



Centro Alti Studi Difesa

Scuola Superiore Universitaria

STRATEGIC LEADERSHIP JOURNAL

CHALLENGES FOR GEOPOLITICS
AND ORGANIZATIONAL DEVELOPMENT

Numero 4 – Anno 2025

Centro Alti Studi Difesa – Scuola Superiore Universitaria

Direzione e Redazione Palazzo Salviati
Piazza della Rovere, 83, 00165 – Roma
www.unicasd.it

Tel 06 4691 23208 – e-mail: irad.usai@casd.difesa.it

ISSN 2975-0148 – ISBN 979-12-5515-125-8

Sara Russo

Ph.D. candidate in Defence and Security Studies at the Centre for High Defence Studies (CASD) and the University of Turin, focusing on leadership, social network analysis, and cognitive warfare

Yordanka Peteva

Assistant professor in the Department of National security at Nikola Vaptsarov Naval Academy - Varna, Bulgaria.

Ph.D. candidate at Nikola Vaptsarov Naval Academy, Master's degree in psychology.

FRAMING THE UNFRAMED: WHY STRATEGIC LEADERSHIP NEEDS A COHERENT UNDERSTANDING OF COGNITIVE WARFARE

ABSTRACT

As contemporary conflict gradually extends into the cognitive domain, strategic leaders encounter a dilemma: they are expected to respond to a phenomenon that, in many respects, is still undefined. Although the term *cognitive warfare* now circulates widely in policy documents and military scholarship, its boundaries remain unsettled. Given this conceptual fragmentation, the present article adopts an integrative conceptual review approach to identify convergences and offers a preliminary synthesis that situates cognitive warfare in relation to neighbouring constructs.

1. Introduction – The Cognitive Turn in Warfare

The concept of Cognitive Warfare (CW) has evolved from theoretical contemplation to strategic reality in recent years. References to CW appear in NATO planning documents and circulate with increasing frequency in Western defense discourses¹, yet the term remains unsettled. Its growing visibility has not resolved contentious over meaning; instead, the variation in how CW is described highlights both the strategic sensitivity and its relative conceptual underdevelopment. Scholars and practitioners alike seem to recognise that CW points toward the foundational processes through which individuals and societies interpret, decide, and act².

To intensify this debate and the conceptual ambiguity, a crowded taxonomy emerges that often obscures more than it clarifies. A range of related concepts, including psychological operations (PsyOps), information operations (InfoOps), influence activities, and information warfare (IW), are regularly used interchangeably, even though they differ in scope, intended audience, and doctrinal lineage. Such collapsing of terms tends to generate a kind of conceptual «fog of war»³ that complicates both operational planning and ethical evaluation. Without clearer boundaries, the cognitive dimension risks becoming a convenient rhetorical label rather than a domain with analytical and practical utility. The strategic implications of

¹ BERNARD CLAVERIE - BENOÎT PRÉBOT - NATHAN BUCHLER - FRANÇOIS DU CLUZEL, Cognitive Warfare: The Future of Cognitive Dominance, Papers presented at the first NATO Scientific Meeting on Cognitive Warfare, Bordeaux, France, 21 June 2021, pp. 2-1, available at: <https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf>

² BERNARD CLAVERIE et al., Cognitive Warfare..., op. cit., pp. 2.1 – 2-7.

³ CLAUSEWITZ, C. VON, On war, Princeton 1976, Book 1, Ch.3 pp. 100. A phrase that is now often used to describe the complexity of nowadays military conflicts (The Fog of War was the name of Errol Morris's 2004 award-winning documentary). Clausewitz is frequently credited with coining the phrase "fog of war", but it is in fact a paraphrase of his statement that «war is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty».

this uncertainty are far from trivial. When doctrinal terms remain fluid, responsibility for cognitive-related activities becomes fragmented, and the development of both counterinfluence measures and defensive preparedness proceeds unevenly. Therefore, strategic readiness requires conceptual clarity.

In this light, the present article advances the view that, despite its growing prominence, Cognitive Warfare still lacks the coherent conceptual scaffolding and shared taxonomy needed for systematic analysis or robust doctrinal formulation. To address this gap, the study undertakes an integrative conceptual review, comparing definitions to map areas of convergence, divergence, and unresolved tension.

How can Cognitive Warfare be conceptually framed and analytically distinguished from adjacent concepts to enable coherent research, policy, and strategic practice?

The article proceeds in a structured sequence that mirrors the logic of the inquiry. Section 2 sets out the methodological orientation that guides the analysis. Section 3 maps the definitional landscape and introduces a comparative matrix that highlights the boundaries of what CW plausibly includes - and what it does not. Section 4 proposes an integrated working synthesis, while Section 5 shares the leadership and policy implications. Section 6 concludes by reflecting how definitional precision has become a strategic requirement rather than a merely conceptual concern.

2. Methodology⁴

This article proposes an integrative conceptual review⁵⁻⁶ to clarify the definition of Cognitive Warfare (CW) as delineated by the most prominent doctrinal and academic sources. The study approach maps the definitional foundations⁷ and identifies areas of convergence, ambiguity, and divergence that presently obstruct cumulative research and cogent policy development. The process, informed by integrative reviews⁸, in contrast to systematic reviews, prioritise theoretical representation over exhaustive coverage, concentrating on sources that elucidate foundational perspectives, influence doctrine, or present unique contributions. The analysis followed a purposive theoretical sampling⁹ to include authoritative definitions, both from doctrine and academic sources that, at present, influence military doctrine, policy discourse, and academic discussion.

3. The Fragmented Landscape of Cognitive Warfare

3.1 Terminological Confusion and Doctrinal Overlaps

Cognitive Warfare (CW) has not emerged from a single doctrinal lineage but from a constellation of overlapping traditions. The literature on CW exhibits what might be described as a terminological overload. Across military, psychological, security and communication studies, terms such as PsyOps, InfoOps, IW, IO, and CW are frequently employed as near-synonyms, however they differ in scope, intent, and theoretical ground. This confusion is not fortuitous. It originates from institutional inheritance and from the persistence of disciplinary silos: psychology emphasising behavioural modification, military studies privileging command and control (C2), communication theory focusing on narrative and media systems.

⁴ CALLAHAN J. L., Constructing a Manuscript: Distinguishing Integrative Literature Reviews and Conceptual and Theory Articles, in «Human Resource Development Review» 9/3 (2010), pp. 300–304. Although conceptual papers do not typically include a detailed methodological protocol, the analytical approach is informed by integrative literature review principles and therefore a concise methodological clarification is provided to ensure rigor and transparency.

⁵ TORRACO R. J., Writing Integrative Literature Reviews: Guidelines and Examples, in «Human Resource Development Review» 4/3 (2005), pp. 356–67.

⁶ SNYDER H., Literature Review as a Research Methodology: An Overview and Guidelines, in «Journal of Business Research» 104 (2019), pp. 333–39.

⁷ SUDDABY R., Editor's Comments: Construct Clarity in Theories of Management and Organization, in «Academy of Management Review» 35/3 (2010), pp. 346–57.

⁸ WHITEMORE R. – KNAFL K., The Integrative Review: Updated Methodology, in «Journal of Advanced Nursing» 52/5 (2005), pp. 546–53.

⁹ PATTON, M. Q., Qualitative Research & Evaluation Methods, 3. ed. Thousand Oaks, California: 2002, pp. 230.

The terminological fragmentation manifests across three main structurally distinct dimensions. Horizontal conflation arises from overlapping operational vocabularies across functions, services and agencies. Secondly, academic diffusion further dilutes the terminology, importing military vocabulary into academic contexts, stretching them beyond recognition. Lastly, partly due to the previous point, vertical confusion, often neglected in this definitional discourse, occurs when strategic, operational, and tactical levels are superficially acknowledged but not systematically integrated as defining criteria, leaving ambiguity about which concept operates at which level and impeding effective organizational response.

The terminological scenery reflects also the historical evolution. As Libicki observes, «to add to the confusion, circa 1996, what was “information warfare” became “information operations” within the military, ostensibly to subsume activities, such as propaganda, that could take place during peacetime»¹⁰. This change in language from warfare to operations weakened the Clausewitzian meaning of contest¹¹, replacing it with an administrative vocabulary that broadened scope while blurring intent. The U.S. monograph «*What Is Information Warfare*»¹², despite its intention to clarify categories within its ecosystem, paradoxically exacerbated the inflation of terminology by listing seven distinct activities under the same label (including psychological operations, electronic warfare, and cyberwarfare) proposing how the psyops lexicon was absorbed into a capacious, and increasingly ambiguous, informational umbrella.

Empirical evidence of this conflation appears across multiple scholarly sources. Ibrahim et al.¹³ further document this confusion through their systematic review, which indicates that the concepts of Cognitive Warfare and Psychological Warfare share significant elements across the communicative components outlined by Lasswell’s Model of Communication¹⁴, suggesting that the distinction between the two constructs remains tenuous and often unsettled. In a similar vein, Danet describes cognitive warfare as the logical «extension of information warfare»¹⁵, marking a qualitative continuity rather than a rupture: the contest expands from controlling information flows to shaping cognitive processing itself. This perspective emphasises the necessity of establishing clear boundaries within the expansive influence spectrum, rather than proliferating overlapping terminology. Hung and Hung’s¹⁶ analysis distinguishes information warfare, influence operations, cyber warfare, and cognitive warfare, as sequentially deepening layers of influence, moving from the control of information systems to the contestation of human cognition itself. Their framework, arose from the empirical standpoint grounded in Taiwan’s experience with Chinese disinformation campaign, suggesting how cognitive warfare transcends mere informational control to focus on the meaning-making processes that influence perception and decision-making.

3.2 Terminological Confusion and Definition Fragmentation

While the previous sub-section mapped doctrinal overlaps, an equally critical challenge lies in definitional fragmentation, the proliferation of competing or overlapping formulations of Cognitive Warfare across doctrines, institutions, and scholarly sources. This fragmentation is not merely semantic, it exposes divergent ontologies regarding the nature of cognition, influence, and warfare itself.

¹⁰ LIBICKI M., *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge 2007, pp. 17.

¹¹ CLAUSEWITZ, C. VON, *On war*, Princeton 1976, Book 1, Ch.2 pp. 95. The sentence refers to a broader shift of doctrine in which the Clausewitzian idea of war as a contest of opposing wills is increasingly reframed through the managerial language of operations and competition, expanding the scope of military activity while diluting its adversarial intent.

¹² LIBICKI M., *What Is Information Warfare*, Washington (NDU Press) 1995, pp.7.

¹³ IBRAHIM F., RHODE S., DASEKING M., *A Systematic Review of Cognitive and Psychological Warfare*, in «*The Defence Horizon Journal*» 2023, pp. 35–58.

¹⁴ LASSWELL H. D., *The structure and function of communication in society*, in «*The communication of ideas*», ed. Lyman Bryson (New York: Harper and Row 1948), pp. 37-51.

¹⁵ DANET D., *Cognitive Security: Facing Cognitive Operations in Hybrid Warfare*, in «*Proceedings of the 22nd European Conference on Cyber Warfare and Security (ECCWS)*» 22/1, Jyväskylä 2023, pp. 161-168.

¹⁶ HUNG T. – HUNG T., *How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars*, in «*Journal of Global Security Studies*» 7/4 (2022), pp. 1–18.

Source	Definition	Core Emphasis	Excluded or Overlooked Aspects
Innovation Hub of NATO-ACT and ENSC (2021)	“The art of using technologies to alter the cognition of human targets...” and “Cognitive warfare is thus an unconventional form of warfare that uses cyber tools to alter enemy cognitive processes...”	Technology-enabled manipulation of cognition; defensive awareness.	Downplays cultural, narrative, and emotional mechanisms; ambiguous on ethics.
Statto Maggiore della Difesa (Italy, 2023)	Defines CW as “...a multi-domain operation (or part thereof) that employs means, actions, and tools... influencing human behaviour and generating effects in the cognitive dimension, with the aim of gaining an advantage over the adversary”	Integration within multi-domain warfare; emphasis on behaviour influence and cognitive effects through cross-domain tools and means.	Limited treatment of civil-societal dimension, narrow definition of CW as an “operation”, minimal attention to friendly-side cognitive enhancement; and ethical safeguards.
Debidour Lazzarini (2024)	“...multifaceted concept encompassing strategies aimed at influencing the perceptions, behaviours and decisions of individuals, groups and societies in an immaterial conflict context”	Distinguishes IW (content-focused) from CW (cognitive-process-focused) and maps CW across multiple domains (offensive/defensive) and targets (individual/society).	Remains conceptually broad and partly overlapping with advanced influence / information warfare; briefly addresses legal/ethical and regulatory implications.
Danet (2023)	Considers CW “an extension of information warfare,” where the contest moves from data control to mental control.	Continuity with IW; introduce the concept of cognitive safety; epistemic shift.	Risks reductionism, viewing cognition as merely an information layer.
Ibrahim et al. (2023)	Identify CW as “... a historical descendant of the term psychological warfare”	Integrative behavioural approach; recognises cross-disciplinary roots; uses Lasswell’s Model of Communication to compare definitions.	Overlaps with psyops; limited doctrinal specificity.
Hung and Hung (2022)	“... activities undertaken to manipulate environmental stimuli to control the mental states and behaviours of enemies as well as followers in both hot and cold wars”	Hierarchical continuum; empirical grounding (Taiwan).	May oversimplify multi-directionality of influence.

Table 1- Comparative overview of principal definitions of Cognitive Warfare

A comparative reading of these definitions reveals the following recurring axes of divergence, or what we could interpret as patterns of fragmentation:

1. Ontology of Cognition: whether cognition is treated as a psychological, informational, or socio-cultural process;
2. Operational Scope: whether CW is a subset of information warfare or a meta-domain encompassing it;
3. Normative Orientation: whether CW is viewed as defensive (protecting cognition) or offensive (manipulating it).

These divergences generate an unstable conceptual terrain in which cognitive warfare oscillates between metaphor and doctrine. Some authors reduce it to a semantic intensifier for traditional

influence operations; others elevate it to a new operational domain. The lack of shared criteria, what counts as cognitive effect, attack or defense, prevents cumulative theorisation. But why does terminology matters? Terminological confusion is not a mere academic nuisance. Each definition reconfigures responsibilities, ethics, and scope of action. If CW is framed as psychological warfare, it falls under behavioural sciences; if seen as information warfare, it belongs to cyber commands; if conceived as a meta-domain, it requires integrative leadership and inter-agency coordination. This semantic instability translates into fragmented policy, duplicated structures, and inconsistent education curricula. Hence, clarifying terminology is a prerequisite for conceptual coherence. Establishing a taxonomy of influence, from information control to meaning control, would allow strategic communities to align doctrine, research, and training around a common cognitive lexicon.

4. Toward Conceptual Integration

4.1 Analytical Boundaries Among Adjacent Concepts

A first step toward conceptual integration requires distinguishing Cognitive Warfare from adjacent concepts. While terminological confusion persists across agencies and disciplines, analytical clarity about conceptual boundaries remains achievable.

At the doctrinal level, the distinctions among these terms could be simplified and expressed through their respective ontologies (*Table 2*):

Concept	Primary Focus	Operational Domain	Core Objective
<i>PsyOps</i>	Behavioural targeting	Tactical	Compliance, demoralisation
<i>InfoOps</i>	Informational control	Operational	Information superiority
<i>Influence Operations</i>	Shaping decision-making ecosystems	Operational	Attitudinal change
<i>Information Warfare</i>	Strategic contest over data and systems	Strategic	Dominance, disruption
<i>Cognitive Warfare</i>	Cognitive capabilities and frameworks	Meta-domain	Cognitive superiority

Table 2 – Simplified comparative table

This comparative framework reveals a critical distinction often obscured by terminological overlap: while PsyOps, InfoOps, and Influence Operations function as discrete interventions, Cognitive Warfare operates at a higher order, targeting the cognitive capabilities (neurobiological substrate), processes (perception and reasoning), and frameworks (epistemic structures) through which information acquires meaning and constructs reality itself. This perspective reveals a critical distinction: cognitive warfare differs qualitatively from adjacent concepts in what it targets. PsyOps, InfoOps, and Influence Operations, despite their variations, target cognitive content (beliefs, attitudes, perceptions) seeking to modify what individuals and collectives think. CW, conversely, targets cognitive capacity, the underlying architecture through which any information is processed, evaluated, and integrated. Where traditional influence operations aim to win arguments, CW aims to compromise the cognitive infrastructure that enables coherent argumentation itself. The COVID-19 pandemic infodemia illustrates this distinction¹⁷: while disinformation campaigns disseminated false content (InfoOps), the compounding effect of information overload, source proliferation, and systematic trust erosion degraded populations' capacity to navigate the information environment altogether. National doctrines increasingly

¹⁷ BUCCI F.S. – CRISTOFARO F. – GIARDINO P.L., Infodemia e pandemia: la cognitive warfare ai tempi del SARS-CoV-2 (2021), pp. 1-7, DOI: 10.13140/RG.2.2.20229.68322.

recognize this qualitative shift. Within the Italian context, Stato Maggiore della Difesa¹⁸ represents one of the first national defense authorities to publish an official definition of cognitive warfare, providing a structured framework that stimulated the academic debate which promptly responded with fixes to tighten intent, scope, and boundaries¹⁹.

In emerging NATO doctrine, the cognitive domain is increasingly recognised as a distinct operational environment, complementing the traditional domains of land, air, maritime, space, and cyber²⁰, a discrete operational environment where military effects are generated, contested, and defended. This doctrinal categorization reflects institutional logic: if cognition is targeted, it must constitute a targetable domain requiring specific capabilities, command structures, and doctrine. Yet this framing risks analytical reduction. CW does not merely operate within a bounded cognitive space; it operates across all domains, shaping the cognitive conditions under which effects in all other domains are produced, perceived, and interpreted. This dual character suggests CW functions simultaneously as both: an operational domain when conceptualized through military doctrine (requiring dedicated capabilities, training, and command arrangements), and a meta-domain when analysed conceptually (conditioning the efficacy of operations across all other domains). The distinction matters strategically. Treating CW solely as a domain risks compartmentalization, that is assigning cognitive warfare to specialized units while leaving other formations cognitively unprepared. Conversely, recognizing its meta-domain character requires integrating cognitive considerations into cross-domain planning, leader development, and institutional resilience. The synthesis proposed here therefore positions CW as a domain for operational purposes and a meta-domain for strategic understanding, a duality that must inform both doctrine development and leadership education.

4.2 Four Core Convergences

Despite the conceptual volatility surrounding Cognitive Warfare, the definitional landscape is not entirely disordered. When examined comparatively, the major doctrinal and academic sources reveal some recurring features that cut across disciplinary and cultural boundaries. These convergences suggest that CW possesses a coherent conceptual core, even if its periphery remains contested. Across these divergent definitions, four elements recur with striking consistency.

1. First, cognition emerges as the primary target, not information flows or attitudes, but cognitive capabilities and framework themselves. CW operates at the level of perception, judgment, and meaning making, targeting how individuals and collectives process reality rather than what they believe. The intent is to alter decision-making capacity: not merely to change beliefs, but to compromise the cognitive mechanisms through which beliefs are formed and decisions are reached. This targeting operates through mechanisms extensively documented in cognitive psychology and organizational theory such as cognitive biases, epistemic trust, and collective sensemaking²¹⁻²²⁻²³⁻²⁴⁻²⁵.
2. Second, CW is characterized by its position along the continuum of conflict and its whole-of-society scope. This whole-of-society character implicates a wide range of actors beyond the military domain, including digital platforms, media organisations, technology firms, and civil

¹⁸ STATO MAGGIORE DELLA DIFESA (UGID), Cognitive Warfare – La competizione nella dimensione cognitiva, Ed. 2023.

¹⁹ MESSINA R., Cognitive Warfare: an urgent fix for the Italian definition in «Strategic Leadership Journal» 1 (2025), pp. 49-55.

²⁰ BERNARD CLAVERIE - BENOÎT PRÉBOT - NATHAN BUCHLER - FRANÇOIS DU CLUZEL, Cognitive Warfare: The Future of Cognitive Dominance, Papers presented at the first NATO Scientific Meeting on Cognitive Warfare, Bordeaux, France, 21 June 2021, pp. 3-1 – 3-5.

²¹ BERNARD CLAVERIE - BENOÎT PRÉBOT - NATHAN BUCHLER - FRANÇOIS DU CLUZEL, Cognitive Warfare: The Future of Cognitive Dominance, Papers presented at the first NATO Scientific Meeting on Cognitive Warfare, Bordeaux, France, 21 June 2021, pp. 4-1 – 4-14.

²² WEICK K. E., Sensemaking in organizations, Thousand Oaks (CA) 1995.

²³ BENSON B., Cognitive bias cheat sheet, in «Better Humans» (2016), available at: <https://betterhumans.pub/cognitive-bias-cheat-sheet-55a472476b18>

²⁴ SPERBER D. - CLÉMENT F. - HEINTZ C. - MASCARO O. - MERCIER H. - ORIGGI G. - WILSON D., Epistemic vigilance, in «Mind & Language» 25/4 (2010), pp. 359-393.

²⁵ LI E. - CAMPBELL C. - MIDGLEY N. - LUYTEN P., Epistemic trust: A comprehensive review of empirical insights and implications for developmental psychopathology, in «Research in Psychotherapy» 26/3 (2023).

society institutions, creating significant coordination challenges for strategic leadership. Unlike discrete psychological operations tied to specific campaigns or military targets, CW blurs multiple boundaries: peace-war, military-civilian, and combatant-noncombatant. Crucially, it proceeds sub-threshold, below both the awareness threshold (targets typically do not recognize cognitive manipulation is occurring) and the conflict threshold (interventions remain below the level that triggers conventional warfare responses or international law protections). This dual sub-threshold character distinguishes CW from overt influence and traditional military operations.

3. Third, definitions converge to strategic intentionality and bidirectional capacity. CW is framed as purposeful intervention into cognitive processes to achieve strategic objectives, distinguishing it from incidental influence or organic information exchange. Although the vast majority of literature focuses on cognitive degradation, a corresponding mirroring dimension addresses cognitive enhancement, such as the super soldier²⁶. This bidirectional potential distinguishes CW from purely antagonistic concepts. While commonly framed as “warfare” within adversarial contexts, the same mechanisms could equally serve “peacefare” applications: strengthening conflict resolution capacities, enhancing cross-cultural understanding, or building societal resilience against manipulation. The bidirectionality reflects the technology's inherent dual-use character rather than its ethical or strategic orientation.
4. A fourth element covers the cognitive warfare's vectors of action, that recurs across sources, though definitions diverge on which mechanisms are essential. Building on, but also reinterpreting, tripartite logic outlined by the *Stato Maggiore della Difesa*²⁷, it seems that contemporary CW operates through three spheres, individually or in combination: technological vector (eg.: algorithmic manipulation, AI-driven personalization, platform-mediated influence), neurobiological vector (eg: neurocognitive tools, pharmacological interventions, brain-computer interfaces), and psychological vector (eg: cognitive bias exploitation, emotional manipulation, persuasion techniques). What characterizes contemporary CW, in addition to what above mentioned, is the availability and frequent convergence of all three spheres, distinguishing it from traditional propaganda (predominantly psychological) or cyber warfare (purely technological). This multi-vector framework (*fig .1*) matters strategically, as effective countermeasures must address cognitive resilience, technological defenses, and neuroscientific understanding, rather than assuming any single intervention point is sufficient.

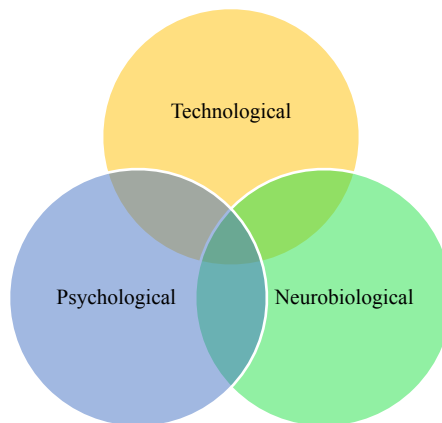


Figure 1 - The three-dimensional Cognitive Warfare's vectors of actions

These convergences suggest that despite terminological variation and doctrinal divergence, practitioners implicitly recognize CW as the continuous, sub-threshold targeting of cognitive

²⁶ DAVIDOVIC J. - FORREST S. C., Soldier Enhancement, Consent, and Long-Term Care: The Super Soldier Perspective, in « Journal of Bioethical Inquiry : An Interdisciplinary Forum for Ethical and Legal Debate» 22/3 (2025), pp. 707–720.

²⁷ STATO MAGGIORE DELLA DIFESA (UGID), Cognitive Warfare..., op.cit., pp. 14.

processes, both individual and collective, designed to compromise reasoning and decision-making capacity for strategic advantage.

This synthesis clarifies what cognitive warfare is, its ontological boundaries and distinguishing features. Yet definitional clarity, while necessary, does not automatically resolve how CW operates mechanistically or how strategic leaders should respond organizationally. Convergence on the nature of the target (cognition) does not settle questions about the architecture of defense; agreement that CW operates sub-threshold does not determine appropriate command structures; recognizing whole-of-society scope does not specify the distribution of responsibilities across military, civilian, and alliance institutions

5. From Conceptual Synthesis to Strategic Practice

5.1. Implications for Strategic Leadership

The emergence of Cognitive Warfare (CW) demands that strategic leadership evolve from managing information to safeguarding meaning. The following discussion translates the analytical convergences identified above into leadership-relevant capabilities. If cognition itself becomes a battlespace, then leaders are no longer peripheral observers of influence, they are its principal defenders.

This calls for a new form of *strategic leadership competency*: cognitive literacy. In this context, cognitive literacy refers to the ability to recognise that cognitive manipulation mechanisms exist, understand how influence operates across organisational and information environments, and maintain coherence and preserve trust under cognitive pressure within complex organisations. Cognitive literacy extends beyond traditional communication skills. It integrates psychological awareness, ethical reflection, and systemic understanding of influence dynamics. This literacy may be coupled with cognitive readiness²⁸, «a state of being that influences the correct interpretation of information and subsequent execution of appropriate behaviour»²⁹. In the absence of conceptual clarity, however, such readiness cannot be cultivated systematically.

Training curricula focus on decision-making, resilience, and strategic communication but, without a shared framework on how cognition is attacked or defended, these elements remain disconnected³⁰. Leadership institutions across the Euro-Atlantic community, such as the NATO Defense College, the European Security and Defense College (ESDC), and Italy's Centro Alti Studi per la Difesa (CASD), could reinforce CW-related content contributing to reducing this gap. These programmes could develop awareness of influence tactics, bias exploitation, and social contagion, while reinforcing ethical leadership and collective sensemaking. A practical first step, might include scenario-based simulations, wargaming exercises focused on perception management, and interdisciplinary seminars linking behavioural science with military decision-making, an approach already tested in Finnish defense education³¹.

A second implication is related to alliance interoperability. Distinct organizations use overlapping vocabularies (Information Operations, StratCom, influence activities) without a shared conceptual base. This delays coordination and limits the ability to determine what could constitute a “cognitive” action. Without a shared conceptual framework, multinational operations risk friction not from technological incompatibility but from semantic confusion. Interoperability among allied forces is weakened by doctrinal asymmetry. When partners label different activities as “cognitive,” operational cohesion is compromised at the level of planning and execution. Because CW functions as a whole-of-society targeting strategy, it necessarily requires a whole-of-government response to ensure coherence across policy, education, and operational domains.

²⁸ MORRISON J. - FLETCHER J. D., Cognitive Readiness, IDA Paper P-3735, Institute for Defense Analyses, 2002.

²⁹ CUEVAS H. M. - SCHMORROW D. D., Exploring Cognitive Readiness in Complex Operational Environments: Advances in Theory and Practice, «Proceedings of the Human Factors and Ergonomics Society Annual Meeting» 56/1 (2012), pp- 433–434.

³⁰ U.S. DEPARTMENT OF DEFENSE, Joint Publication 3-13: Information Operations, Washington, DC: Joint Chiefs of Staff 2022, pp. I-3 - I-13; GL-3 - GL4. The reference to JP 3-13 is used here by analogy: while the document concerns hybrid and information warfare, its articulation offers guiding insights applicable to cognitive warfare.

³¹ SAARI D. - GRAHN H., -HÄKKINEN T. - HAUTALA M., OSKARI VESTERINEN – MOILANEN P., Wargaming in Information Warfare Training: A Study of Finnish Officials, in «European Conference on Cyber Warfare and Security» 23/1 (2024), pp. 439–445.

For these reasons, conceptual readiness must precede strategic readiness. As the present analysis suggests, we cannot defend what we cannot define, although recognizing that asymmetric and emergent threats often force action ahead of conceptual consolidation. Conceptual clarity is not a matter of academic precision; it is a prerequisite for the coherence of command. By defining the boundaries and mechanisms of the cognitive domain, strategic communities can transform CW from an abstract concern into a manageable field of education, policy and operations. Conceptual clarity is not an academic luxury but the foundation of coherent command. Ultimately, preparing leaders for the cognitive era involves more than adopting new analytical tools; it entails cultivating a mindset capable of operating amid ambiguity. Cognitive resilience arises not from certainty but from disciplined reflection, moral coherence, and institutional trust. As warfare extends into perception and belief, leadership itself becomes a strategic capability. The integrity of human cognition constitutes the decisive frontier of twenty-first-century security. Only through conceptual convergence, anchored in leadership education, the Alliance can move from reactive posture to proactive cognitive resilience.

5.2. Limitations and Future Research Directions

The implications outlined above operate within four key constraints that define boundaries for the present analysis and signal directions for future research.

First, this study reflects predominantly Euro-Atlantic perspectives. While NATO, allied doctrines, and Western academic sources provide essential foundations, they conceptualize the cognitive domain through the normative frames of resilience, ethics, and human-centric defense. Alternative perspectives remain underexplored or analysed through a Western point of view. Future research could explore comparative doctrinal analysis and examine whether the convergences identified here hold across strategic cultures or whether CW remains inherently context-dependent.

Second, this article has focused on clarifying terminology and identifying convergences rather than constructing a complete integrative framework. The four convergences establish necessary foundations, but a full theoretical architecture requires empirical validation, mechanism modelling, and operational testing. In this respect, emerging computational methodologies are particularly promising. Recent analytical approaches quantify information disorder as a discernible component of cognitive warfare³², demonstrating how data-driven models can illuminate patterns of cognitive disruption and support doctrinal clarification. Future research should further explore how these computational techniques (ranging from machine-learning classifiers to immersive, metaverse-based behavioural simulations) can empirically ground CW concepts, test cognitive-effect hypotheses, and inform the development of measurable operational indicators.

Third, the legal and ethical dimensions of cognitive warfare require dedicated treatment. Questions of cognitive freedom, mental privacy, neuro-rights governance, and the boundaries of legitimate influence remain largely unaddressed. A central unresolved issue concerns the ethical boundary between legitimate cognitive defence and manipulative practices, and how strategic leadership can operate within this ambiguous space without undermining institutional trust, democratic accountability, or normative legitimacy. While international efforts, namely *UNESCO Recommendation on the Ethics of Artificial Intelligence*³³, *Council of Europe's Report on Neurotechnologies and Human Rights*³⁴, Chile's constitutional amendment on *neuro-rights*

³² GAETA A. - LOIA V. - LORUSSO A. - ORCIUOLI F. - PASCUIZZO A., Computational Analysis of Information Disorder in Cognitive Warfare, in « Online Social Networks and Media », 48 (2025) 100322, pp. 1-13.

³³ UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris 2021.

³⁴ IENCA M., Common human rights challenges raised by different applications of neurotechnologies in the biomedical fields, Council of Europe, October 2021.

(Law 21.383/2021)³⁵ and scholarly including Ienca and Andorno³⁶, Yuste et al.³⁷, and Bublitz³⁸ demonstrate growing recognition that existing legal frameworks may inadequately protect cognitive integrity. Future research could develop normative architectures that balance security imperatives with individual rights, addressing whether law of armed conflict, human rights law, and information ethics can regulate cognitive operations or whether new legal categories are required.

Fourth, empirical validation through operational contexts is essential. While this conceptual synthesis provides analytical clarity, testing its utility requires application in real-world scenarios. Research in contexts such as *Mare Aperto*³⁹ and the one involving Finnish national defense wargaming⁴⁰ demonstrates how CW concepts translate into leadership challenges, organizational responses, and communication dynamics under cognitive stress. Systematic case studies across diverse operational environments would test whether this framework enables coherent analysis, effective doctrine development, and measurable improvement in organizational cognitive resilience.

These limitations point toward a robust research agenda: comparative strategic culture analysis, complete framework integration, leadership training implications and normative architecture development, and empirical validation across operational contexts.

6. Conclusion

Cognitive Warfare (CW) has moved from theoretical speculation to operational relevance, yet the field remains conceptually unstable. Its definitions vary across doctrines, disciplines, and strategic cultures, producing analytical ambiguity and operational confusion. The term encompasses everything from psychological manipulation to data exploitation and perception control, without a shared understanding of scope or mechanism. This fragmentation obscures the human dimension of conflict. The level at which perception, trust, and leadership converge to determine strategic outcomes.

Conceptual readiness is a strategic necessity. Without a coherent analytical framework, discussions of CW risk devolving into rhetoric, and policy responses into improvisation. Establishing conceptual order is not merely an intellectual exercise; it is the first act of cognitive defense. This article contributed to the field by offering a structured synthesis of Cognitive Warfare by harmonising overlapping terminologies and identifying four core convergences (targeting of cognition, sub-threshold action, strategic intentionality with bidirectional capacity and multi-vector architecture) that together establish a coherent conceptual foundation for doctrine, leadership education, and policy development. Only when scholars and practitioners operate within a shared conceptual grammar can they design policies, training, and cognitive technological enablers that reinforce cognitive resilience rather than multiply confusion.

Leadership offers the pathway to this coherence. By integrating insights from psychology, organisational theory, and strategic studies, leaders can translate abstract notions of cognition into practical doctrine and training. They can identify when information becomes influence, when influence becomes manipulation, and when manipulation threatens institutional integrity. To lead in the cognitive domain is therefore to understand both its vulnerabilities and its ethical boundaries.

In conclusion, Cognitive Warfare should neither be dismissed as rhetorical innovation nor embraced as technological inevitability. It must be recognised as a global phenomenon interpreted through diverse strategic, cultural, ethical and, ultimately, holistic lenses. Developing shared conceptual ground, within and beyond the Euro-Atlantic community, together with normative safeguards for cognitive integrity, constitutes the foundation of strategic resilience.

³⁵ CHILE, LAW 21.383, Constitutional Amendment on the Protection of Mental Integrity and Neuro-Rights, Chile 2021.

³⁶ IENCA M. - ANDORNO R., Towards new human rights in the age of neuroscience and neurotechnology, «Life Sciences, Society and Policy», 13/1 5 (2017).

³⁷ YUSTE R. ET AL., Four ethical priorities for neurotechnologies and AI, «Nature», 551 (2017), pp. 159–163.

³⁸ BUBLITZ J. C. My Mind Is Mine!? Cognitive Liberty as a Legal Concept, in HILDT, E. - FRANKE, A. (eds) Cognitive Enhancement. Trends in Augmentation of Human Performance, vol 1. Springer, Dordrecht 2013.

³⁹ RUSSO S. Analisi dinamiche dei giocatori, In PANTALEO A. (ed.) Mare Aperto – The Home Front. Roma: Centro Alti Studi Difesa 2025, pp. 47–65, 10.5281/zenodo.17749749.

⁴⁰ SAARI D., Wargaming..., op.cit, pp. 439–445.



STRATEGIC LEADERSHIP
JOURNAL

