Strategic Security Initiative (SSI)
ADVANCING INSIGHT ON GLOBAL SECURITY

Cognitive Warfare in Context:

Doctrinal Innovation or Terminological Drift?

Implications for Information Operations Doctrine and Allied Strategy

Megi Benia

May 2026

www.ssi-policy.org

Cognitive Warfare in Context: Doctrinal Innovation or Terminological Drift?

Implications for Information Operations Doctrine and Allied Strategy

FIRST PUBLISHED May 2026 by SSI

Founder and Director: Megi Benia

Author: Megi Benia

Executive Summary

The increasing prominence of the concept of cognitive warfare within Euro-Atlantic security discourse, particularly in analytical and conceptual work associated with NATO, has generated a perception that a fundamentally new domain of conflict is emerging, one that targets human cognition rather than the informational environment. This policy brief advances the argument that such interpretations overstate the degree of novelty involved. While contemporary developments in artificial intelligence, data analytics, and digital communication infrastructures have significantly transformed the scale, speed, and precision of influence activities, the underlying strategic logic remains consistent with established doctrines of Information Operations and Psychological Operations.

Accordingly, cognitive warfare should be understood not as a distinct doctrinal innovation but as a manifestation of terminological drift driven by technological change and institutional dynamics. The proliferation of this concept risks generating fragmentation within policy and doctrinal frameworks, undermining coherence in Allied strategic planning. The brief therefore recommends that policymakers prioritize the modernization and integration of existing information operations doctrine, incorporating advances in cognitive science and artificial intelligence without introducing redundant conceptual categories.

The Emergence of Cognitive Warfare in Contemporary Discourse

Recent years have witnessed a marked expansion in the use of the term “cognitive warfare” across policy documents, academic analyses, and strategic assessments. This concept is frequently associated with the proposition that conflict has extended into a cognitive domain in which adversaries seek to manipulate perception, reasoning, and decision-making processes at both individual and societal levels[1;2]. Reports produced within NATO-affiliated scientific and strategic communities emphasize the convergence of neuroscience, behavioral psychology, and digital technologies as constitutive elements of this purportedly new battlespace[3].

Parallel developments in broader strategic literature, including assessments of technologically advanced state actors, underscore the growing integration of artificial intelligence, social media manipulation, and data-driven targeting into national security

[1] NATO Science and Technology Organization, *Cognitive Warfare* (Brussels: NATO STO, 2021), https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-4.pdf

[2] National Defense University, “Cognitive Warfare and the Changing Character of Conflict,” *Strategic Insights*, https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1055&context=strategic-insights.

[3] NATO Science and Technology Organization, *Cognitive Warfare* (Brussels: NATO STO, 2021), https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-4.pdf

strategies[4][5]. These developments are often presented as evidence that contemporary conflict transcends traditional informational and cyber domains. However, such interpretations risk conflating changes in technological capability with transformations in strategic function. The existence of new tools and infrastructures does not, in itself, imply the emergence of a fundamentally distinct domain of warfare.

Doctrinal Continuity and Functional Equivalence

A systematic comparison between cognitive warfare and established doctrines reveals substantial continuity at the level of objectives, mechanisms, and intended effects. The central aim of Information Operations has long been to influence, disrupt, corrupt, or usurp adversarial decision-making processes while protecting one's own[6]. Similarly, Psychological Operations have historically targeted beliefs, perceptions, morale, and reasoning in order to shape behavior and strategic outcomes[7].

The contemporary framing of cognitive warfare largely reiterates these objectives, albeit in more technologically sophisticated terms. Activities such as exploiting cognitive biases, reinforcing particular narratives, undermining trust in institutions, and inducing epistemic uncertainty are not novel in their intent. Rather, they represent refined applications of long-standing practices of perception management and psychological influence. Empirical research on misinformation dynamics, including studies examining the effects of repetition, social validation, and cognitive bias on belief formation, further reinforces the argument that the mechanisms underpinning influence have remained fundamentally stable over time[8].

Consequently, the distinction between cognitive warfare and information operations appears to be primarily semantic and contextual rather than substantive. The introduction of new terminology does not correspond to the identification of a qualitatively distinct strategic function.

---

[4] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024* (Washington, DC: Department of Defense, 2024), https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF

[5] Institute for the Study of War, *Interactive Tour: Russia's Cognitive Warfare Infrastructure*, ArcGIS StoryMaps, https://storymaps.arcgis.com/stories/128853ee28fb40809148d548e0851b62

[6] NATO Cooperative Cyber Defence Centre of Excellence, *Ontological Foundations of Cognitive Warfare* (Tallinn: CCDCOE, 2026), https://ccdcoe.org/uploads/2026/04/ONTOLOGICAL_FOUNDATIONS_OF_COGNITIVE_WARFARE.pdf.

[7] National Defense University, "Cognitive Warfare and the Changing Character of Conflict," *Strategic Insights*, https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1055&context=strategic-insights.

[8] Sander van der Linden et al., "Psychological Inoculation Improves Resistance Against Misinformation," 2021, https://moodle2.units.it/pluginfile.php/745151/mod_resource/content/0/Roozenbeek%2C%20vander%20Linden%2C%20Goldberg%2C%20Rathje%2C%20Lewandowsky%202021.pdf.

Technological Transformation Without Doctrinal Disruption

Notwithstanding the strong case for continuity, it is essential to acknowledge the extent to which technological developments have transformed the operational environment. Three interrelated dimensions are particularly significant in this regard.

First, digital platforms and algorithmic systems have enabled unprecedented levels of amplification and reach. Social media infrastructures facilitate the rapid dissemination of content across vast networks, while engagement-driven algorithms prioritize emotionally salient and polarizing material, thereby enhancing the effectiveness of influence operations[9].

Second, influence activities have become persistent and embedded within everyday information consumption. Unlike traditional campaigns, which were often temporally bounded, contemporary operations are continuous and cumulative, shaping cognitive environments over extended periods[10].

Third, advances in data analytics and artificial intelligence have increased the precision with which audiences can be targeted. Behavioral profiling and predictive modeling allow actors to tailor messages to specific demographic and psychological characteristics, thereby improving the efficiency of influence efforts[11].

While these developments represent significant changes in capability, they do not alter the fundamental strategic objective of influencing cognition. Rather, they should be understood as intensifying existing practices within a transformed technological context.

Risks Associated with Terminological Proliferation

The adoption of cognitive warfare as a distinct conceptual category introduces several risks for policy and strategy. Foremost among these is the potential for conceptual fragmentation, whereby overlapping and ambiguously defined terms complicate doctrinal clarity and hinder effective coordination within and across institutions. In addition, the emergence of new terminology often entails the creation of new organizational structures and mandates, which may duplicate existing functions and generate inefficiencies. Without a clear delineation of added value, the institutionalization of cognitive warfare risks diverting resources from capability development toward conceptual differentiation.

[9] Cognitive Warfare Project, "How Social Media Algorithms Work," https://cognitivewars.org/how-social-media-algorithms-work/.

[10] Institute for the Study of War, *Interactive Tour: Russia's Cognitive Warfare Infrastructure*, ArcGIS StoryMaps, https://storymaps.arcgis.com/stories/128853ee28fb40809148d548e0851b62

[11] European Commission AI Alliance, *AI and Cognitive Warfare Infrastructure: Population-Level Cognitive Formatting*, https://futurium.ec.europa.eu/en/apply-ai-alliance/community-content/ai-cognitive-warfare-infrastructure-four-paper-research-series-population-level-cognitive-formatting.

A further concern relates to strategic ambiguity. The lack of precise definition and operational boundaries associated with cognitive warfare may impede its practical application, thereby reducing its utility as a guiding concept for policy formulation. Finally, the framing of the human mind as a domain of warfare raises normative and ethical questions, particularly in democratic contexts where the protection of individual autonomy and cognitive integrity is of central importance.

Implications for Allied Strategy and Doctrine

For NATO and its member states, the appropriate response to the challenges associated with cognitive warfare lies not in the creation of a new doctrinal category but in the adaptation and refinement of existing frameworks. Integrating insights from cognitive science, behavioral research, and artificial intelligence into information operations doctrine would allow for a more coherent and effective approach to contemporary influence threats.

In practical terms, this requires a shift toward enhancing societal resilience, including the development of educational and preventive measures designed to increase resistance to manipulation. Approaches such as prebunking, which aim to inoculate individuals against misleading narratives by exposing them to manipulation techniques in advance, offer promising avenues for strengthening cognitive resilience at scale.

At the same time, investment in technical capabilities, including detection, attribution, and response mechanisms, remains essential. Coordinated efforts across governmental, private sector, and civil society actors will be necessary to address the complex and interconnected nature of the contemporary information environment.

Maintaining conceptual clarity should be regarded as a strategic priority. A disciplined approach to terminology will facilitate interoperability, reduce ambiguity, and support the effective implementation of policy across Allied structures.

Conclusion

The concept of cognitive warfare reflects important developments in the technological and informational landscape of contemporary conflict; however, it does not constitute a fundamentally new domain of warfare. Its core characteristics align closely with the established logic of information operations, which have long sought to influence cognition as a means of achieving strategic objectives.

Interpreting cognitive warfare as a distinct doctrinal innovation risks generating unnecessary complexity and undermining strategic coherence. A more analytically robust approach is to view it as the technological intensification of existing practices, requiring adaptation rather than redefinition. For policymakers, the central task is therefore to modernize and integrate information operations doctrine in a manner that reflects current technological realities while preserving conceptual clarity and strategic focus.