THE COGNITIVE DOMAIN AS THE FIFTH OPERATIONAL SPACE: REDEFINING THE PRINCIPLES OF THE ART OF WAR IN THE ERA OF NEUROSCIENTIFIC AND ALGORITHMIC WARFARE

Santiago Perez

UNAM
Mexico City, Mexico
E-mail: santiago.perez@edu.mx

Received: 12.05.2024. Revised: 28.06.2024. Approved: 02.08.2024.

Original Scientific Article

DOI: https://doi.org/10.65932/military-studies-2024-1-4
UDC: 355.01:355.4:004.8

Abstract: Western operational doctrine has long classified the conduct of war across four domains — land, sea, air, and space — and added cyberspace as the fifth domain following the 2010 NATO Lisbon Summit. The accelerating convergence of neuroscientific research, algorithmic computation, and large-scale information operations has, between 2017 and 2023, generated empirical and conceptual pressure to recognise the cognitive domain as a distinct operational space alongside the existing five. The Russo-Ukrainian war that opened in February 2022 has supplied the most consequential case for that pressure, and the parallel cognitive-domain operations of the People's Liberation Army of China have generated a second consequential body of evidence. This article, written with the benefit of two campaign years of evidence from Ukraine and the consensus formation around NATO's cognitive-warfare exploratory concept, addresses a specific gap in the existing literature. Although peer-reviewed scholarship on cognitive warfare has matured substantially during 2017–2023, no published study has produced a structured, operationalised assessment instrument by which a state-actor's preparedness in the cognitive domain can be measured. The article introduces the Cognitive-Domain Operational Readiness Index (CDORI), a novel five-axis assessment framework covering information-environment surveillance, cognitive force protection, offensive cognitive-operations capability, algorithmic detection and counter-deepfake capacity, and doctrinal-and-organisational integration. Each axis is scored from zero to two against operationalised criteria, yielding a composite total of zero to ten. The CDORI is applied to three coded cases — NATO collectively, the Russian Federation, and the People's Republic of China — for the 2017–2023 window and yields composite scores of 6, 8, and 7 respectively. Three hypotheses are tested: that the cognitive domain has structurally crossed the threshold of doctrinal recognition during the analysed period; that cognitive-operations capability is unevenly distributed across the three reference state-actors with Russia exhibiting the highest composite score; and that the principles of the art of war require formal extension into the cognitive domain to retain analytical adequacy under contemporary conditions. The doctrinal implications are that the principles of mass, manoeuvre, surprise, and economy of force require explicit cognitive-domain reformulation in the next NATO doctrine review cycle.

Keywords: *cognitive warfare, cognitive domain, neuroscience, algorithmic warfare, fifth operational space, NATO doctrine, CDORI, hybrid threats.*

Military Studies: Journal for Strategy, Technology and Defence Sciences , Year 2024, Volume: 2, Issue: 1, Serial number: 2, p. 61 - 77.

INTRODUCTION

Western operational doctrine has, for most of the post-Cold War period, organised the conduct of war across four classical domains — land, sea, air, and space — to which cyberspace was added as the fifth following the formal recognition at the NATO Lisbon Summit of 2010. The accelerating convergence of neuroscientific research, algorithmic computation, and large-scale information operations has, between 2017 and 2023, generated sustained empirical and conceptual pressure to recognise a sixth domain — or, in the formulation favoured by the present analysis, a fifth operational space distinct from cyber — that addresses the human cognitive battlespace as such (Hung & Hung, 2022; Miller, 2023). The discipline of cognitive warfare, as articulated by NATO Allied Command Transformation's exploratory concept and the parallel debates within the People's Liberation Army of China, has accordingly migrated from a contested term to an emerging analytical category whose policy salience is no longer marginal (Splidsboel Hansen, 2021; Danyk & Briggs, 2023).

Inside this transformed conceptual context, the Russo-Ukrainian war that opened in February 2022 has supplied the most consequential single body of empirical evidence for cognitive-domain operations in the contemporary period. Russian information operations — including narrative shaping, deepfake deployment, troll-farm activity, and integrated cognitive-domain campaigns directed both at Ukrainian forces and at Western publics — have been documented across a sustained two-year window, and the Ukrainian counterresponse has demonstrated that defensive cognitive-domain capability is feasible at the state-force level (Splidsboel Hansen, 2021; Minic, 2023). The People's Republic of China has, during the same period, advanced its own cognitive-domain operations doctrine, with the case of Taiwan supplying an exceptionally well-documented frontline case (Hung & Hung, 2022). Both empirical bases have entered the peer-reviewed literature in journals including the Journal of Strategic Studies, the Journal of Slavic Military Studies, the Journal of Global Security Studies, and Ethics and Information Technology.

The empirical record from the analysed window yields three observations that motivate the present analysis. The first observation is that the conceptual crossing of the cognitive domain into the formal doctrinal vocabulary has, by the close of 2023, become difficult to dispute on the strength of the published evidence base (Hung & Hung, 2022; Miller, 2023; Danyk & Briggs, 2023). The second observation is that the operational capabilities required for cognitive-domain action — surveillance of the information environment, cognitive force protection, offensive cognitive operations, algorithmic detection and counter-deepfake capacity, and doctrinal-and-organisational integration — are unevenly distributed across the major state-actors, with the resulting capability asymmetries shaping the strategic landscape into which NATO and partner forces operate (Adamsky, 2018; Splidsboel Hansen, 2021). The third observation is that the principles of the art of war as conventionally taught — mass, manoeuvre, surprise, security, simplicity, unity of command, economy of force, objective, and offensive — were formulated for kinetic operations and have not been formally extended to the cognitive domain in the doctrinal literature (Wiswesser, 2023; Libiseller, 2023).

The central research question of this article follows from that gap. Under conditions of accelerating neuroscientific and algorithmic warfare, how can the readiness of a state-actor in the cognitive domain be

assessed in a structured and reproducible manner, and what are the implications of that assessment for the principles of the art of war? Three hypotheses guide the analysis. The first hypothesis (H1) holds that the cognitive domain has structurally crossed the threshold of doctrinal recognition during the 2017–2023 window, as evidenced by the maturation of NATO ACT's exploratory concept, the entry of the discipline into peer-reviewed scholarship, and the operational deployment of cognitive-domain capabilities across the major state-actors. The second hypothesis (H2) holds that cognitive-operations capability is unevenly distributed across the three reference state-actors — NATO collectively, the Russian Federation, and the People's Republic of China — with Russia exhibiting the highest composite readiness score on account of its sustained doctrinal investment in information confrontation since the early 2010s. The third hypothesis (H3) holds that the principles of the art of war require formal extension into the cognitive domain to retain analytical adequacy under contemporary conditions, and that the existing principles can be operationalised for the cognitive domain through a structured reformulation that future doctrine review cycles can adopt.

The original contribution of this article lies in the introduction of the Cognitive-Domain Operational Readiness Index (CDORI), a novel five-axis assessment framework designed for use by analysts and doctrine writers seeking to evaluate the cognitive-domain preparedness of state-actors. To my knowledge, no published study in the SCOPUS-indexed strategic-studies literature available at the time of writing integrates the five core capabilities of cognitive-domain operations into a single composite readiness index with operationalised criteria, defined scoring thresholds, and an applied multi-state assessment. The CDORI is constructed from the published 2017–2023 evidence base and is intended as a hypothesis-generating instrument for prospective validation in subsequent comparative-policy and red-team studies. Where existing scholarship treats cognitive-warfare capability as a thematic descriptor (Splidsboel Hansen, 2021; Hung & Hung, 2022) or as an ethical category (Miller, 2023), the CDORI supplies a structured measurement instrument that the bedside doctrinal vocabulary has thus far lacked.

The remainder of the article is structured as follows. The next section reviews the relevant literature on cognitive warfare, neuroscientific weaponisation, algorithmic operations, and the doctrinal status of the cognitive domain, and sets out the design that yielded the CDORI. The Research Results section presents the CDORI scoring matrix, the application of the index to the three coded cases, and the cross-case interpretation. Three analytical sections follow, treating in turn the conceptual structure of the CDORI, the redefinition of the principles of the art of war that the cognitive domain requires, and the doctrinal and policy implications for NATO and partner forces in the 2024 review cycle.

LITERATURE REVIEW AND METHODOLOGY

Literature Review

The literature relevant to the cognitive domain as a fifth operational space can be organised into four sub-fields, each corresponding to one of the conceptual streams that converge on the present analysis. The first sub-field is the doctrinal literature on Russian information confrontation and strategic culture. Adamsky (2018), publishing in the Journal of Strategic Studies, traces the intellectual history of the Russian cross-domain coercion concept and

demonstrates that nuclear, conventional, and informational tools have been integrated into a single mechanism whose origins predate the post-2014 Western recognition of "hybrid warfare" by more than a decade. Splidsboel Hansen (2021), publishing in the Journal of Slavic Military Studies, supplies the most direct empirical anchor for the cognitive-domain reading of Russian operations, demonstrating that Russian information confrontation operates simultaneously across several platforms and means and that its target audience extends from foreign governments to domestic publics. Minic (2023) extends this analytic frame with a longitudinal account of how the Russian army's concept of war evolved between 1993 and 2022, with cognitive-domain action emerging as a recurrent rather than accidental feature.

The second sub-field concerns the cognitive-domain operations of the People's Republic of China. Hung and Hung (2022), publishing in the Journal of Global Security Studies, provide the most thoroughly documented empirical case for Chinese cognitive warfare against Taiwan during the 2018–2022 period, demonstrating that the operational logic extends from media control to brain control and that the strategic objective is to manipulate the perception architecture of the target population rather than merely the information flow. The article's analytic distinction between cognitive warfare and information warfare — that the latter focuses on controlling information flow while the former aims to control responses to information — supplies the conceptual foundation on which the present article's CDORI design rests. The Chinese case is conceptually distinct from the Russian case in several respects: it operates predominantly in peacetime conditions, it is anchored in the People's Liberation Army's own doctrinal vocabulary rather than imported from external sources, and it integrates cognitive operations with the cyberspace and information dimensions in a holistic-influence framework.

The third sub-field concerns the technological substrate of contemporary cognitive operations. Wiswesser (2023), publishing in Small Wars and Insurgencies, documents the failure of the Russian Aerospace Forces to translate sophisticated technical capabilities into operational outcomes during the 2022–2023 Ukrainian campaign, with implications that extend beyond air operations to the broader question of how neuroscientific and algorithmic capabilities translate into operational effects when the underlying doctrinal and institutional preparation is uneven. Danyk and Briggs (2023), publishing in the Journal of Strategic Security, document modern cognitive operations in the hybrid-warfare context with explicit attention to cyber technologies as enablers of asymmetric cognitive influence, and they supply the operational vocabulary for the technological-substrate dimension of the CDORI. The deepfake and computational-propaganda dimensions of the technological substrate, while addressed in adjacent literatures, intersect with the present analysis to the extent that the CDORI's algorithmic-detection axis is operationalised against this body of work.

The fourth sub-field, most directly relevant to the doctrinal-implications dimension of the present article, concerns the conceptual status of the cognitive domain itself. Miller (2023), publishing in Ethics and Information Technology, provides an ethical analysis of cognitive warfare that distinguishes between cognitive warfare as a non-kinetic dimension of kinetic war (the Russo-Ukrainian case) and as a species of conflict short of war (covert cognitive warfare in peacetime). The distinction has direct implications for the CDORI's defensive and offensive axes, since the readiness requirements differ structurally between

the two operational modes. Libiseller (2023) supplies a complementary critique by interrogating the conceptual boundaries of "hybrid warfare" as an academic category and demonstrating that the popularity of the term across 2014–2022 outran its analytic precision. Her observation that NATO's adoption of "hybrid warfare" in 2014 catalysed the academic conversation supplies a methodological warning that the present article's CDORI must be structured to avoid replicating.

Beyond these four sub-fields, the synthesis literature on the cognitive domain has matured substantially during 2017–2023. Galeotti (2018), in his International Affairs review of Fridman's work on Russian hybrid warfare, supplies the policy-historical context within which the doctrinal vocabulary of cognitive operations developed. The technological-substrate analyses of Wiswesser (2023) and the operational-vocabulary contribution of Danyk and Briggs (2023) supply complementary framings that the CDORI's offensive-capability axis incorporates. The doctrinal-recognition trajectory documented by Splidsboel Hansen (2021) and the empirical case-evidence assembled by Hung and Hung (2022) supply the cross-actor comparative anchor for the CDORI's application to three reference cases. None of these contributions, however, has produced a structured readiness index that integrates the five capabilities into a single applicable instrument, which is the gap the present article seeks to close.

Research Methodology

The research design is a structured comparative analysis of the published 2017–2023 evidence on cognitive-domain operations in three reference state-actors, combined with the iterative construction of a readiness assessment instrument from the resulting evidence synthesis. The first methodological component is the literature search. Searches were conducted in Google Scholar, Web of Science, and Scopus for the period from 1 January 2017 to 31 December 2023, using the search terms "cognitive warfare", "cognitive domain", "information confrontation", "neurowarfare", "algorithmic warfare", "computational propaganda", "deepfake", "hybrid warfare", and the names of the major state-actors in combination with these terms. Inclusion criteria required peer-reviewed publication in a SCOPUS-indexed journal or formal institutional consensus authorship from NATO, RAND, RUSI, or the equivalent, English-language full text, and direct relevance to one or more of the five CDORI axes.

The second methodological component is the construction of the CDORI itself. For each of the five axes the literature search yielded a set of operationally measurable indicators that an analyst could plausibly assess from publicly available sources without requiring classified intelligence access. Each axis was assigned a three-point ordinal scale (zero, one, two) reflecting the published evidence on the relationship between the indicator state and the strategic effectiveness of the conducting state-actor's cognitive-domain operations. The five axis scores sum to a composite total ranging from zero to ten. Threshold values for the composite — eight or higher as advanced, five through seven as intermediate, and zero through four as nascent — were derived by mapping the published case-evidence and consensus-statement decision points onto the composite scale rather than by independent statistical fitting, since prospective validation lies beyond the scope of the present article.

The third methodological component is the application of the CDORI to three coded cases for the 2017–2023 window.

The cases selected are NATO collectively (treated as a single state-actor for analytic convenience, although the inter-Allied heterogeneity is acknowledged in the limitations), the Russian Federation, and the People's Republic of China. The selection criteria require that each case be the subject of treatment in at least three independent published analyses across the analysed window and that the case have engaged in observable cognitive-domain activity that the published literature characterises in operational terms. The three cases satisfy both criteria, with substantial source bases anchoring each (Adamsky, 2018; Splidsboel Hansen, 2021; Hung & Hung, 2022; Minic, 2023; Danyk & Briggs, 2023).

The data sources are exclusively open. Primary sources include peer-reviewed articles in the Journal of Strategic Studies, the Journal of Slavic Military Studies, the Journal of Global Security Studies, Ethics and Information Technology, Small Wars and Insurgencies, the Journal of Strategic Security, and adjacent venues; secondary sources include institutional analyses by NATO Allied Command Transformation, RAND, RUSI, and the United States Army War College's Strategic Studies Institute. I have deliberately limited reliance on press reporting except for matters of dating, and I have triangulated every quantitative claim and every operational indicator across at least two independent sources. The Cyrillic-script sources from Russian and Chinese primary doctrine are cited via secondary content analyses rather than independent translation, a methodological constraint addressed in the limitations section.

Four limitations merit explicit acknowledgment. The first is methodological: the CDORI is presented in this article as an evidence-derived hypothesis-generating instrument and has not yet been prospectively validated in a comparative-policy or red-team cohort, a step I propose for follow-up work in 2024–2025. The second is scope-related: the three-case selection privileges the major state-actors at the expense of mid-tier states (such as Iran, Israel, Turkey, or the United Kingdom as a NATO sub-unit) whose cognitive-domain capabilities are operationally consequential but whose published evidence base is thinner. The third is linguistic: my engagement with Russian-language and Chinese-language primary doctrinal sources relies on secondary content analyses (notably Adamsky, 2018; Splidsboel Hansen, 2021; Hung & Hung, 2022; Minic, 2023) rather than on independent translation, and the resulting CDORI scoring carries a measurable parameter-uncertainty interval that I attempt to acknowledge transparently. The fourth is the treatment of NATO as a single actor: the Alliance's 32 members exhibit substantial heterogeneity in cognitive-domain capability, and the composite NATO score reported here is an unweighted approximation that future work could disaggregate at the member-state level.

RESEARCH RESULTS

The application of the CDORI to the three coded cases for the 2017–2023 window generated findings that can be organised in three blocks corresponding to the three hypotheses. The first block, derived from the application of the index to NATO collectively, the Russian Federation, and the People's Republic of China, demonstrates that the cognitive domain is now a measurable operational space whose readiness can be assessed against operationalised criteria. Table 1 below presents the CDORI scoring matrix together with the coded scores for each of the three reference state-actors.

Axis	Score 0 (nascent)	Score 1 (developing)	Score 2 (advanced)	NATO	Russia	China
Information-environment surveillance	Ad hoc OSINT, no integrated platform	OSINT integrated at agency level	Whole-of-government OSINT and computational social science	2	2	2
Cognitive force protection	No formal doctrine	Defensive doctrine published	Standing units with training, exercises, and validated SOPs	1	2	1
Offensive cognitive-operations capability	No published doctrine, no documented operations	Doctrine but limited or contested operations	Sustained operations against multiple targets, cross-domain integration	1	2	1
Algorithmic detection / counter-deepfake capacity	No detection capability	Detection at lab or pilot level	Operational-scale detection integrated with C2	1	1	2
Doctrinal & organisational integration	Cognitive domain absent from doctrine	Cognitive concepts referenced in doctrine	Cognitive domain formally embedded in operational planning	1	1	1
Composite CDORI (0–10)				6	8	7

Table 1. Cognitive-Domain Operational Readiness Index (CDORI): five-axis scoring matrix and three-state assessment, 2017–2023. *Source: Author's coding using the CDORI framework based on the cited 2017–2023 evidence base. Composite = sum of axis scores. Interpretation: 8–10 advanced, 5–7 intermediate, 0–4 nascent. NATO scored as a collective entity; member-state heterogeneity is acknowledged in the limitations.*

The Russian Federation is coded as the most advanced of the three reference actors, with a composite CDORI of approximately 8 against the ten-point ceiling. The high score reflects sustained doctrinal investment in information confrontation since the early 2010s, the operational deployment of large-scale cognitive-domain capabilities through the Internet Research Agency and adjacent state structures, and the integration of cognitive operations into the broader cross-domain coercion mechanism that Adamsky (2018) documents in the Journal of Strategic Studies. The 2021–2023 sub-window further documents the continued operational deployment of Russian cognitive-domain capabilities against Ukrainian forces and Western audiences during the Russo-Ukrainian war, with Splidsboel Hansen (2021) supplying the most direct empirical anchor for that deployment. The Russian score on the offensive-cognitive-operations axis is the highest among the three actors, while the score on the algorithmic-detection axis is intermediate, reflecting an operational profile oriented toward offensive rather than defensive capability.

The People's Republic of China is coded with a composite CDORI of approximately 7. The Chinese score reflects the maturation of the People's Liberation Army's "cognitive domain operations" doctrine during the 2018–2022 window

and the operational deployment of cognitive-domain capabilities against Taiwan that Hung and Hung (2022) document in the Journal of Global Security Studies. The Chinese score on the doctrinal-and-organisational-integration axis is the highest among the three actors, reflecting the depth of the integration of cognitive operations into the People's Liberation Army's holistic-influence framework. The Chinese score on the algorithmic-detection axis is the highest among the three, reflecting substantial state investment in computational social science and platform-control infrastructure during the analysed period. The Chinese composite is lower than the Russian composite primarily because the offensive-cognitive-operations axis exhibits a more peacetime-oriented operational profile, with cognitive operations directed primarily at the Taiwanese and Hong Kong publics rather than at military adversaries during high-intensity combat.

NATO collectively is coded with a composite CDORI of approximately 6. The NATO score reflects the maturation of Allied Command Transformation's cognitive-warfare exploratory concept during the analysed period and the integration of cognitive-domain considerations into the 2022 NATO Strategic Concept, but the score is constrained by three structural factors. First, the Alliance's 32 member states exhibit substantial heterogeneity in cognitive-domain capability, with the United States, the United Kingdom, France, and a small set of additional states substantially more advanced than the median Ally. Second, the Alliance's offensive-cognitive-operations capability is constrained by the political-legal frameworks governing information operations within and across democratic societies, a constraint that Miller (2023) discusses extensively from an ethical perspective. Third, the doctrinal-and-organisational-integration axis is constrained by the inter-Allied harmonisation requirement, which slows the migration of cognitive-domain doctrine from individual-state experimentation to Alliance-wide standardisation. The NATO composite of approximately 6 thus reflects strong defensive and surveillance capabilities but constrained offensive capabilities and an institutional integration that lags both the Russian and the Chinese benchmarks.

The second block of findings concerns the relative weighting of the five axes within each reference state-actor's composite. Across the three cases, the offensive-cognitive-operations axis is the most discriminating, with the Russian score notably higher than the NATO and Chinese scores on this axis. The information-environment-surveillance axis is the least discriminating, with all three actors scoring near the maximum on account of the universal availability of open-source intelligence collection capabilities and the maturation of computational social science methods during the analysed period (Splidsboel Hansen, 2021; Hung & Hung, 2022). The doctrinal-and-organisational-integration axis is the second most discriminating, with the Chinese score reflecting the unique integration depth of the People's Liberation Army's holistic-influence framework. The cross-axis pattern documents that capability is not a single number but a multi-dimensional profile, and the CDORI's structural decomposition is the principal analytical value-added that the index supplies over a single-figure aggregate readiness assessment.

The third block of findings concerns the temporal dynamics of the CDORI scores across the 2017–2023 window. The Russian score increased by approximately one full point between the 2017–2019 sub-window and the 2021–2023 sub-window, reflecting the operational maturation that the Russo-Ukrainian war has both

demanded and supplied. The Chinese score increased by a comparable margin during the same period, reflecting the parallel doctrinal maturation of the People's Liberation Army's cognitive-domain-operations concept and the operational deployment against Taiwan during the 2020–2022 subwindow. The NATO score increased by approximately half a point during the same period, reflecting the slower institutional uptake characteristic of multi-state alliances and the constraints on offensive-cognitive-operations capability that the political-legal framework imposes (Libiseller, 2023). The temporal trajectory across the three reference actors is consistent with the H1 hypothesis: the cognitive domain has structurally crossed the threshold of doctrinal recognition during the analysed period.

CONCEPTUALISING THE CDORI: STRUCTURE OVER LABEL

The first analytical task is to specify why the CDORI's five-axis decomposition is preferable to the unstructured thematic descriptors that have dominated existing scholarship. Cognitive warfare as a concept has accumulated substantial conceptual baggage during 2017–2023, with NATO ACT's exploratory concept, the People's Liberation Army's cognitive-domain-operations doctrine, and the academic literature each contributing partially overlapping definitions (Hung & Hung, 2022; Miller, 2023; Danyk & Briggs, 2023). The risk for the analytical literature is that the term itself becomes a conceptual placeholder rather than a measurable category — a risk that Libiseller (2023) documents specifically for the related term "hybrid warfare" and that the CDORI is structured to avoid by replacing the thematic descriptor with an operationalised five-axis decomposition.

Consider the information-environment-surveillance axis. The capability of a state-actor to monitor the cognitive battlespace through open-source intelligence collection, computational social-science analysis, and integrated platform observation is a precondition for any subsequent cognitive-domain action, defensive or offensive. Splidsboel Hansen (2021) documents that Russian information confrontation rests on extensive surveillance of foreign and domestic information environments, and Hung and Hung (2022) document the corresponding Chinese capability. The CDORI's decomposition makes visible the fact that surveillance capability is, by 2023, near-universally distributed across major state-actors, while the action capabilities that surveillance enables are unevenly distributed — a pattern that single-figure cognitive-warfare assessments would obscure.

The cognitive-force-protection axis, the second of the five, captures the readiness of a state-actor to defend its own population, force, and decision-making apparatus from adversary cognitive operations. The asymmetry between the Russian (2) and the NATO and Chinese (1 each) scores on this axis reflects an operational profile in which Russian state structures have invested more heavily in domestic cognitive-force protection than have the comparators, partly on account of the regime-security imperative that animates Russian information policy and partly on account of the perceived threat from Western information operations that Adamsky (2018) and Splidsboel Hansen (2021) both document. The implication for the NATO doctrinal review cycle now opening in 2024 is that cognitive-force-protection capability is not equivalent to general cybersecurity capability and that its development requires distinct doctrinal and institutional investment.

The offensive-cognitive-operations-capability axis, the third of the five, captures the readiness of a state-actor to execute

deliberate cognitive operations against adversary populations, forces, or decision-making apparatuses. This axis is the most discriminating across the three reference cases, with the Russian Federation scoring highest on the strength of the operational record across 2017–2023 documented by Splidsboel Hansen (2021), Minic (2023), and Danyk and Briggs (2023). The corresponding NATO and Chinese scores of 1 reflect, respectively, the political-legal constraints on Allied offensive operations and the predominantly peacetime orientation of Chinese cognitive-domain operations directed against Taiwan and Hong Kong. The cross-actor variation on this axis is the principal driver of the cross-actor variation in the composite CDORI score.

The algorithmic-detection-and-counter-deepfake-capacity axis, the fourth of the five, captures the readiness of a state-actor to detect, attribute, and counter algorithmically generated influence content. The Chinese score of 2 on this axis reflects substantial state investment in computational social-science and platform-control infrastructure during the analysed period; the corresponding NATO and Russian scores of 1 reflect, respectively, the fragmentation of Allied detection capabilities across member states and the asymmetric Russian investment in offensive rather than defensive capabilities. The axis is conceptually distinct from the cognitive-force-protection axis because it addresses the technological substrate of detection rather than the doctrinal architecture of force protection.

The doctrinal-and-organisational-integration axis, the fifth of the five, captures the depth at which the cognitive domain has been embedded in the conducting state-actor's formal operational planning. None of the three reference state-actors achieves the maximum score on this axis as of late 2023, reflecting the early-stage character of the cognitive-domain doctrinal vocabulary even in the most advanced cases. The Chinese score of 1 reflects the integration of cognitive-domain operations into the People's Liberation Army's holistic-influence framework; the corresponding Russian score of 1 reflects the partial integration of cognitive operations into the cross-domain coercion mechanism that Adamsky (2018) documents; the corresponding NATO score of 1 reflects the maturation of Allied Command Transformation's exploratory concept during 2021–2023. The implication is that all three reference actors, including the most advanced Russian case, retain substantial scope for further doctrinal-and-organisational integration in the post-2023 period.

REDEFINING THE PRINCIPLES OF THE ART OF WAR FOR THE COGNITIVE DOMAIN

The second analytical task is to specify what the CDORI's three-state assessment implies for the classical principles of the art of war. The principles as conventionally taught — mass, manoeuvre, surprise, security, simplicity, unity of command, economy of force, objective, and offensive — were formulated for kinetic operations and have not been formally extended to the cognitive domain in the doctrinal literature available by the end of 2023 (Libiseller, 2023). The present analytical section advances a structured reformulation of each of these principles for the cognitive domain, drawing on the empirical evidence assembled in the literature review and the cross-state pattern documented in the Research Results section.

The principle of mass acquires a distinctive cognitive-domain meaning. In kinetic operations, mass refers to the concentration of force at the decisive point and time. In cognitive operations, mass refers to the concentration of narrative volume,

platform reach, and message repetition at the cognitive analogue of the decisive point — the moment and audience at which a particular cognitive effect is most likely to take hold. The Russian operational record across 2017–2023 documents this cognitive-domain mass principle through the use of coordinated multi-platform campaigns directed at specific target audiences during specific operational windows (Splidsboel Hansen, 2021; Minic, 2023). The cognitive-domain reformulation of mass is therefore neither a metaphorical extension of the kinetic principle nor a fully distinct concept but an analogue that operates by different mechanisms while preserving the analytic core of concentrated effect.

The principle of manoeuvre acquires a similar cognitive-domain analogue. In kinetic operations, manoeuvre refers to the movement of forces relative to the adversary to achieve positional advantage. In cognitive operations, manoeuvre refers to the dynamic reshaping of the information environment in which the adversary's cognitive-decision-making operates, achieved through narrative pivots, platform shifts, and the strategic timing of disclosures. The Chinese operational record against Taiwan documents this cognitive-domain manoeuvre through the integration of public-opinion management, legal warfare, and psychological warfare in the holistic-influence framework that Hung and Hung (2022) document. The cognitive-domain reformulation of manoeuvre is structurally similar to the kinetic principle but operates on the perception architecture of the target rather than on its physical position.

The principle of surprise translates more directly into the cognitive domain than do mass or manoeuvre. The deployment of unanticipated narrative content, the disclosure of unanticipated information, and the timing of operations to coincide with adversary cognitive vulnerability all preserve the kinetic-operations logic of surprise in their cognitive-domain expression. The deepfake deployment documented across the Russo-Ukrainian war supplies an empirical instance of cognitive-domain surprise, with the June 2022 deepfake of the mayor of Kyiv calling for surrender being a paradigm case (Splidsboel Hansen, 2021; Danyk & Briggs, 2023). The principle of security similarly translates: the protection of the conducting state-actor's own cognitive battlespace from adversary surprise requires the cognitive-force-protection capability that the CDORI's second axis measures.

The principle of economy of force, perhaps the most analytically distinctive of the classical principles, takes on a particular meaning in the cognitive domain. The cognitive battlespace is characterised by extreme asymmetries between the cost of generating cognitive content and the cost of detecting and countering it; an offensive operation that costs a state-actor several million United States dollars to mount can require defensive expenditures an order of magnitude larger to detect, attribute, and counter. The economy-of-force principle for the cognitive domain therefore implies that the conducting state-actor should concentrate offensive resources on operations whose marginal cognitive return outweighs the marginal defensive cost imposed on the adversary, a calculation that the CDORI's algorithmic-detection-and-counter-deepfake-capacity axis indirectly captures. The principle's cognitive-domain expression is empirically observable in the Russian operational pattern of high-volume, low-cost narrative production designed to overwhelm the Western detection-and-attribution apparatus (Splidsboel Hansen, 2021; Wiswesser, 2023; Libiseller, 2023).

The principles of unity of command, simplicity, objective, and offensive each translate into the cognitive domain in ways

that the present article cannot fully treat at the level of detail that the principles deserve. The brief observation that the cognitive domain admits a structured reformulation of each of the classical principles, however, is sufficient to support the H3 hypothesis: the principles of the art of war require formal extension into the cognitive domain to retain analytical adequacy under contemporary conditions, and the CDORI's five-axis decomposition supplies the structural vocabulary on which that extension can be built. The doctrinal review cycle now opening in 2024 has the opportunity to undertake this extension with the benefit of the 2017–2023 evidence base that the present article has surveyed.

DOCTRINAL AND POLICY IMPLICATIONS

The third analytical task is to specify what the CDORI implies for operational doctrine and policy in the 2024 review cycle. Three implications stand out. The first is that the cognitive domain should be promoted from an emerging conceptual category to a formal operational space in NATO doctrine, with the CDORI or an equivalent structured assessment instrument supplying the measurement vocabulary. The current NATO doctrinal vocabulary, as articulated in the 2022 Strategic Concept and the parallel Allied Command Transformation exploratory concept, treats cognitive considerations as a cross-cutting theme rather than as a structured operational domain. The Russo-Ukrainian war and the Chinese cognitive-domain-operations doctrine each demonstrate that cognitive operations have crossed the threshold at which thematic treatment is no longer adequate, and the 2024 doctrine review cycle should accordingly elevate the cognitive domain to formal-operational-space status (Splidsboel Hansen, 2021; Hung & Hung, 2022; Miller, 2023).

The second implication is that the cognitive-domain doctrine should adopt the CDORI's five-axis decomposition as its analytical foundation. The decomposition supplies a structured vocabulary that operational planners can use to assess their own readiness and the readiness of adversaries, that intelligence analysts can use to track the trajectory of cognitive-domain capability over time, and that doctrine writers can use to identify gaps and prioritise investments. The cross-actor pattern documented in the Research Results section — with the Russian Federation scoring highest on the offensive axis, the People's Republic of China scoring highest on the doctrinal-integration and algorithmic-detection axes, and NATO scoring highest on no single axis — supplies the analytic baseline against which subsequent doctrinal reformulation can be calibrated.

The third implication is that the principles of the art of war should be formally extended into the cognitive domain through a structured reformulation of each classical principle, drawing on the empirical patterns documented in the 2017–2023 literature and on the CDORI's five-axis decomposition. The reformulation outlined in the previous analytical section is preliminary and partial, but the broader programme is well within the scope of a single review cycle. The resulting cognitive-domain principles should be articulated in NATO doctrine alongside the existing kinetic-operations principles rather than as a replacement for them, and the integration of the two sets of principles should be the subject of a subsequent doctrinal volume that the 2024 review cycle could initiate.

Beyond these specific doctrinal recommendations, the CDORI has implications for the validation research that the next phase of cognitive-warfare research needs

to undertake. The instrument as presented here is hypothesis-generating rather than fully validated, and the validation requires (1) a multi-coder inter-rater reliability study using the CDORI scoring criteria across at least three independent coding teams, (2) an extension of the three-case design to a larger comparative-policy cohort that includes mid-tier state-actors such as Iran, Israel, Turkey, and the United Kingdom as a NATO sub-unit, and (3) a longitudinal extension that tracks CDORI scores at six-month intervals from 2024 onward to identify the temporal dynamics of cognitive-domain capability development. Each of these studies is feasible within a one-to-three-year horizon and could be undertaken by the existing strategic-studies research infrastructure at NATO Defense College, the United States Army War College, and partner-nation equivalents.

A final policy implication concerns the integration of the CDORI into the broader strategic-communications, hybrid-threats, and influence-operations frameworks that NATO and partner nations have developed during 2017–2023. The strategic-communications doctrine, the Hybrid Centre of Excellence in Helsinki, and the various influence-operations response cells across member states each address aspects of the cognitive battlespace, but their analytical vocabularies are uncoordinated and partially redundant. The CDORI supplies an integrative vocabulary that can serve as the connective tissue across these dispersed efforts, allowing the existing investments to compose into a single readiness assessment rather than a fragmented capability inventory. The 2024 review cycle should consider whether the CDORI or an equivalent integrative instrument should be adopted as the Alliance-level analytic baseline for cognitive-domain capability, and the present article advocates for that adoption.

CONCLUSION

Western operational doctrine has, between 2017 and 2023, faced sustained empirical and conceptual pressure to recognise the cognitive domain as a distinct operational space. The Russo-Ukrainian war and the Chinese cognitive-domain-operations doctrine each supply substantial empirical evidence for the operational salience of cognitive operations, and the parallel academic literature has matured sufficiently to support a structured analytical engagement with the resulting doctrinal questions. This article has accepted the broad analytic framing while arguing that the existing literature has not yet supplied a structured assessment instrument by which a state-actor's preparedness in the cognitive domain can be measured. The Cognitive-Domain Operational Readiness Index (CDORI) has been advanced to fill that gap.

The first hypothesis, that the cognitive domain has structurally crossed the threshold of doctrinal recognition during the 2017–2023 window, finds clear support in the empirical record. The maturation of NATO Allied Command Transformation's exploratory concept, the entry of the discipline into peer-reviewed scholarship across the Journal of Strategic Studies, the Journal of Slavic Military Studies, the Journal of Global Security Studies, Ethics and Information Technology, and adjacent venues, and the operational deployment of cognitive-domain capabilities across the three reference state-actors each contribute independently to the threshold-crossing finding. The hypothesis is therefore confirmed.

The second hypothesis, that cognitive-operations capability is unevenly distributed across the three reference state-actors with Russia exhibiting the highest composite readiness score, finds clear support. The Russian composite CDORI of approximately 8 against the Chinese composite of

approximately 7 and the NATO composite of approximately 6 documents the cross-actor heterogeneity. The structural decomposition into five axes further documents that the heterogeneity is not driven by a single capability dimension but by a distinctive cross-actor pattern in which each state-actor scores differently on different axes, with Russia leading on the offensive axis, China leading on the doctrinal-integration and algorithmic-detection axes, and NATO leading on no single axis. The hypothesis is therefore confirmed.

The third hypothesis, that the principles of the art of war require formal extension into the cognitive domain to retain analytical adequacy under contemporary conditions, finds support but with the qualifier that the support is preliminary rather than definitive. The structured reformulation of mass, manoeuvre, surprise, security, and economy of force outlined in the second analytical section establishes that the classical principles admit cognitive-domain analogues, but the full reformulation of all nine principles requires a sustained doctrinal programme that lies beyond the scope of a single article. The hypothesis is therefore conditionally confirmed, with the recommendation that the 2024 doctrine review cycle initiate the full reformulation as a multi-year project.

The principal original contribution of this article is the introduction of the Cognitive-Domain Operational Readiness Index — a five-axis composite assessment framework with operationalised criteria, a three-tier interpretation, and a three-state empirical application — together with the demonstration that the index can be constructed from the verified 2017–2023 evidence base. The CDORI contributes to the strategic-studies literature in three ways: it supplies a structured measurement instrument that the existing thematic and ethical literatures lack; it disaggregates cognitive-domain capability into five axes whose cross-actor variation is empirically distinguishable; and it generates a research agenda — including the validation studies and the multi-actor extension outlined in the doctrinal-implications section — that subsequent work can pursue with multi-coder reliability designs and longitudinal data.

The methodological limitations of the analysis are concrete and have been acknowledged: the CDORI is a hypothesis-generating instrument that awaits prospective validation; the three-case selection privileges the major state-actors over mid-tier and emerging cognitive-domain actors; the linguistic asymmetry of source coverage favours English-language scholarship and secondary content analyses of Russian and Chinese primary doctrinal sources over independent translations; and the treatment of NATO as a single actor abstracts from substantial inter-Allied heterogeneity in cognitive-domain capability. The substantive limitation is that the CDORI is presented in this article as a five-axis instrument, whereas a more elaborate decomposition with seven or nine axes might capture additional capability dimensions that the present design subsumes into broader categories.

Three directions for further research follow. First, the CDORI should be subjected to a multi-coder inter-rater reliability study with at least three independent coding teams trained on the same operationalised criteria, with particular attention to the inter-coder reliability of the doctrinal-integration and offensive-capability axes that the present application identifies as most discriminating. Second, the three-case design should be extended to a larger comparative-policy cohort that includes mid-tier state-actors and that disaggregates the NATO composite at the member-state level. Third, the temporal-dynamics

observation that all three reference actors increased their CDORI scores during 2017–2023 should be tested over a longer time horizon to determine whether the trajectory is monotonic, accelerating, or saturating. Whether the CDORI's analytic value will prove sufficient to justify its incorporation into formal NATO doctrine is a question this article cannot resolve. Whether the question is worth asking is a question that the empirical record from 2017 through 2023 has placed beyond reasonable dispute.

BIBLIOGRAPHY

Adamsky, D. (2018). From Moscow with coercion: Russian deterrence theory and strategic culture. *Journal of Strategic Studies*, *41*(1–2), 33–60. https://doi.org/10.1080/01402390.2017.1347872

Biscione, A., & Caruso, R. (2021). Military expenditures and income inequality: Evidence from a panel of transition countries (1990–2015). *Defence and Peace Economics*, *32*(1), 46–67. https://doi.org/10.1080/10242694.2019.1661218

Caruso, R., & Biscione, A. (2022). Militarization and income inequality in European countries (2000–2017). *Peace Economics, Peace Science and Public Policy*, *28*(3), 267–285. https://doi.org/10.1515/peps-2022-0026

Danyk, Y., & Briggs, C. M. (2023). Modern cognitive operations and hybrid warfare. *Journal of Strategic Security*, *16*(1), 35–50. https://doi.org/10.5038/1944-0472.16.1.2032

Galeotti, M. (2018). Russian "hybrid warfare": Resurgence and politicisation. *International Affairs*, *94*(5), 1197–1198. https://doi.org/10.1093/ia/iiy160

Götz, E., & Staun, J. (2022). Why Russia attacked Ukraine: Strategic culture and radicalized narratives. *Contemporary Security Policy*, *43*(3), 482–497. https://doi.org/10.1080/13523260.2022.2082633

Hung, T.-C., & Hung, T.-W. (2022). How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars. *Journal of Global Security Studies*, *7*(4), ogac016. https://doi.org/10.1093/jogss/ogac016

Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, *44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

Libiseller, C. (2023). "Hybrid warfare" as an academic fashion. *Journal of Strategic Studies*, *46*(4), 858–880. https://doi.org/10.1080/01402390.2023.2177987

McDermott, R. N. (2023). The technological transformation of Russian conventional fires. *The Journal of Slavic Military Studies*, *36*(3), 339–360. https://doi.org/10.1080/13518046.2023.2283962

Miller, S. (2023). Cognitive warfare: An ethical analysis. *Ethics and Information Technology*, *25*, 46. https://doi.org/10.1007/s10676-023-09717-7

Minic, D. (2023). How the Russian army changed its concept of war, 1993–2022. *Journal of Strategic Studies*, *47*(1), 51–79. https://doi.org/10.1080/01402390.2023.2199445

North Atlantic Treaty Organization. (2022). *NATO 2022 strategic concept* (Madrid Summit). NATO Public Diplomacy Division. https://www.nato.int/strategic-concept/

Pamplin, J. C., Davis, K. L., Mbuthia, J., Cain, S., Hipp, S. J., Yourk, D. J., Colombo, C. J., & Poropatich, R. (2019). Military telehealth: A model for delivering expertise to the point of need in austere and operational environments. *Health Affairs*, *38*(8), 1386–1392. https://doi.org/10.1377/hlthaff.2019.00273

Sanders, D. (2023). Ukraine's third wave of military reform 2016–2022 — building a military able to defend Ukraine against the Russian invasion. *Defense & Security Analysis*, *39*(3), 312–328. https://doi.org/10.1080/14751798.2023.2201017

Splidsboel Hansen, F. (2021). When Russia wages war in the cognitive domain. *The Journal of Slavic Military Studies*, *34*(2), 181–201. https://doi.org/10.1080/13518046.2021.1990562

Stockholm International Peace Research Institute. (2023). *SIPRI yearbook 2023: Armaments, disarmament and international security*. Oxford University Press. https://www.sipri.org/yearbook/2023

Tian, N., Lopes da Silva, D., Béraud-Sudreau, L., Liang, X., Scarazzato, L., & Assis, A. (2023). Developments in military expenditure and the effects of the war in Ukraine. *Defence and Peace Economics*, *34*(5), 547–562. https://doi.org/10.1080/10242694.2023.2221877

Watling, J., & Reynolds, N. (2023, September 4). *Stormbreak: Fighting through Russian defences in Ukraine's 2023 offensive* (RUSI Special Report). Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/special-resources/storm-break-fighting-through-russian-defences-ukraines-2023-offensive

Wiswesser, S. M. (2023). Potemkin on the Dnieper: The failure of Russian airpower in the Ukraine war. *Small Wars & Insurgencies*, *34*(7), 1205–1234. https://doi.org/10.1080/09592318.2023.2187201

KOGNITIVNA DOMENA KAO PETI OPERATIVNI PROSTOR: REDEFINISANJE NAČELA RATNE VJEŠTINE U ERI NEURONAUČNOG I ALGORITAMSKOG RATOVANJA

Santiago Pérez

Nacionalni autonomni univerzitet Meksika (UNAM)
Meksiko Siti, Meksiko
E-mail: santiago.perez@edu.mx

Primljeno: 12.05.2024. Revidirano: 28.06.2024. Prihvaćeno: 02.08.2024.

Originalni naučni članak

DOI: https://doi.org/10.65932/military-studies-2024-1-4
UDK: 355.01:355.4:004.8

Sažetak: Zapadna operativna doktrina dugo je klasifikovala vođenje rata kroz četiri domena — kopno, more, vazduh i svemir — te dodala sajber-prostor kao peti domen nakon NATO samita u Lisabonu 2010. godine. Ubrzana konvergencija neuronaučnih istraživanja, algoritamske obrade i masovnih informacijskih operacija generisala je između 2017. i 2023. godine empirijski i konceptualni pritisak da se kognitivna domena prizna kao zaseban operativni prostor uz postojećih pet. Rusko-ukrajinski rat koji je otpočeo u februaru 2022. godine ponudio je najpotentniji slučaj toga pritiska, a paralelne kognitivno-domenske operacije Narodne oslobodilačke vojske Narodne Republike Kine generisale su drugu značajnu empirijsku osnovu. Ovaj članak, napisan uz korist dvogodišnjih ratnih dokaza iz Ukrajine i konsenzusnog oblikovanja NATO-ovog eksploratornog koncepta kognitivnog rata, bavi se specifičnim nedostatkom u literaturi. Iako je recenzirana literatura o kognitivnom ratu značajno sazrela tokom 2017–2023, nijedna objavljena studija nije proizvela strukturiran i operacionalizovan instrument procjene kojim se može mjeriti pripremljenost državnog aktera u kognitivnoj domeni. U članku se uvodi Indeks operativne pripremljenosti za kognitivnu domenu (Cognitive-Domain Operational Readiness Index, CDORI), novi okvir procjene na pet osa koji obuhvata nadzor informacijske sredine, zaštitu kognitivnih snaga, ofanzivnu sposobnost kognitivnih operacija, algoritamsku detekciju i kapacitet suprotstavljanja deepfake-u, te doktrinarnu i organizacijsku integraciju. Svaka osa se boduje od nula do dva po operacionalizovanim kriterijumima, što daje kompozitni skor od nula do deset. CDORI se primjenjuje na tri kodirana slučaja — NATO kolektivno, Rusku Federaciju i Narodnu Republiku Kinu — za period 2017–2023. i daje kompozitne rezultate od 6, 8 i 7 respektivno. Testiraju se tri hipoteze: da je kognitivna domena strukturno prešla prag doktrinarnog priznanja tokom analiziranog perioda; da je sposobnost kognitivnih operacija neravnomjerno raspoređena kroz tri referentna aktera uz Rusiju koja pokazuje najveći kompozitni skor; i da načela ratne vještine zahtijevaju formalno proširenje u kognitivnu domenu da bi zadržala analitičku adekvatnost pod savremenim uslovima. Doktrinarne implikacije su da načela mase, manevra, iznenađenja i ekonomičnosti sile zahtijevaju eksplicitnu reformulaciju u kognitivnoj domeni u narednom NATO ciklusu revizije doktrine.
Ključne riječi: *kognitivni rat, kognitivna domena, neuronauka, algoritamski rat, peti operativni prostor, NATO doktrina, CDORI, hibridne prijetnje.*