COGNITIVE WARFARE
– A NEW OPERATIONAL DOMAIN –

Colonel Dr. Marian HOGEA
"Nicolae Bălcescu" Land Forces Academy, Sibiu
DOI: 10.55535/RMT.2025.3.10

Cognitive warfare is one of the most recent and complex forms of conflict in the global environment, in which the human mind becomes both a target and a strategic tool. The cognitive dimension, considered an emerging operational domain distinct from traditional ones – land, sea, air, space, and cyberspace, focuses on influencing the perceptions, emotions, and decision-making processes of individuals and communities, constituting an essential strategic vector in the dynamics of contemporary international relations. A comparative analysis of the strategies used by NATO, Russia, and China illustrates that cognitive warfare has become a central tool in the dispute between the great powers, with direct effects on the stability of the world order.

Keywords: cognitive warfare; global security; strategic influence; strategic manipulation; psychological influence;

INTRODUCTION

In the current context of globalization, marked by technological progress and information globalization, *cognitive warfare* stands out as a new battlefield. Unlike traditional domains – land, sea, air, space, and cyberspace –, it seeks to influence the perceptions, emotions, and decision-making processes of individuals and communities, thus representing a particularly relevant strategic tool in confrontations between major powers.

The cognitive dimension of global confrontations highlights the differences between information and psychological warfare, as well as its implications for global security and social cohesion. Campaigns to influence democratic processes illustrate the concrete effects of cognitive warfare, while ethical and legal analysis underscores the need to develop resilience policies and appropriate international regulatory frameworks

The term *"cognitive"* comes from the Latin *cognoscere ("to know"*, *"to understand"*), derived from the root *gnoscere ("to learn"*, *"to know"*). In its modern sense, it was established with the development of cognitive psychology and neuroscience, becoming a central concept for describing mental actions.

In psychology, the term gained visibility in the second half of the 20th century as a reaction to the limitations of *behaviourism* (a psychological current focused on the study of behaviour, of the external stimulus-response relationship), which facilitated the analysis of observable behaviour, excluding internal processes. In the period 1950–1960, the cognitive revolution (https://brainly.ro/tema/6593720,b2025) emerged, proposing an approach to the mind as an information processing system, analogous to the functioning of computers. (Miller, 1956, pp. 81-97). Ulric Neisser established the terminology in his work *Cognitive Psychology*, where he defined cognitive psychology as the study of the processes by which information is acquired, stored, and used (Neisser, 1967, pp. 3-20).

Thus, the term *"cognitive"* now refers both to the fundamental processes of cognition – perception, reasoning, attention, memory, decision-making – and to the conceptual framework that integrates the interaction between mind, brain, and environment. This evolution explains the expansion of the term beyond psychology and neuroscience to fields such as social sciences, communication theory, and security studies, where *"cognitive"* is analysed in relation to the influence, manipulation, and control of information in geopolitical and strategic contexts.

In his analysis entitled *"Cognitive Warfare: A Conceptual Analysis of NATO's Cognitive Warfare Concept"*, Christoph Deppe defines cognitive warfare as an emerging form of conflict focused on influencing and manipulating the perception and decision-making processes of individuals or groups of individuals in order to gain a strategic advantage. (Deppe, Schall, 2024). Cognitive warfare systematically exploits scientific knowledge about the cognitive functioning of the human mind to influence and manipulate the perceptions, decision-making processes, and behaviours of individuals and communities. It redefines the human mind as an operational domain, using psychological operations, disinformation, propaganda, social engineering, and digital technologies to achieve strategic and tactical objectives without resorting to conventional force. This emerging form of conflict seeks to gradually erode the collective will and resilience of adversaries. Thus, cognitive warfare directly targets the mental and cognitive processes of actors, influencing how they perceive, interpret, and process information, as well as their decision-making processes.

In modern conflicts, the terms cognitive warfare, information warfare, psychological warfare, ideological warfare, economic warfare, technological warfare, religious warfare, diplomatic warfare, and cyber operations are often used interchangeably, but each represents a distinct dimension of the struggle for influence and control.

In the post-Cold War context, the evolution of armed conflicts has highlighted a diversification of tactics and procedures, accompanied by a doctrinal reconfiguration that has shifted the emphasis from kinetic to non-kinetic means, subsumed under the neo-military paradigm (Hoffman, 2007, pp. 6-17).

Table 1: Comparisons between kinetic tactics and non-kinetic (neo-military) tactics

Dimension	Kinetic (traditional)	Non-kinetic (neo-military)
Main objective	Physical destruction of the adversary's force and infrastructure	Influencing the adversary's perceptions, will and decision-making capacity
Means	Conventional armament, land, air, naval, space operations	Information, psychology, economy, cyberspace, culture, law
Method of action	Direct strikes, classic military confrontation	Manipulation, disinformation, indirect pressure, cyber attacks
Immediate effect	Human losses, material destruction	Confusion, demoralization, social and political destabilization

Dimension	Kinetic (traditional)	Non-kinetic (neo-military)
Attribution	Easy to identify (it is known who is attacking)	Often ambiguous or denied ("under /below the threshold" operations, deniable)
Duration of impact	Short or medium term (until capacity is reconstituted)	Long term (modifies mentalities, social relations, economic dependencies)
Examples	Military invasions, bombings, conventional battles	Information warfare, psychological warfare, cyber, economic, cognitive warfare

Cognitive warfare refers to actions aimed at influencing the mental processes of individuals or groups, including perception, information assessment, and decision-making (Claverie, du Cluzel, 2023, pp. 1-4). Its central objective is not only to manipulate informational content, but to shape the way it is processed, thereby affecting the interpretation of reality and the ability to make rational decisions. Relevant examples include the use of structured information flows, subtle disinformation, or artificial intelligence algorithms to shape public opinion and indirectly influence social behaviour. Therefore, cognitive warfare targets the human mind and internal information processing mechanisms.

Information warfare consists of *"the collection, manipulation, and dissemination of information to influence the perceptions and behaviours of the adversary"* (Joint Chiefs of Staff, 2004, pp. 21–30). Unlike cognitive warfare, the focus is on the content of messages and communication channels rather than on internal cognitive processing. Examples include propaganda, fake news, digital disinformation campaigns, or the interception and modification of communications. Thus, information warfare aims to control the flow of information and shape perceptions of external reality.

Psychological warfare aims to influence emotions, attitudes, and behaviours through direct or indirect psychological techniques. Unlike cognitive warfare, which targets the structures and mechanisms of thought, psychological warfare focuses on motivations and emotional reactions (Neacșu, 2004, pp. 21-30). Examples include psychological terror campaigns, demoralizing messages to opposing troops, or inducing fear and uncertainty to undermine group cohesion. This type of warfare has older historical roots and is still relevant in traditional influence operations.

Ideological warfare aims to promote and impose a set of values, beliefs, or doctrines on a social group or nation. The main objective is to shape collective

beliefs and cultural norms, influencing long-term behaviours (Dobrinescu, 2017, pp. 33-44). Unlike cognitive warfare, which targets individuals, ideological warfare focuses on communities and cultural structures. Examples include promoting political doctrines, supporting social movements to destabilize the adversary, or transnational propaganda campaigns.

Economic warfare involves the use of financial, commercial, and industrial resources to diminish an adversary's ability to act strategically. Actions are aimed at disrupting production, access to resources, or economic stability (Popa, 2018. pp. 45-53). Examples include economic sanctions, trade blockades, manipulation of financial markets, or attacks on critical infrastructure. Unlike cognitive or information warfare, the effects are material and quantifiable, with indirect repercussions on social perceptions and behaviours.

Technological warfare focuses on the development and application of advanced technologies to achieve strategic or tactical superiority. Objectives include either improving one's own capabilities or sabotaging those of the adversary (Zodian, 2019, pp. 7-18). Examples include the development of hypersonic weapons, autonomous drones, advanced surveillance systems, or encryption and automated disinformation technologies. Unlike cyber operations, technological warfare includes both hardware and software components integrated into complex systems

Religious warfare uses religious beliefs and institutions to mobilize mass support, generate divisions, or weaken the adversary. Unlike ideological warfare, the emphasis is on spiritual values and sacred norms, not political or social doctrines (Cîrstocea, 2016, pp. 55-67). Examples include tensions or confrontations between different religious groups, religious radicalization, or the use of religion to legitimize a conflict. The impact is felt at the social and cultural level, influencing the cohesion and stability of communities.

Diplomatic warfare involves the use of international relations, negotiations, and political pressure to gain strategic advantages without resorting to direct force. The objective is to influence the behaviour of states or international organizations through alliances, isolation of the adversary, or manipulation of external opinions (Mouslim, 2022, pp. 423-445). Examples include international sanctions, lobbying in multilateral organizations, strategic bilateral negotiations, or diplomatic image campaigns. Unlike economic or military warfare, the main instrument is politics and diplomacy, not material resources or physical force.

Cyber operations refer to the use of computer systems and digital technologies to attack, defend, or manipulate an adversary's infrastructure. The effects can be direct on data and infrastructure or indirect, through the impact on the target's

cognitive and psychological processes (Haataja, 2022, pp. 423-445). Examples include cyber attacks on critical infrastructure, ransomware, manipulation of electoral databases, or compromise of communications systems. Unlike other types of warfare, the action is predominantly technological and digital.

Within the theory and practice of modern conflict, we can say that cognitive warfare is an emerging operational domain focused on influencing mental processes. Unlike traditional forms of warfare, which seek to have a direct impact on the physical strength or infrastructure of the adversary, cognitive warfare focuses on the perceptions, assessments, and decisions of actors, targeting how they interpret reality and react in an operational context. Conceptually, it differs from information, psychological, or cyber warfare in that it is not limited to manipulating messages or disrupting digital infrastructures, but seeks to reshape fundamental cognitive processes at the individual and collective levels.

CHARACTERISTICS OF THE COGNITIVE DOMAIN

The cognitive domain is distinguished by a series of defining features that make it a unique operational space that is difficult to control using traditional methods. Firstly, it is intangible, as its actions do not produce direct and visible effects on the physical environment, but rather operate on the minds and internal thought processes of individuals or groups. This intangibility makes it difficult to measure success or assess the tactical or strategic impact of interventions.

Second, the cognitive domain is both individual and collective. At the individual level, cognitive warfare targets the processes of perception, attention, memory, and decision-making, seeking to alter how information is interpreted and integrated. At the collective level, the impact extends to public opinion, social cohesion, and cultural norms, influencing group behaviours and their ability to respond coherently. This duality requires approaches that combine psychological, sociological, and cybernetic analysis, integrating interdisciplinary perspectives for a comprehensive understanding of the cognitive domain.

Thirdly, the cognitive domain is based on perception (Claverie, du Cluze, 2023, pp. 1-13), which implies that operational reality is constructed subjectively. Unlike physical or digital environments, where the effects of actions can be measured objectively, in the cognitive domain, success depends on how information and messages are perceived and interpreted. Thus, manipulating information flows, introducing subtle misinformation, or amplifying emotions and prejudices become central tools in cognitive warfare, as they directly influence the target's decision-making and risk-assessment processes.

COGNITIVE WARFARE AS THE SIXTH OPERATIONAL DOMAIN

Recognizing the cognitive dimension as the *"sixth operational domain"* (Le Guyader, Cole, 2022, pp. 1-5) of contemporary conflict is an essential conceptual step in integrating this perspective into modern military doctrine. In the classical tradition, military operations are conducted in the land, sea, air, space, and, more recently, cyber domains. The introduction of the cognitive domain reflects the recognition that strategic success no longer depends exclusively on physical or technological superiority, but also on the ability to influence the adversary's decision-making processes and perceptions.

This concept has been reinforced in the literature by identifying the interdependencies between the physical and cognitive domains: military conflicts on land, in the air, or in cyberspace can have limited effects if they are not accompanied by strategic management of the adversary's perceptions and decisions. In this context, cognitive warfare becomes an emerging operational domain that not only complements but redefines the dynamics of modern conflict, highlighting the importance of integrating cognitive components into the planning and execution of military and non-military operations.

With regard to the role of artificial intelligence, social networks, and big data (https://www.oracle.com/ro/big-data/what-is-big-data/), recent technological developments have amplified the importance of the cognitive domain, making it a critical operational one. Artificial intelligence (AI) plays a central role in the rapid processing of massive amounts of data and in modelling target behaviours (Deppe, Schaal, 2024 pp. 1-6). Machine learning algorithms enable the identification of patterns of thought and behaviour in individuals or groups, facilitating the design of more precise and adaptive influence campaigns. In addition, AI can be used to generate content, simulate response scenarios, or optimize cognitive strategies, increasing the effectiveness of actions on the perceptions and decisions of the adversary.

Social networks are the central infrastructure through which a significant part of cognitive warfare is conducted. They allow for the rapid and targeted dissemination of messages, the amplification of emotions, and the polarization of opinions. Unlike traditional media, social networks offer the possibility of instant feedback and allow for the adaptation of influence campaigns in real time, transforming communication into a dynamic and interactive process.

Big data complements this architecture, providing unprecedented analytical resources for understanding collective behaviours and cognitive susceptibilities. Quantitative analysis of big data allows for the identification of population

segments vulnerable to certain messages, the evaluation of campaign impact, and the adjustment of strategies to maximize the effect on cognitive processes. The integration of AI, social networks, and big data thus transforms cognitive warfare into an operational domain characterized by speed, complexity, and adaptability.

SPECIFIC TACTICS OF COGNITIVE WARFARE

Cognitive warfare manifests itself through a wide range of indirect actions, unscrupulously targeting the human mind and social cohesion, including multiple forms of psychological pressure, information manipulation, and institutional undermining, which take the form of the following types of actions:

Actions aimed at undermining the morale of the civilian population – this type of actions targets social, professional, demographic, and geographic categories, adapting its messages and vectors to exploit the specific vulnerabilities of each group (from the elderly and single parents to workers in affected industries, students, ethnic or religious minorities, social protection, access to services, or discrimination, and geographically, campaigns exploit perceptions of rural marginalisation or urban pressures – housing, transport, health) (Munteanu, pp. 10-18).

Actions that diminish citizens' standard of living – against the backdrop of public discontent, cognitive warfare amplifies its effectiveness by using misinformation and emotional manipulation to exploit social frustrations and accentuate perceptions of economic and political injustice. *"The decline in living standards is exacerbated by information campaigns that induce panic, stimulate the division of personal or collective opinions, and undermine the legitimacy of public decision-makers, deliberately seeking to dramatically lower citizens' living standards by creating economic, financial, social, and health crises"* (UNDP, pp. 85–102). In this climate of tension, citizens become more prone to irrational collective decisions (panic buying, capital withdrawals, spontaneous protests), which generates economic instability and additional pressure on the political system, forcing the redirection of public resources from development to the management of informational and social crises.

Intergroup antagonism between different social categories – mechanisms that generate and amplify conflict act on the community by cultivating the perception that certain social categories are undeservedly privileged and have resources or rights that, in fact, do not belong to them. This strategy aims to create division between segments of the population, inducing a sense of injustice and fuelling tensions based on perceived inequalities. Manipulative information campaigns reinforce the image of certain privileged groups to the detriment of others, a process that promotes social division, undermines collective solidarity, and erodes social cohesion.

Actions that weaken national economic capacity – that manifest themselves through subtle mechanisms that influence strategic decisions, causing decision-makers to adopt policies and measures that weaken the industrial base. Under the impact of information campaigns and persuasive narratives, decision-makers are persuaded to close, sell, resize, or outsource industrial production, citing pretexts such as excessive pollution, lack of profitability, lack of raw materials, avoidance of trade union movements, insufficient funds for re-engineering, the absence of markets, or even the encouragement of foreign investment (Galeotti, pp. 85-112). Discourses that minimize the importance of strategic resources for the national economy or the need for major infrastructure (such as highways) are also promoted, thus justifying the processes of deindustrialization. The result of these actions is the closure of factories/companies, the reduction of domestic production capacity, and increased external economic dependence, which significantly weakens national security and lowers the standard of living of the population.

Actions to coerce and influence a state outside of military occupation – the aim is to induce policies and decisions that gradually (using the technique of small steps) lead to the loss of economic and financial-banking sovereignty, the surrender of control over critical infrastructure, national resources, capital flows, and even the workforce. Through persuasive discourse and informational pressure, decision-makers are steered towards measures that favour the alienation of public and private property, tipping the balance of agricultural land and strategic resource ownership in favour of external entities. At the same time, risk insurance systems and social protection mechanisms are compromised, reducing the state's ability to protect its citizens and domestic economy (Galeotti, pp. 113–139). Overall, these actions aim to gradually integrate the target state into a framework of structural dependence, whereby economic, financial, and social decision-making is diverted from the national interest to the interests of external actors.

Actions that undermine the functionality of critical systems – through manipulative discourse and policies promoted under the pretext of reform (Ib., pp. 8–20), actually aimed at dismantling the functional systems of society, eliminating vital elements without proposing viable replacement solutions. These actions directly or indirectly target essential segments of social and state infrastructure – education, the pension system, social assistance, justice and the legislative framework, the health system, as well as the financial, economic and commercial architecture, environmental protection and research capacity – eroding institutional cohesion and the capacity to provide public goods. Consequently, what is presented as modernisation, if not kept under legal control, becomes in practice a process of structural weakening that amplifies social vulnerabilities and reduces national resilience.

Military operational actions – the primary objective of this type of actions is not necessarily the physical destruction of the adversary's combat capability, but rather the induction and maintenance of a perceived state of imminent threat (Giles, 2022, pp. 8–20) – a persistent psychological pressure capable of degrading decision-making, internal cohesion, and the political will to respond effectively.

From a theoretical perspective, this dimension combines elements from studies on hard/soft power and from strategic game theory based on uncertainty: the aim is to maximize the perceived cost of a reaction from the target, without necessarily crossing the threshold of open confrontation. The operational mechanism is based on the synergy between material manifestations (military capabilities, shows of force) and non-material manifestations (narratives, information manipulation, subversive foreign policy), so that the threat remains credible and persistent.

The tactics used to achieve this cognitive pressure include, without providing operational instructions, the development and display of superior military capabilities (which fuel the perception of technical and military superiority), the conduct of shows of force and exercises with a deterrent role in the vicinity of borders, limited penetrations or incursions that test reaction thresholds, as well as political and administrative initiatives (e.g., the creation of autonomous enclaves governed by ethnic minorities) designed to erode the sovereignty and internal cohesion of the targeted state. The deliberate activation of frozen conflicts (Bargués et al., pp. 8-20), the justification of interventions through the rhetoric of minority protection, airspace and maritime violations, or illegal practices regarding the treatment of prisoners are all tools that amplify the feeling of vulnerability and uncertainty.

The intended effects are multiple and interconnected: disruption of the command-and-control process, intensification of information jamming (contradictory information, deliberate noise), erosion of domestic public and political support for security policies, weakening of internal and external ties (alliances), and induction of strategic or tactical errors on the part of the adversary. The strategy relies on the fact that decisions made under pressure are more susceptible to cognitive errors (excessive optimism, distortion of normality, overreactions, passivity).

From a legal and ethical perspective, these practices raise significant issues: many of the actions mentioned may violate international law (territorial sphere, protection of civilians, treatment of prisoners) and ethical standards of political-military leadership. In addition, the use of information manipulation and synthetic deepfake technologies (Barela, 2024/2025, p. 1) amplifies the risk of eroding public trust and fragmenting the information space, affecting the long-term resilience of societies.

Actions aimed at undermining military cohesion and morale – this type of actions deliberately targets the destruction of trust: in military and political-military leadership, in the legitimacy of the cause for which they are fighting, and in the reliability of the weapons and logistics on which the military entity relies. By eroding this trust, not necessarily through physical force, but through informational and symbolic campaigns that cast doubt on the competence, honesty, and purpose of the leadership or the safety of the equipment, the aim is to transform the motivation and individual and collective behaviour of the military.

The expected effect is progressive and holistic: initially, demotivation and a decline in confidence appear, which can evolve into segments of personnel abandoning the fight, then into a total loss of will to fight, and finally into a replacement of military order with indiscipline, disorganization, chaos, and insubordination. This decline creates a vicious circle: the loss of discipline facilitates the spread of rumours and panic, which in turn increases the receptivity of military personnel to new cognitive attacks.

The psychosocial mechanisms involved are based on compromising trust capital (legitimacy, competence, integrity), exploiting cognitive errors (confirmation, availability), and attacking social cohesion (exacerbating ethnic, professional, or economic tensions). From an informational perspective, the strategy combines credibility reduction (coupled with amplification of informational *"noise"*) with symbolic actions designed to discredit leaders and undermine cohesion and morale in military units.

The operational consequences are severe: degradation of command-and-control capabilities, erosion of coherent response capabilities, increased error rates and decisions made under pressure, as well as an increased risk of institutional collapse in the affected structures. In strategic terms, the objective is not necessarily immediate physical destruction, but rather neutralizing the adversary's ability to leverage its human and moral resources.

Political compromise actions – this type of actions targets a whole set of informational practices designed to distort collective representations, degrade decision-making capacity, and reconfigure the political power structure by exploiting cognitive and algorithmic mechanisms.

In this logic, political compromise operations (blackmail, intentional disclosures of information, deepfakes, discredit campaigns) are mobilized to draw high-ranking political elites to one side, to generalize and exaggerate reprehensible acts, and thus to discredit individuals regardless of their achievements, a phenomenon that undermines the credibility of actors and institutions.

At the same time, narrative manipulation and polarizing amplification (through social platforms, networks of automated accounts, and complicit media) sow irreconcilable contradictions between factions, fuel internal controversies, and stimulate ideological hatred, resulting in prolonged political crises and social fragility.

At the strategic level, external actors/parties have used institutional capture mechanisms to ensure the loyalty of the administrative leadership – frequent promotion/rotation of politicians in key positions, replacing technical experts with political figures, supporting doctrine and legislation favourable to the economic interests of certain groups and, in extreme cases, facilitating the emergence of politically affiliated paramilitary groups, all in order to undermine the continuity of state projects, encourage corruption, and maximize political division.

Therefore, based on the examples listed, we can provide a convincing picture of the socio-political contexts in which cognitive warfare becomes operational as well as of its destructive effects. The combination of different tactics, in varying proportions, aims to maximize impact, and the cost-effectiveness ratio of these operations is significantly more favourable to the aggressor than that of conventional military means.

CONCLUSIONS

Cognitive warfare is an emerging operational domain aimed at shaping the mental processes, perceptions, and decisions of both individuals and communities. Unlike traditional conflicts, which focus on immediate kinetic effects, this form of conflict frequently resorts to non-kinetic instruments – propaganda, disinformation, psychological operations, and digital means – designed to restructure the way information is processed and interpreted, thus generating lasting strategic effects.

The integration of digital technologies, social platforms, big data analytics, and artificial intelligence significantly amplifies the effectiveness of cognitive operations, increasing the speed of response, adaptability, and micro-targeting capabilities of influence campaigns. Consequently, the cognitive dimension is becoming a central factor in contemporary geopolitical strategies, with repercussions on social cohesion, institutional resilience, and the level of trust between state actors.

Institutional and normative divergences between political regimes outline a paradox of cognitive vulnerability: democracies, through transparency and informational pluralism, are increasingly exposed to manipulation and division, while authoritarian regimes show structural resilience to such attacks, often achieved by restricting civil liberties. At the same time, cognitive warfare intersects with strategic persuasion tools and psychological operations, integrating normative,

emotional, and cognitive influence into a coherent strategic framework on an international scale.

The impact on collective security and international law is considerable: the erosion of trust between states, the fragmentation of coalitions, and regulatory gaps regarding non-kinetic aggression raise complex issues of regulation and response. The political response requires the development of vectors of societal resilience, international standards of transparency, and coordinated mechanisms for counteraction and harmonization.

In this context, conceptualizing cognitive warfare as a *"sixth operational domain"* emphasizes the need to integrate the cognitive dimension into strategic planning and international security architecture, recognizing the influence on perceptions and decisions as a central element of current strategic dynamics.

BIBLIOGRAPHY:

1. Babacek, M. (2024). *Războiul cognitiv*: *Opriți competiția mondială pentru "Controlul creierului uman"*, in Revista Art – Emis Academy.
2. Barela, S.J. (2024/2025). *Digital Disinformation Operations in Armed Conflict* – Info-Brief. Switzerland: Geneva Academy of International Humanitarian Law and Human Rights.
3. Bargués P., Bourekba, M., Colomina, C. (2022). *Hybrid threats, vulnerable order*, CIDOB Report.
4. Cîrstocea, I. (2016). *Religia ca factor de conflict și război*, in *Impact Strategic*, no. 1. București: Editura Universității Naționale de Apărare "Carol I".
5. Claverie, B. du Cluzel, F. (2023). *Cognitive Warfare Concept*. Innovation Hub – Allied Command Transformation (ACT), NATO.
6. Deepe, C., Schall, G.S. (2024). *Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept*, Frontiers in Big Data, vol. 7.
7. Galeotti, M. (2022). *The Weaponisation of Everything*. A Field Guide to the New Way of War. Yale University Press, New Haven.
8. Giles, K. (2016). *Russia's 'New' Tools for Confronting the West*. Chatham House Research Paper.
9. Haataja, S. (2022) *Cyber operations against critical infrastructure under norms of state behaviour in cyberspace*, in *International Journal of Law and Information Technology*, vol. 30, no. 4.
10. Hoffman, F.G. (2007). *Conflict in the 21st Century*. The Rise of Hybrid Wars.
11. Joint Publication JP 3-13: Information Operations (updated 2014).
12. Miller, G.A. (1956). *The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information*, in *Psychological Review*, Washington, D.C., vol. 63, no. 2.
13. Mouslim, H. (2025). *Coercive Diplomacy Recalibrated: Evaluating Effectiveness, Risks, and Modern Challenges*, in *African Scientific Journal*, vol. 3, no. 29.

14. Munteanu, D. (2022). *Barometrul rezilienței societale la dezinformare*. Euro-Atlantic Resilience Centre (E-ARC).
15. Naganuma K. (2021). *Warfare in the Cognitive Domain: Narrative, Emotionality, and Temporality*, NIDS Commentary no. 163, National Institute for Defense Studies Japan.
16. Neacșu, I. (2004), *Războiul psihologic. Tehnici și strategii de influență*. București: Editura Militară.
17. Neisser, U. (1967). *Cognitive Psychology*. Prentice Hall.
18. Popa, I. (2018). *Războiul economic: forme, mijloace şi efecte*, in *Revista de Ştiinţe Militare,* no. 2. Bucureşti: Editura Centrului Tehnic-Editorial al Armatei.
19. Thomas, T.L. (2025). *Russian Military Thought: Concepts and Elements*, TRADOC G-2/OE Watch.
20. UNDP (2022). *Human Development Report 2022*. Uncertain Times, Unsettled Lives, UNDP, New York.
21. Voicu, M. (2018). *Matrioșka mincinoșilor: fake news, manipulare, populism*. Editura Humanitas.
22. Zodian, V. (2019). *Impactul progresului tehnologic asupra conflictelor armate contemporane*, in *Impact Strategic*, no. 3. București: Editura Universității Naționale de Apărare "Carol I".
23. https://brainly.ro/tema/6593720, retrieved on 11 September 2025.
24. https://www.oracle.com/ro/big-data/what-is-big-data/, retrieved on 15 September 2025.