaining coalition will. The cognitive domain provided the trigger, while the social domain provided the transmission mechanism. This also shows the recursive and dynamic interplay in the STCB domains.

While the Indian MDO places emphasis on cognitive operations, it treats this aspect as part of information operations. In the STCB framework, the cognitive domain is broader than messaging, deception, or narrative management. This is the deeper terrain in which perception, trust, legitimacy, confidence, and decision-making are formed.

The algorithmic substrate amplifies both the social and cognitive domain effects and introduces vulnerabilities of its own. During active conflict, platform governance decisions materially shape the information battlespace. When Meta, YouTube, and Twitter restricted Russian state media following the 2022 invasion, and Facebook temporarily permitted calls for violence against Russian soldiers in some countries, the cognitive environment of the conflict was altered by content moderation decisions made in corporate offices in California.[9] MDO can treat information as an operational input, but it does not account for the algorithmic layer that determines whether that information is ever seen, how it is framed, and whether it is believed.

While the Indian MDO places emphasis on cognitive operations, it treats this aspect as part of information operations. In the STCB framework, the cognitive domain is broader than messaging, deception, or narrative management. This is the deeper terrain in which perception, trust, legitimacy, confidence, and decision-making are formed.

## THE ACTOR DIMENSION

MDO assumes a battlespace populated primarily by military actors within command structures. The STCB includes actors who exercise strategic influence but exist entirely outside any military authority.

The Starlink case is the most vivid illustration. SpaceX's satellite terminals provided Ukrainian forces with critical battlefield connectivity during the war with Russia. However, when Ukraine planned an operation towards Kherson in September 2022, Elon Musk deactivated Starlink access over the area of the offensive. A private citizen's risk calculus directly constrained military operations of a sovereign nation at war.[10]

In July 2025, Microsoft abruptly cut digital services to the Indian company Nayara Energy due to EU sanctions compliance, despite Nayara having violated no Indian law.[11] The decision was made in a foreign corporate headquarters, pursuant to a foreign legal framework, with no reference to Indian sovereign interests. This was a clear sign that foreign platform dependency creates operational vulnerability that can be activated without warning by foreign legal or political decisions.

The global cloud infrastructure on which military logistics, intelligence processing, and command systems increasingly depend is owned by a handful of corporations whose commercial decisions, legal jurisdictions, and terms of service can shape military capability. Content moderation teams on social media platforms exercise de facto control over the cognitive battlespace. A doctrine designed for military forces cannot fully address a battlespace where these actors shape outcomes as materially as any opposing commander.

In July 2025, Microsoft abruptly cut digital services to the Indian company Nayara Energy due to EU sanctions compliance, despite Nayara having violated no Indian law. The decision was made in a foreign corporate headquarters, pursuant to a foreign legal framework, with no reference to Indian sovereign interests.

## MDO WITHIN STCB: THE CORRECT RELATIONSHIP

The preceding analysis does not diminish the value of MDO but clarifies its limits. MDO remains a vital operational doctrine, but it must be understood as operating within the wider STCB. MDO is an operational method for integrating military effects across domains. STCB is the strategic environment that determines whether such integration can be generated, trusted, sustained, and translated into strategic effect.

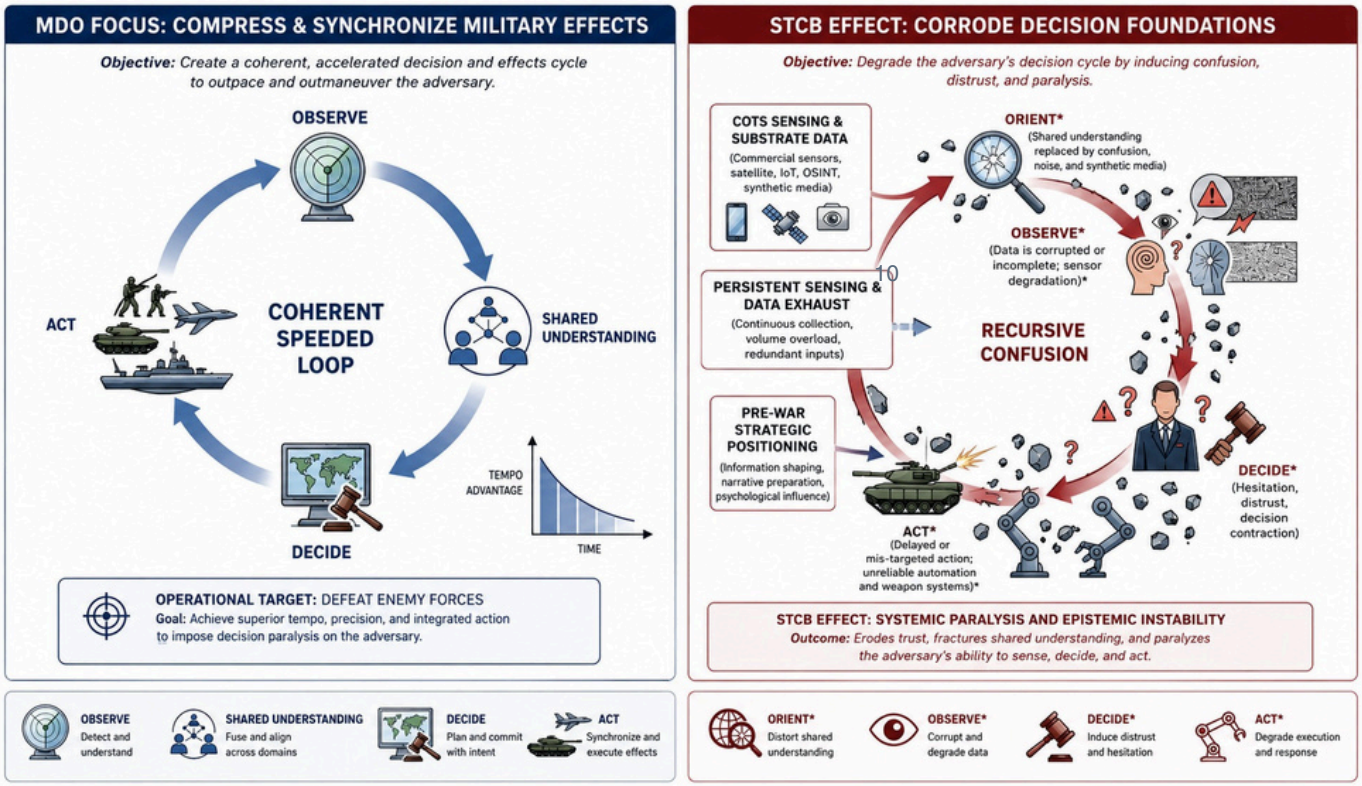
MDO seeks convergence. STCB determines the conditions under which convergence remains possible. MDO compresses decision cycles. STCB shapes the reliability of the information, institutions, networks, and cognitive processes that feed those cycles. MDO aims to impose dilemmas through superior tempo, precision, and interoperability. STCB asks what happens if the systems that make tempo, precision, and interoperability have already been penetrated, manipulated, or placed under conditions of doubt?

Operation Absolute Resolve, the January 2026 US kidnapping of Venezuelan President Maduro, demonstrated this relationship across every domain of STCB. The social domain had been degraded over the years with economic collapse, the mass emigration of over seven million citizens, and a narrative of a stolen election that stripped institutional legitimacy. The technical substrate was fragile, with networks penetrated by months of covert intelligence operations. When US forces executed the kinetic extraction, there was a cognitive collapse in Venezuela's military, which mounted no response. The operation was MDO on a substrate where every layer of the STCB had been won before the first helicopter crossed the coastline.

The relationship becomes clearest in the decision cycle. MDO depends on the ability to observe, orient, decide, and act faster and more coherently than the adversary. STCB degrades not merely the speed of this cycle but the confidence that sustains it. When sensor inputs are corrupted and ISR feeds are spoofed, observation becomes unreliable. When false narratives and algorithmic manipulation flood the information environment, orientation becomes difficult. When institutional trust erodes and political authority hesitates, decision-making slows. All this leads to a slowdown in the necessary action.

Operation Absolute Resolve, the January 2026 US kidnapping of Venezuelan President Maduro, demonstrated this relationship across every domain of STCB. The social domain had been degraded over the years...The technical substrate was fragile, with networks penetrated by months of covert intelligence operations. When US forces executed the kinetic extraction, there was a cognitive collapse in Venezuela's military, which mounted no response. The operation was MDO on a substrate where every layer of the STCB had been won before the first helicopter crossed the coastline.

**Fig 2 - How STCB Disruption Degrades the MDO OODA Loop**




The error, therefore, lies in treating MDO as a complete theory of victory. MDO explains how forces should fight. It cannot by itself explain whether the state possesses the resilient social, technical, and cognitive foundations required for such fighting. Multi-domain integration can multiply combat power when those foundations are secure. Where they are fragile, there are serious vulnerabilities.

This has direct implications for doctrine, planning, and force design. MDO cannot be built solely on platforms, fires, sensors, and joint command structures, but on the conditions that enable those instruments to function with trust and coherence. These are not peripheral concerns. They are preconditions for operational success.

The military that understands this relationship will not merely prepare to fight across domains. It will create the conditions that make fighting across domains matter.

> MDO seeks convergence. STCB determines the conditions under which convergence remains possible.

## MDO AND THE PROBLEM OF STCB CONTROL

If MDO depends on the STCB, then the decisive question becomes whether all states possess equal control over that battlespace. MDO may be a universal military requirement, but its effectiveness varies with the depth, resilience, and sovereignty of the foundations on which it rests. A state cannot simply adopt the vocabulary of MDO and assume that it has acquired the underlying capacity to conduct multidomain warfare. For states whose substrate is partially foreign-owned, externally dependent, or insufficiently secured, MDO risks becoming an architecture built on vulnerable ground.

The United States and China illustrate two different forms of STCB depth. The United States pioneered MDO, and the doctrine does not explicitly address the STCB because American power already permeates the substrate on which modern conflict depends. American corporations own the platforms through which global narratives are shaped. American companies provide the cloud infrastructure on which governments and militaries worldwide operate. American semiconductor design houses dominate chip architecture. When American forces execute MDO, they do so from a position of unusual influence over the substrate.

China recognized this asymmetry far earlier than most nations and responded with one of the most comprehensive attempts to build a sovereign alternative. The Great Firewall created a self-contained digital ecosystem in which the cognitive domain of 1.4 billion people is shaped by algorithms under Chinese regulatory control. WeChat, Baidu, Douyin, and Alibaba provide a parallel information environment under Chinese jurisdiction. While China has not yet achieved the substrate dominance of the United States, when the People's Liberation Army plans for multi-domain contingencies, it does so on a substrate that Beijing has deliberately built.

MDO’s effectiveness varies with the depth, resilience, and sovereignty of the foundations on which it rests. A state cannot simply adopt the vocabulary of MDO and assume that it has acquired the underlying capacity to conduct multidomain warfare. For states whose substrate is partially foreign-owned, externally dependent, or insufficiently secured, MDO risks becoming an architecture built on vulnerable ground.

## INDIA: OPERATIONAL AMBITION ON AN UNOWNED SUBSTRATE

As India looks to operationalize multidomain operations, it must deeply examine its vulnerabilities in the socio-technical-cognitive substrate.

The cognitive domain of India's population, where narratives are formed, political opinions shaped, and social trust built or eroded, is mediated almost entirely by platforms owned by American corporations, governed by American legal frameworks, and managed by algorithms designed in Silicon Valley.

India's cloud computing market is one of the fastest-growing in the world, with 90% of the market dominated by AWS, Microsoft Azure, and Google Cloud. While data localization requirements exist in specific sectors such as financial services, the broader reality is that much of India's sensitive institutional data resides on infrastructure governed by foreign corporate decisions and foreign legal jurisdictions. In a crisis, the availability, integrity, and confidentiality of this data would depend on decisions made outside India's sovereign control.[12]

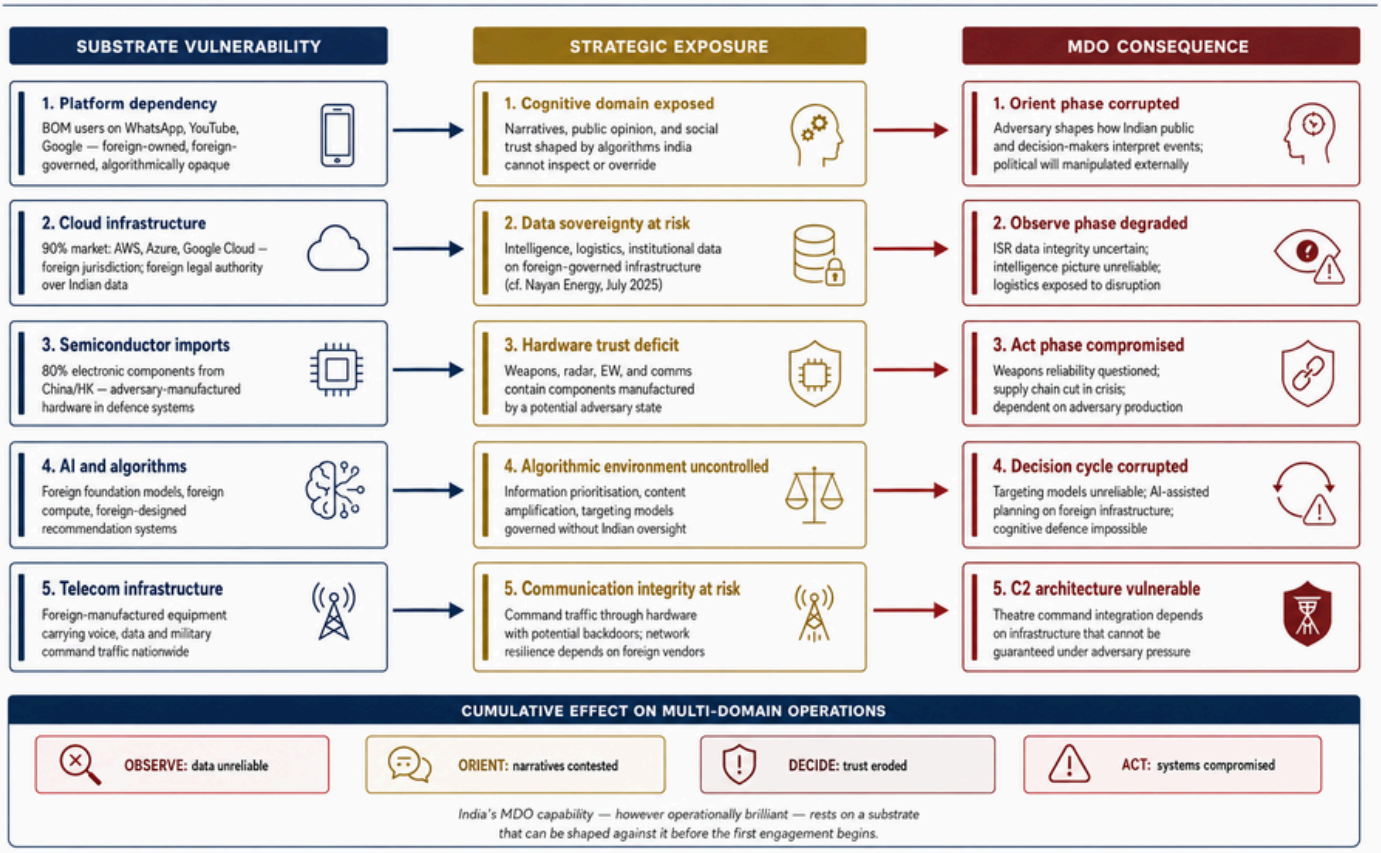
India imports nearly 80 percent of its electronic components, including semiconductors, and 70 percent of these originate from China and Hong Kong.[13] The India Semiconductor Mission has attracted investment in assembly and packaging facilities. Still, these facilities will produce legacy-node chips, not the advanced processors that cutting-edge military systems depend on. India currently has no domestic capability to fabricate chips below 28 nanometres.[14] The advanced semiconductors in India's defense systems are imported, and their supply chains pass through jurisdictions India does not control.

> India's artificial intelligence ecosystem, while growing rapidly in application development, remains dependent on foreign foundation models, foreign-controlled training infrastructure, and foreign cloud compute for model development and deployment. The algorithms shaping the information environment are designed and governed by foreign corporations with no obligation to align with Indian strategic interests.

India's artificial intelligence ecosystem, while growing rapidly in application development, remains dependent on foreign foundation models, foreign-controlled training infrastructure, and foreign cloud compute for model development and deployment. The algorithms shaping the information environment are designed and governed by foreign corporations with no obligation to align with Indian strategic interests. The cumulative effect of these dependencies is that India's MDO architecture, when operational, will rest on a substrate permeated by foreign ownership at every layer. As the Nayara Energy incident shows, this vulnerability will be exposed when India's strategic decisions diverge from the interests of countries like the US, which control much of the substrate.

The implication is not that India should abandon MDO. It is that India must pursue STCB sovereignty as the prerequisite for effective MDO. The sections that follow address what this would mean in practice.

**Fig 3 - How India's substrate vulnerabilities cascade into operational consequences**



# IMPLICATIONS FOR MILITARY DOCTRINE AND FORCE DESIGN

If MDO operates within the STCB and India's STCB substrate is substantially unowned, the implications extend beyond doctrinal refinement. They demand changes in how India conceives national strategy, envisions STCB sovereignty, enhances social cohesion, and educates its officer corps. The following recommendations are not aspirational goals but operational necessities that flow directly from the analysis.

## A NATIONAL STCB STRATEGY

India needs a national strategy that treats STCB sovereignty as a strategic objective on a par with territorial defense or nuclear deterrence. This strategy must begin with a comprehensive mapping of India's STCB dependencies that identifies, for each layer of the substrate, what India controls, what it depends on, and where such dependencies create risk. This audit must cover platforms, cloud and data infrastructure, semiconductor and hardware supply chains, AI and algorithmic systems, and telecommunications infrastructure. The output should be a strategic vulnerability assessment that drives investment priorities, procurement decisions, regulatory action, and force design.

The strategy must be owned by the Cabinet Committee on Security and implemented through mandates that bind ministries such as defense, electronics and information technology, telecommunications, finance, commerce, and external affairs. STCB sovereignty is not a military problem alone, but without a national strategy, the military will continue to build operational capability on a substrate whose vulnerabilities have been identified yet unaddressed.

> India needs a national strategy that treats STCB sovereignty as a strategic objective on a par with territorial defense or nuclear deterrence. This strategy must begin with a comprehensive mapping of India's STCB dependencies that identifies, for each layer of the substrate, what India controls, what it depends on, and where such dependencies create risk.

## BUILDING STCB SOVEREIGNTY

Building substrate independence must be treated as a priority on par with platform acquisition and force modernization. This is the most consequential implication of the analysis, and the most difficult to implement because much of the relevant investment lies outside traditional defense budgets and military authority.

Creating indigenous capability is not a task for the military. It requires national-level investment decisions, industrial policy alignment, and sustained commitment over timescales measured in decades. However, the military must be the organization that articulates the operational requirement for STCB sovereignty and ensures that the national strategy addresses it.

## CIVIL-MILITARY INTEGRATION FOR THE STCB

The STCB dissolves the traditional boundary between military and civilian strategic domains. Much of the terrain that determines military outcomes lies outside military control. This reality demands a model of civil-military integration that goes beyond coordination on specific issues to establish a shared understanding of the STCB as a common strategic environment.

Military leaders must understand that their operational environment is shaped by decisions made in corporate boardrooms and regulatory agencies as much as in opposing headquarters. Civilian leaders in technology, telecommunications, and industrial policy must understand that their decisions have strategic consequences. A procurement favoring a foreign cloud provider, or a regulatory decision permitting foreign equipment in critical networks, is not merely a commercial choice but a decision about the substrate on which India's defense will rest.

> Military leaders must understand that their operational environment is shaped by decisions made in corporate boardrooms and regulatory agencies as much as in opposing headquarters. Civilian leaders in technology, telecommunications, and industrial policy must understand that their decisions have strategic consequences.

## COGNITIVE AND SOCIAL RESILIENCE

In a crisis, India's adversaries will not only seek to disrupt military systems but also to shape perception, amplify divisions, undermine confidence, and slow decision-making. Disinformation, deepfakes, manipulated battlefield imagery, attacks on institutional credibility, and targeted narratives aimed at social fault lines can all become instruments of strategic pressure. In this environment, social cohesion is not merely a domestic concern but is a military enabler.

Cognitive resilience cannot be built only during a crisis. It must be developed before a crisis through credible institutions, transparent communication, media literacy, and practiced coordination between civil and military authorities. A population that trusts official information during a crisis is harder to manipulate.

> Cognitive resilience cannot be built only during a crisis. It must be developed before a crisis through credible institutions, transparent communication, media literacy, and practiced coordination between civil and military authorities. A population that trusts official information during a crisis is harder to manipulate.

A society that understands the possibility of cognitive attack is less likely to panic when adversaries flood the information environment with ambiguity. A military whose commanders are trained to operate amid deception and narrative contestation is less likely to be paralyzed by uncertainty.

## MILITARY EDUCATION

An essential requirement is training and wargaming for STCB conditions. Indian military exercises must test not only whether forces can converge effects across domains, but whether they can do so when the socio-technical-cognitive environment is under attack. Exercises should include degraded networks, corrupted data, spoofed ISR feeds, cyber disruption, social media panic, and decision-making pressure. The aim should be to train commanders to operate when certainty is unavailable and when the information environment itself has become part of the battlefield.

Professional military education must also evolve. Officers trained for MDO must understand not only joint operations, but also data integrity, algorithmic influence, cognitive warfare, public narratives, platform dependencies, and the strategic role of trust. The future Indian commanders will operate in an environment where the adversary is attempting to manipulate what they see, what the public understands, and the political compulsions of national leadership.

Several objections to the STCB framework, including whether it downplays kinetic force, whether full STCB sovereignty is feasible, and whether India should first complete basic jointness before expanding into the STCB, are examined in the Annex.

> Professional military education must also evolve. Officers trained for MDO must understand not only joint operations, but also data integrity, algorithmic influence, cognitive warfare, public narratives, platform dependencies, and the strategic role of trust. The future Indian commanders will operate in an environment where the adversary is attempting to manipulate what they see, what the public understands, and the political compulsions of national leadership.

## CONCLUSION

This report argues that MDO, however brilliantly conceived and executed, will succeed or fail based on conditions established in the STCB environment that MDO does not fully address. Victorious armies win before entering the battlefield, not because cognitive warfare replaces kinetic warfare, but because the environment within which kinetic operations occur is shaped long before the first shot is fired. The army that enters the battlefield having secured its substrate fights a fundamentally different war than the army that enters the battlefield on terrain controlled by others. The forces and the doctrine may be identical. The outcomes will be different.

This is work measured in years and decades through building sovereign digital infrastructure, reducing critical dependencies, developing indigenous capabilities across the substrate, and integrating these efforts into a national strategy owned at the highest level. It is not work that can wait for a crisis to reveal the need.

> The army that enters the battlefield having secured its substrate fights a fundamentally different war than the army that enters the battlefield on terrain controlled by others. The forces and the doctrine may be identical. The outcomes will be different.

# ENDNOTES

[1] “Fostering Joint Warfighting: India’s Joint Doctrine for Multi-Domain Operations - MP-IDSA.” Accessed May 19, 2026. https://idsa.in/publisher/comments/fostering-joint-warfighting-indias-joint-doctrine-for-multi-domain-operations.
[2] “Beyond the Kinetic: Deconstructing Warfare in the Socio-Technical-Cognitive Battlespace - CSDR.” Accessed May 16, 2026. https://csdronline.com/beyond-the-kinetic-deconstructing-warfare-in-the-socio-technical-cognitive-battlespace/.
[3] Headquarters Integrated Defence Staff, JP 2.06 “Joint Doctrine for Multi Domain Operations.”
[4] “How Did Israel Track, Isolate and Kill Khamenei? Hacked Traffic Cameras, Network Disruption on Pasteur Street, & More | Today News.” Accessed May 20, 2026. https://www.livemint.com/news/world/how-israel-tracked-isolated-and-killed-khamenei-hacked-traffic-cameras-network-disruption-on-pasteur-street-mor-11772516322774.html.
[5] “Cyber Warfare in the US-Israel vs Iran Conflict (Roaring Lion & Epic Fury) - ZENDATA Cybersecurity.” Accessed May 19, 2026. https://zendata.security/2026/03/02/cyber-warfare-in-the-us-israel-vs-iran-conflict-roaring-lion-epic-fury/.
[6] “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA.” Accessed May 19, 2026. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.
[7] “Explainer: What Is Volt Typhoon and Why Is It the ‘Defining Threat of Our Generation’? | Hacking | The Guardian.” Accessed May 19, 2026. https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer.
[8] “US, UK to Impose More Sanctions on Russia after Bucha Killings | INTERNATIONAL POLITICAL NEWS - Business Standard.” Accessed May 20, 2026. https://www.business-standard.com/article/international/us-uk-to-impose-more-sanctions-on-russia-after-bucha-killings-122040600875_1.html.
[9] “Facebook Allows War Posts Urging Violence against Russian Invaders | Reuters.” Accessed May 19, 2026. https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/.
[10] “Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia | Reuters.” Accessed May 19, 2026. https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/
[11] “Why the Nayara Energy Crisis Demands India’s Immediate Tech Independence! - Haltdos - Enterprise Application Security & Delivery Platform | Haltdos.” Accessed May 19, 2026. https://www.haltdos.com/knowledge-base/why-the-nayara-energy-crisis-demands-indias-immediate-tech-independence/.
[12] National Imperative for Digital Autonomy. https://bdia.in/white-paper/Data-Swaraj-for-Secure-Digital-India_White%20Paper_V3.pdf
[13] “A Strategic Framework for Mitigating Electronic Hardware-Related National Security Risks in India.” Accessed May 17, 2026. https://www.orfonline.org/research/a-strategic-framework-for-mitigating-electronic-hardware-related-national-security-risks-in-india#_edn6.
[14] “ASML-Tata Electronics Semiconductor Fab: Can India Join the Chip Race?” Accessed May 19, 2026. https://www.indmoney.com/blog/stocks/india-semiconductor-gap-tata-asml-dholera-fab-28nm-vs-2nm-explained.

# BIBLIOGRAPHY

Bousquet, Antoine. The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity. New York: Columbia University Press, 2009.
Boyd, John R. “A Discourse on Winning and Losing.” Unpublished briefing, 1987.
Clausewitz, Carl von. On War. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.
Freedman, Lawrence. The Future of War. New York: PublicAffairs, 2017.
Joint Chiefs of Staff. Joint Publication 3-0: Joint Operations. Washington, DC: Department of Defense, 2022.
Kilcullen, David. The Dragons and the Snakes: How the Rest Learned to Fight the West. Oxford: Oxford University Press, 2020.
Kissinger, Henry A., Eric Schmidt, and Daniel Huttenlocher. The Age of AI: And Our Human Future. New York: Little, Brown and Company, 2021.
Libicki, Martin C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge: Cambridge University Press, 2007.
Mahnken, Thomas G., ed. Competitive Strategies for the 21st Century. Stanford, CA: Stanford University Press, 2012.
NATO Innovation Hub. Cognitive Warfare. Norfolk, VA: NATO Allied Command Transformation, 2021.
Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” International Security 41, no. 3 (2017): 44–71.
Rid, Thomas. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020.
Singer, P.W., and Emerson T. Brooking. LikeWar: The Weaponization of Social Media. Boston: Houghton Mifflin Harcourt, 2018.
Sun Tzu. The Art of War. Translated by Samuel B. Griffith. Oxford: Oxford University Press, 1963.
TRADOC. The U.S. Army in Multi-Domain Operations 2028. TRADOC Pamphlet 525-3-1. Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018.
Zuboff, Shoshana. The Age of Surveillance Capitalism. New York: PublicAffairs, 2019.
Huynen, J.-L., and G. Lenzini. "From Situation Awareness to Action: An Information Security Management Toolkit for Socio-Technical Security Retrospective and Prospective Analysis." In Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 213–224. 2017.
Huynen, J.-L., & Lenzini, G. (2017). From Situation Awareness to Action: An Information Security Management Toolkit for Socio-technical Security Retrospective and Prospective Analysis. Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 213–224. https://doi.org/10.5220/0006211302130224.
Chiriac, O. "Military Applications of Cognitive Sciences: Cognitive Warfare, a Matter of Perception and Misperception." International Scientific Conference "Strategies XXI" 18 (2022): 474–484. https://doi.org/10.53477/2971-8813-22-55.
Gherman, L. "Defence Architecture Based on Information Age OODA Loop." Review of the Air Force Academy 15, no. 3 (2017): 111–118. https://doi.org/10.19062/1842-9238.2017.15.3.13.

ANNEX

# OBJECTIONS AND REBUTTALS

Any argument that places MDO within the larger STCB must confront several important objections. These objections are not trivial. They arise because MDO is already a sophisticated doctrine, the STCB framework appears expansive, and kinetic force remains indispensable to warfare. Addressing these objections is essential if STCB-secured MDO is to be understood not as a rhetorical replacement for existing doctrine, but as a necessary refinement of how modern military power should be conceived.

**Objection One: MDO already incorporates information, cyber, cognitive, and competition below the war level. The STCB adds nothing new**

The first objection is that MDO already addresses many of the issues STCB claims to address. MDO does not imagine war purely as a clash of armies on land. It includes cyber, space, the electromagnetic spectrum, information operations, and competition below the threshold of armed conflict. It recognizes that modern conflict is continuous, multidomain, and technologically mediated. Therefore, it may be argued that STCB adds little beyond a new vocabulary for concerns that MDO already incorporates.

The objection confuses operational integration with strategic scope. MDO integrates cyber and information operations into military campaigns. It does not address who owns the platforms through which information flows, who controls the algorithms that shape what populations believe, who manufactures the semiconductors used in military hardware, or whose cloud infrastructure hosts a nation's intelligence and logistics data. These are not operational questions, but substrate conditions that determine whether operational plans function as designed. MDO operates at the level of force employment, while STCB operates at the level of strategic condition-setting. The argument is not that MDO is wrong, but that it is incomplete unless it is nested within this wider framework.

**Objection Two: STCB Is Too Broad to Be Operationally Useful**

A second objection is that the STCB may be too broad to be analytically useful. If social cohesion, public trust, data systems, supply chains, algorithms, financial networks, media ecosystems, institutional legitimacy, and cognitive confidence are all part of the battlespace, then the concept risks becoming so expansive that it explains everything and therefore explains nothing.

This is a genuine concern. Any useful strategic concept must clarify rather than merely enlarge the field of analysis. However, the breadth of STCB reflects the actual expansion of conflict rather than conceptual excess. Contemporary adversaries do not respect the neat boundaries between military and civilian systems, between war and peace. The battlespace has broadened as the systems that sustain modern states have grown more interconnected.

The value of STCB lies precisely in showing how these elements interact. A cyberattack is not merely technical if it erodes trust in the state. A supply-chain disruption is not merely economic if it constrains military readiness and creates political pressure. STCB does not claim that every social or technical issue is automatically a military problem. It claims that under conditions of strategic competition, these systems can become pathways through which adversaries shape military and political outcomes.

**Objection Three: Kinetic Force Still Decides Wars**

A third objection is that the STCB argument risks overstating the importance of non-kinetic systems. Wars are still ultimately decided by force. No amount of narrative shaping or cognitive manipulation can substitute for the hard realities of military power.

This objection is correct, but incomplete. STCB does not abolish the battlefield. It explains why some armies arrive at the battlefield already advantaged or already compromised. Kinetic force remains essential, but its effectiveness depends increasingly on the condition of the wider system that generates, directs, and sustains it.

A military force fights through command systems, data flows, supply chains, communication networks, political authority, and public morale. If these systems are resilient, kinetic power can be applied with confidence. If they are degraded, even advanced military forces can hesitate, miscalculate, or lose coherence. The argument is therefore not that future wars will be won without fighting. It is that the outcome of fighting will increasingly be conditioned before the first major engagement begins.

**Objection Four: No Nation Can Achieve Full STCB Sovereignty in an Interconnected World**

India faces real resource constraints, bureaucratic complexity, competing modernization priorities, and immediate operational challenges along its borders and maritime approaches. It cannot secure every platform, indigenize every supply chain, control every algorithm, or eliminate every technical dependency.

This objection is valid if STCB-secured MDO is misunderstood as a demand for complete autonomy or total security. The objective is not perfect control, but strategic prioritization. India needs to identify which dependencies are tolerable, which are risky, and which are unacceptable under crisis conditions.

Some dependencies can be managed through redundancy and trusted partnerships, while some require essential domestic capability. The central prerequisite is awareness. A state cannot mitigate vulnerabilities it has not mapped, it cannot protect critical systems it does not recognize as critical. It cannot build MDO on hidden dependencies and expect resilience during conflict.

### Objection Five: India Should Focus First on Basic Military Jointness

A final objection is that India has not yet fully solved the problem of jointness. It may therefore be premature to speak of STCB-secured MDO when the more immediate tasks are theatre commands, service integration, ISR fusion, and operational interoperability. India should first get the military basics right before expanding the concept into society, technology, and cognition.

This objection identifies a sequencing problem but draws the wrong conclusion. India must certainly strengthen jointness. However, jointness and STCB resilience cannot be treated as sequential projects, with one completed before the other begins. If India builds military jointness without simultaneously examining the substrate on which jointness depends, it risks creating an integrated force that remains vulnerable at the foundations.

The practical answer is parallel development. India must build theatre-level military integration while also mapping critical dependencies, improving information assurance, strengthening cognitive resilience, and securing critical infrastructure. This is the condition that will make the Indian MDO credible.



C-21, 3rd Floor, Qutub Institutional Area, New Delhi, India - 110016.
Phone: 011-43104566 | Email: office@csdronline.com | Web: www.csdronline.com | Twitter:@CSDR_India