Issue Brief

February 2026
No: 490

Cognitive Warfare and the Limits of Military-Centric National Security Thinking: Structural Challenges and Implications for India

Colonel Rakesh Kumar Singh

Cognitive Warfare and the Limits of Military-Centric National Security Thinking: Structural Challenges and Implications for India

Abstract

Contemporary conflict is increasingly characterised by efforts to shape perception, belief and decision-making rather than by application ofkinetic force alone. This evolution has foregrounded the cognitive domain of warfare, wherein the human mind becomes a contested battle space. While major powers now acknowledge the strategic significance of this domain—as reflected in recent doctrinal and policy discourse—national security frameworks remain largely organised around military-centric, sectoral and episodic models of response. This paper argues that the challenge posed by cognitive warfare is fundamentally architectural rather than informational or technological in nature. By examining the defining characteristics of cognitive warfare, its operational consequences and the limits of existing security paradigms, the paper highlights a persistent gap between recognition and implementation. Using the Indian context as an illustrative case, it demonstrates how institutional fragmentation, civil–military disconnects, procedural tempo mismatches and societal exposure through open information ecosystems create systemic vulnerabilities. The article reframes cognitive warfare as a structural challenge to national security systems and outlines key design principles—such as integration, continuity, credibility, speed and societal resilience—that logically flows from the nature of the cognitive domain. It concludes by suggesting that addressing cognitive domain threats require rethinking how national security is conceptualised and organised in an era of persistent cognitive contestation.

Keywords: Cognitive Warfare, Cognitive Domain Conflict, National Security Architecture, Strategic Escalation, Decision Making Autonomy, Civil–Military Coordination

Introduction

Contemporary battlefield is increasingly characterised not by decisive engagements alone, but by sustained efforts to shape perceptions, beliefs and decision-making processes of societies and political leaderships. Advances in digital communication, artificial intelligence and behavioural sciences have expanded the ability of state and non-state actors to influence how adversaries interpret reality itself. This has given rise to what is now widely described as the 'cognitive domain of warfare', wherein the humanmind becomes both the target and the terrain of contestation(Rickli, J.M. andMantellassi, F. 2023) and (Cluzel, F.D. 2020).

Cognitive warfare differs fundamentally from traditional information or psychological operations. While information warfare seeks to control narratives and psychological operations aim to influence morale or behavior in specific contexts, cognitive warfare targets the deeper mechanisms of perception, belief formation and decision-making across populations. It operates persistently across the peace–crisis–war continuum, often below the threshold of armed conflict and exploits the openness of modern societies to achieve strategic effects without overt coercion (Cluzel, F.D. 2020). As a result, its consequences are not confined to military outcomes but extends to political stability, societal cohesion and national will.

Recognition of this evolving domain is increasingly evident in the strategic discourse of major powers. Contemporary national security strategies and doctrinal writings now emphasises the importance of influence, information environments and emerging technologies that shape human cognition.The United States' National Security Strategy of 2025, for instance, underscores the centrality of information, technological dominance and societal resilience as components of national power (The White House, 2025). Similar concerns are reflected in NATO's conceptual explorations of cognitive warfare and in policy literature emerging from Europe and East Asia (Cluzel, F.D. 2020).Collectively, these developments suggest a growing awareness that future conflicts will be decided as much in the cognitive domain as in the physical one.

Yet, despite this recognition, national security frameworks remain largely rooted in military-centric and sectoral approaches. Institutional responses continue to privilege armed forces, technological superiority

and episodic information management, while the cognitive domain—by its very nature— cuts across civil–military boundaries, state and society as well as wartime and peacetime distinctions. This misalignment between the character of the threat and the structure of national responses constitutes a critical strategic vulnerability (Rickli, J.M. andMantellassi, F. 2023).

This paper argues that cognitive warfare exposes the limits of traditional military-centric national security thinking. It contends that effectively countering cognitive-domain threats requires a shift towards a whole-of- nation approach that integrates military, governmental, societal and informational capabilities.

Conceptualising Cognitive Warfare

The effort to influence the perceptions and decisions of adversaries is not a novel feature of conflict. Throughout history, states have employed propaganda,deception and psychological pressure to weaken opponents and shape outcomes.What distinguishes cognitive warfare from these earlier practices is not the intent to influence, but the systematic elevation of human cognition itself as a contested domain of warfare (Bernal, A. 2020) and (Claverie, B.and Cluzel, F.D. 2022).

Cognitive warfare can be understood as a form of conflict that targets the mechanisms through which individuals and societies perceive reality, form beliefs and make decisions (Rickli, J.M. and Mantellassi, F. 2023).Unlike information warfare, which focuses on controlling the flow, content, or accessibility of information, cognitive warfare seeks to shape how that information is interpreted and internalised (Maschmeyer, L. 2021).Similarly, while psychological operations traditionally aim to influence morale or behaviour in specific operational contexts, cognitive warfare operates at a deeper and broader level, seeking to alter collective perception, trust and sense-making processes across entire populations.

A defining feature of cognitive warfare is the treatment of the human mind as an 'operational battlespace' (Cluzel, F.D. 2020) and (Claverie, B. and Cluzel, F.D. 2022). In this domain, the objective is not merely to persuade or mislead temporarily, but to influence enduring cognitive frameworks—how threats are perceived, how legitimacy is assigned and how choices are evaluated. This makes cognitive warfare inherently societal in scope, extending beyond military forces to civilian populations, political institutions and cultural narratives.

Cognitive warfare is also characterised by its persistence across the peace– crisis–war continuum (Cluzel, F.D. 2020).Rather than being confined to periods of overt hostilities, cognitive operations are conducted continuously, often below the threshold of armed conflict. Their effects accumulate over time, shaping strategic environments long before kinetic force is employed and constraining decision-making during crisis or war. The difficulty of attribution and the plausibility of deniability further enhance the attractiveness of cognitive warfare as a strategic tool.

Finally, cognitive warfare differs from earlier influence-based approaches inits emphasis on decision-shaping rather than direct behavioural control. Success in the cognitive domain is achieved not by compelling specific actions, but by structuring the informational and perceptual environment in ways that narrow perceived choices and predispose adversaries towards certain decisions (Maschmeyer, L. 2021) and (Maschmeyer, L. 2024).Thisshift has profound implications fornational security, as it challenges traditional assumptions about deterrence, escalation and the boundaries between war and peace.

Global Recognition of the Cognitive Domain:Awareness without Integration

The growing prominence of the cognitive domain is increasingly reflected in the strategic discourse of majorpowers (Rickli, J.M. andMantellassi, F. 2023).Contemporary national security strategies, doctrinal writings and policy debates acknowledge the fact that, future conflicts will not only be shaped by military force but also by the ability to influence perceptions,control narratives and strengthen societal resilience.This shift inlanguage signals an emerging consensus that the human cognitive space constitutes a critical arena of

strategic competition.

The United States' National Security Strategy, published in 2025, exemplifies this evolution in strategic thinking. While remaining firmly grounded in traditional pillars of national power—military strength, economic capacity and technological superiority—the document places notable emphasis on information environments, emerging technologies and resilience against foreign influence (The White House, 2025). References to disinformation, influence operations and protection of democratic societies underscore an awareness that adversaries increasingly seek to shape outcomes by targeting cognition rather than territory alone.Similar concerns are echoed in NATO'sconceptual explorations of cognitive warfare and in European policy literature addressing hybrid and grey-zone conflict (Cluzel, F.D. 2020).

However, this growing recognition has not been accompanied by a corresponding transformation in national security structures or strategic frameworks— however, tracing of cognitive-domain challenges remains dispersed across multiple sectors viz. defence, technology, information and governance, that too without any unifying conceptual or institutional framework. Cognitive warfare is often acknowledged as a concern, rather than being articulated as a distinct domain requiring integrated planning, dedicated capabilities, or sustained civil–military coordination.

The preceding review of contemporary strategic documents indicates that, while influence operations, disinformation and societal resilience are increasingly acknowledged, however, they are addressed across separate policy domains like defence modernisation, technological competitiveness and democratic protection, rather than under an integrated cognitive-security framework. This entails that, the organisation continues to see national security from the lens of military threat, technological competition and crisis response. Hence, existing frameworks are structured primarily to respond to episodic events, identifiable adversarial actions and escalation scenarios involving kinetic activities. Cognitive warfare, by contrast, is characterised by persistence, deniability and operation within civilian information ecosystems that fall outside traditional military jurisdictions.The structural characteristics viz. continuity across peace and crisis, decision-shaping rather than force application, and societal embedding, do not map neatly onto security architectures designed for bounded crisis and domain-specific responses. In this sense, the emerging gap between recognition and implementation is less a question of political intent than of institutional design (Rickli, J.M. andMantellassi, F. 2023).While major powers increasingly acknowledge the cognitive dimension of conflict, their systems remain organised around legacy distinctions between military and civilian spheres, external and internal security and war and peace. The resulting misalignment underscores the need to reconsider how national security frameworks conceptualise and coordinate responses to persistent cognitive domain contestation.

The Indian Context: Structural Vulnerabilities in the Cognitive Domain

India's exposure to cognitive-domain contestation is shaped less by adversarial intent than by the structural characteristics of its political, societal and security architecture.As a pluralistic democracy with an open information environment (Zuboff, S. 2019),India generates a densely contested cognitive space in which multiple narratives, identities and interpretations coexist and compete. While this pluralism is a democratic strength, it also increases the susceptibility of the information ecosystem to sustained influence operations aimed at amplifying distrust, polarisation and perceptual fragmentation. In such an environment, cognitive effects can accumulate over time without any single triggering event, thus complicating detection and response.

A central vulnerability arises from institutional reflexes shaped by legacy paradigms of information control and secrecy.Historically, national security institutions have been oriented towards guarding sensitive information and preventing leakage rather than proactively engaging contested cognitive spaces. This orientation, while appropriate in conventional security contexts, is ill-suited to a domain wherein influence operates through open platforms, social discourse and societal trust rather than classified channels. The result is a persistent asymmetry between the openness of the cognitive environment and the state's predominantly defensive posture within it.

Fragmentation across functional domains further compounds these Challenges (Maschmeyer, L. 2021).

Responsibilities related to information management, influence, public communication and psychological resilience are distributed across military, intelligence, civilian and regulatory institutions, each operating within their own silos. In the absence of a unifying cognitive-security framework, responses remain 'episodic, reactive and sector-specific'. This mirrors the broader pattern identified in global strategic thinking, where recognitionofcognitivethreatshasnottranslatedintointegratedinstitutional design. In India's case, this fragmentation is particularly consequential given the scale and diversity of the societal terrain involved.

Civil–military coordination represents another structural constraint. Existing coordination mechanisms are optimised for kinetic contingencies, crisis response and clearly attributable threats. Cognitive warfare, by contrast, unfolds persistently across civilian domains, often without a clear transition point from peace to crisis. This creates coordination gaps in which responsibility is diffused and ownership becomes ambiguous. The cognitive domain thus falls between institutional boundaries, neither fully military nor fully civilian, thus reducing the effectiveness of both.

The mismatch between the tempo of cognitive warfare and bureaucratic processes further accentuates these vulnerabilities. Cognitive influence operations operate at high speed, high volume and with cumulative effect, while decision-making within state institutions remain deliberative and sequential by design. Delays that are tolerable in conventional policy cycles can prove strategically costly in a domain wherein perception and narrative hardens rapidly. This temporal asymmetry allows adversarial influence to establish cognitive footholds before countervailing responses are formulated.

India's reliance on globally networked digital platforms introduces an additional layer of exposure (Zuboff, S. 2019) and (Paul, C. and Matthews, M. 2016). External social media ecosystems enable influence operations that transcends territorial boundaries and jurisdictional controls, embedding cognitive contestation directly within everyday social interaction. Traditional instruments of state power, designed for territorially bounded threats, struggles to operate effectively within these diffuse and transnational environments. As a result, cognitive-domain vulnerabilities extend well beyond formal security institutions into society at large.

Importantly, these challenges should not be interpreted as uniquely Indian deficiencies. Rather, they reflectstructural tensions inherent to open, democratic societies confronting a domain of conflict that collapses distinctions between war and peace, internal and external security andcivilian & military spheres. India's experience thus illustrates a broader analytical point:cognitive warfare exposes the limits of security architectures designed for episodic, kinetic conflict when confronted with persistent, perception-driven contestation.

Taken together, these structural characteristics underscore why cognitive warfare cannot be addressed through incremental adaptation of existing frameworks alone. The challenge is not in lack of awareness or intent, but is in misalignment between the natureof the threat andthe architecture ofnational response. In this sense, India's cognitive-domain vulnerabilities are best understood not as operational shortcomings, but as symptoms of a deeper structural mismatch that demands rethinking how national security is conceptualised and organised (Rickli, J.M. and Mantellassi, F. 2023) and (Freedman, L. 2013).

Structural Implications for National Security Reform in the Cognitive Domain

The preceding analysis highlights a persistent misalignment between the characteristics of cognitive warfare and the institutional architectures through which national security is conventionally organised (Rickli, J.M.and Mantellassi, F. 2023).If cognitive domain contestation is continuous, societal in scope and centred on shaping perception and decision-making, then incremental adjustments within existing military-centric frameworks are unlikely to be sufficient. Rather than proposing specific organisational solutions, the following structural implications outline the design principles that logically emerge from the nature of the cognitive domain and the challenges it poses to contemporary national security systems.

Cognitive warfare requires institutional architectures designed for sustained and continuous engagement rather than episodic coordination. Because cognitive-domain contestation unfolds persistently across peace and crisis, effective response depends on mechanisms capable of long-term integration across governmental functions, rather than ad hoc mobilisation triggered by discrete events or crisis.

Structural coherence matters more than intent in the cognitive domain. The effectiveness of responses to cognitive warfare is determined less by political intent or messaging clarity than by the presence of institutional arrangements that enables coordination, consistency and continuity across domains. Without such coherence, even well-intentioned efforts becomes fragmented and reactive.

Credibility functions as a strategic asset that cannot be generated during crisis (Bernal, A. 2020) and (Mazarr, M. 2015). In the cognitive domain, trust and legitimacy are cumulative and path-dependent, requiring sustained engagement and coherence overtime rather than reactive communication during moments of escalation. Once eroded, credibility cannot be rapidly restored through institutional or informational surges.

The speed and coherence of response in the cognitive domain depends on architectural alignment rather than directive authority. Cognitive warfare exposes the limits of sequential and procedural decision-making, highlighting the importance of institutional designs that enables timely, coordinated responses while preserving legitimacy and accountability.

Cognitive-domain reform implies the principled management of civil–military boundaries rather than their erosion. As cognitive warfare blurs conventional distinctions between civilian and military spheres,effective response depends on clearly articulated principles governing roles, responsibilities and coordination across these domains, rather than adhoc expansion of authority.

Finally, societal resilience emerges as a core security function rather than a secondary outcome (Bernal, A. 2020). Cognitive warfare shifts elements of national security beyond exclusive state control, underscoring the importance of societal awareness, adaptive capacity and cognitive resilience as integral components of national security architecture.

Conclusion

Cognitive warfare represents a fundamental shift in the character of contemporary conflict (Cluzel, F.D. 2020), challenging long-standing assumptions that underpins national security thinking. By elevating human cognition as a contested domain, cognitive warfare operates persistently across the peace– crisis–war continuum, exploits societal vulnerabilities and shapes strategic outcomes without relying on overt kinetic force. The resultant effects are cumulative, indirect and difficult to attribute, yet strategically consequential in constraining decision-making, eroding trust and reshaping perceptions of legitimacy and success.

This article has argued that while major powers increasingly recognise the cognitive dimension of conflict, existing national security frameworks remain structurally ill-suited to address it. The gap is not one of intent or awareness, but of architecture. Military-centric, sectoral and episodic approaches— optimised for clearly bounded crisis and attributable threats—struggle to cope with a domain that is continuous, civilian-embedded and perception- driven. As illustrated through the Indian context, cognitive warfare exposes systemic vulnerabilities arising from institutional fragmentation, civil–military disconnects, procedural tempo mismatches and reliance on open information ecosystems beyond traditional state control.

The central contribution of this article lies in reframing cognitive warfare as an architectural challenge rather than merely an informational, technological, or communicativeproblem (Rickli, J.M. and Mantellassi, F. 2023). Addressing cognitive domain threats therefore requires more than enhanced messaging or incremental institutional adjustments; it demands a re-examination of how national security systems are designed, co-ordinated and aligned with persistent cognitive contestation. Structural principles such as integration, continuity, credibility, speed and societal resilience emerge not as policy preferences, but as logical imperatives derived

from the nature of the domain itself.

As cognitive warfare continues to evolve, its strategic salience is likely to increase. Future research must therefore move beyond definitional debatesto examine how national security architectures can adapt to domains that blur the boundaries between war and peace, state and society and military and civilian spheres. Addressing this challenge will be central to preserving strategic autonomy and decision-making freedom in an era wherein the mind itself has become a battleground.

Works Cited

Bernal, A. et al., *Cognitive Warfare: An Attack on Truth and Thought* (2020). Baltimore: Johns Hopkins University and NATO Allied Command Transformation.

Claverie, B. and Chuzel, F.D. (2022). Cognitive Warfare: The Advent of Cognitics. *HAL Open Science.*https://hal.science/hal-03725533.

Cluzel, F.D. (2020). Cognitive Warfare. *NATO Innovation Hub*.

Freedman, L. (2013). *Strategy: A History.* Oxford: Oxford University Press.

Maschmeyer, L. (2021). Subversion, Cyber Operations, and the Strategic Logic of Influence. *International Security*, 46 (3). Pp. 97–136.

Maschmeyer, L. (2024). *Subversion:The Strategic Logic of Influence.* Cambridge: Cambridge University Press.

Mazarr, M. (2015). Mastering the Gray Zone. Carlisle, PA: USArmy War College Press.

National Security Strategy of the United States ofAmerica (2025). *The White House*.

Zuboff, S. (2019). *The Age of Surveillance Capitalism.* London:Profile Books.

Paul, C. and Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model*. Santa Monica: RAND Corporation.

Rickli, J.M.and Mantellassi, F. (2023). Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century. *GCSP Policy Brief No. 9.*

Rickli, J.M. and Mantellassi, F. (2023). Cognitive Warfare:A New Form of Strategic Competition. *Survival65 (2)*. Pp. 7-28.

.

About the Author

Colonel Rakesh Kumar Singh was commissioned into the Infantry and is an alumnus of the National Defence Academy, Defence Services Staff College, and College of Defence Management. He has served in varied operational environments, including desert, semi-developed, high-altitude, and counter-insurgency areas. He has held key staff appointments at Command Headquarters, with responsibilities encompassing information outreach and digital and social media engagement, and has also served in instructional roles at the Officers Training Academy, Chennai. He is presently a Research Fellow at Savitribai Phule Pune University.