# THE COGNITIVE COMPONENT OF THE RUSSIAN FEDERATION'S WAR AGAINST UKRAINE

*Lieutenant Georgiana BLĂJAN*

*Psychological Operations Center "Samoilă Mârza", Bucharest*

DOI: 10.55535/RMT.2025.3.21

*The global competition among major powers is taking on new dimensions in the context of technological evolution, particularly with the emergence of new forms of conflict. The war between the Russian Federation and Ukraine marks a transformation in modern warfare, highlighting the use of methods specific to cognitive warfare, in which information technologies, artificial intelligence, and media channels are employed to influence the perceptions, behaviors, and societal cohesion of the civilian population. Russia has made extensive use of such tools to shape specific narratives, induce confusion, and undermine Ukraine's informational resilience. This article aims to provide a perspective on the importance of the information space as a new strategic battlefield, illustrating specific practices of the Russian Federation's cognitive warfare in Ukraine.*

*Keywords: cognitive warfare; artificial intelligence; war in Ukraine; media literacy; cognitive superiority;*

## INTRODUCTION

Concerns regarding the cognitive component of warfare, viewed in NATO's doctrine for information operations as a dimension of the information environment, have increased significantly in recent years, particularly due to the difficulty of identifying specific threats. With the development of propaganda tools employed by the Russian Federation against the West, the North Atlantic Alliance has placed greater emphasis on the need to achieve cognitive advantage, which has led to the conceptualization of the term *"cognitive warfare"* (adopted in Romanian as *"război cognitiv"*) (NATO Cognitive Warfare Concept, 2025).

Although controversies have existed, either regarding the similarity of this concept to other related notions or concerning the challenges of defining it as a distinct domain or dimension, the importance of its application is indisputable, especially in the context of technological advances in artificial intelligence and innovations in cognitive sciences. These aspects are considered fundamental for leveraging this dimension on a much broader scale.

Currently, the most relevant example of the application of cognitive warfare can be found in the conflict in Ukraine, where the Russian Federation has made extensive use of this type of warfare to influence not only the perceptions of the Ukrainian population but also international public opinion. The leadership in Moscow benefits from long-standing experience in this field, frequently being cited in discussions on information manipulation and media control. Thus, through elaborate disinformation campaigns, manipulation of the information environment, and strict control of internal information flows, Russia has sought to erode trust in Ukrainian institutions and to divide society. This strategy was intended to compensate for certain deficiencies in conventional military capabilities, by providing a strategic advantage through influencing the adversary's decisions and behaviors. Moreover, the use of advanced technologies, such as artificial intelligence and digital platforms, has amplified the impact of these actions.

Taking the above into consideration, this article proposes an analysis of the evolution of the concepts underlying the term *"cognitive warfare"*, culminating in an examination of the application of cognitive warfare in Russia's strategy against Ukraine. Finally, the article outlines future development perspectives of the cognitive warfare concept, highlighting not only its strategic and technological implications in current and future conflicts, but also the associated ethical dimensions, as well as the need to enhance societal resilience in the face of this type of threat.

## THEORETICAL APPROACHES TO THE CONCEPT OF COGNITIVE WARFARE

The term *"cognitive warfare"* has been the subject of significant debate in the specialized literature, either due to its perceived similarities with other pre-existing forms of conflict or because of the variable interpretations of the proposed definitions, which did not indicate substantial conceptual evolution beyond earlier theoretical frameworks. Nevertheless, the use of specific instruments by certain actors to shape the information environment for their own purposes, combined with the exponential development of technology, has generated the need to address such a concept. In order to outline a comprehensive and nuanced understanding of cognitive warfare, this section analyzes a series of relevant definitions from the specialized literature.

### *The Russian Federation's Perspective*

The Russian Federation possesses one of the oldest and most consolidated traditions in the use of psychological influence instruments, disinformation, and strategic manipulation, with roots that long predate the emergence of modern concepts of cognitive warfare. In this context, Russian military doctrine can be analyzed over time through several key concepts, such as *Maskirovka*, *Active Measures*, *Reflexive Control*, and *New Generation Warfare*. Although each of these notions has distinct characteristics, they are linked through doctrinal continuity, representing successive stages in refining the way Russia conceives and conducts influence operations and indirect conflict.

The term *Maskirovka*, often inadequately translated as *"camouflage"*, represents the traditional foundation of Russian military deception in the twentieth century. The concept dates back to 1904, with the establishment of the first specialized school, the Higher School of Studies (Bouwmeester, 2017). A more concrete explanation of military deception refers to the use of *"the complex of measures devised to confuse the enemy regarding the presence and disposition of forces, their condition, readiness, actions and plans*" (Bechis, 2020, p. 122). Although historically similar measures can be identified as far back as antiquity

(Sun Tzu's philosophy – *"All warfare is based on deception"*), the adaptation of *Maskirovka* covered a much broader scope, aiming at *"rational manipulation, either through the dissemination of contradictory information or by supporting false conclusions."* (Anuța, 2016, p. 45). The method reached its peak during the Second World War, through the success achieved against German troops; a result later explained (Don Levine, 1960 apud Zimmer, 2013) by the fact that *"the government wasessentially a counterintelligence apparatus. It was conceived in 1903 by Lenin as an operation in counterintelligence against the Czarist regime, and it remained a conspiracy ever since"*, suggesting that Russian ideology has long been closely tied to practices of disinformation and information control, whose scale significantly exceeded the capabilities of other actors.

The *Active Measures Program* (in Russian, *Aktivnye Meropriyatiya*) was intended to go well beyond the previous concept, being carried out primarily by state structures (intelligence services, government agencies) in order to achieve strategic objectives without resorting to military force. The dating of the term is relatively vague, but it is generally accepted that the Union of Soviet Socialist Republics (USSR) used it beginning in the late 1950s to describe a set of covert and deniable operations of political influence or subversion. These included (but were not limited to) the establishment of front organizations, support for allied political movements, the orchestration of internal unrest, and the dissemination of disinformation (Galeotti, 2019). According to the same author, the concept was described in the *Counterintelligence Dictionary* (1972) of the KGB's *"Felix Dzerzhinsky"* Higher School as being used in counterintelligence activities by state security organs, encompassing projects aimed at strengthening the position of spies within and near the enemy camp, targeted disinformation actions against the adversary, compromise and demoralization operations, the transfer to USSR territory of individuals with special operational value, the acquisition of information of strategic interest, and similar activities.

The theory of *Reflexive Control (RC)* is the concept most frequently encountered in the specialized literature when discussing the introduction of the domain of *"cognitive warfare"* in connection with the Russian Federation. First formulated in the Soviet Union in the 1960s by Vladimir Lefebvre, it attracted interest within Soviet military circles and was formally adopted by the Soviet Army only in the late 1970s. Reflexive Control is most often examined as *"a mechanism for influencing the decision-making process of a state and involves the transmission of fabricated* *information (partially true, partially false) to the adversary in order to induce it to make a voluntary decision favorable to the initiator's interests"* (*Reflexive Control Theory in the Logic of Hybrid Warfare*, 2017). Consequently, Reflexive Control is considered an important component in the evolution of Russian doctrine, as it goes beyond the tactical and operational levels associated with *Maskirovka*, having a strategic impact during the Cold War.

The most up-to-date approach to the use of manipulation at the strategic level is the so-called *Gerasimov Doctrine*, derived from an article written in 2013 by Russian General Valery Gerasimov, Chief of the General Staff of the Armed Forces of the Russian Federation, translated into English as *"The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations".* The author's vision referred to the blurring of the line between war and peace, as well as to the fact that *"the focus of applied methods of conflict has alteredin the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitarymeasures – applied in coordination with the protestpotential of the population."* (Gerasimov, 2013, p. 1). This description further intensified the interest of the Russian Federation in applying non-kinetic instruments to achieve cognitive advantage.

Ultimately, the concepts practiced by Russia in association with cognitive warfare are not an innovation of the Putin era, but rather a strategy with deep historical roots. Nevertheless, under his leadership, forms of influence have been refined and applied on a large scale, with the introduction of a new key instrument – the civilian population – increasingly used as a means of shaping the information environment.

### *The Interdisciplinary Approach*

The notion of *cognitive warfare* has been adopted both in military and academic literature, with multiple experts becoming aware of how technology has been used to influence the evolution of certain trends across various states.

The cognitive component was studied several decades ago, during the analysis of the USSR's success in applying Reflexive Control. Specialized literature (Chotikul, 1986, p. 43) noted that *"cognition results from the reflection of the material world in the human mind"*, which explains why Soviet doctrine focused on influencing environmental conditions in order to constrain the enemy to act accordingly.

Beginning in 2019, the concept was adopted by several authors who specifically associated it with its exploitation by the Russian Federation or China, emphasizing that it represents *"a strategy that focuses on altering how a target population thinks – and through that how it acts"* (Backes, Swab, 2019 apud Deppe, Schaal, 2024). A more comprehensive definition describes cognitive warfare as *"an unconventional form of warfare that uses cybertools to alter enemy cognitive processes, exploit mental biases or reflexivethinking, and provoke thought distortions, influence decision-making andhinder actions, with negative effects, both at the individual and collective levels"* (Bernard, Cluzel, 2020, p. 2). This definition introduces technology as a key vector for transmitting manipulative messages.

### *NATO's Conceptualization*

The first NATO member to invoke the term *"cognitive warfare"* was the United States of America (2017), with the aim of describing the means available to an actor to manipulate the cognitive mechanisms of an enemy or a population in order to weaken, penetrate, influence, or even subjugate or destroy it (Ib.).

Within NATO, the term was officially institutionalized and promoted starting in 2020 by the NATO Innovation Hub, through a series of strategic reports defining cognitive warfare as an advanced form of conflict that targets not only information control, but also the cognitive processes of individuals – perceptions, emotions, memory, and decision-making capacity. The development of a common concept within the Alliance became necessary as a result of hostile actions conducted in the sphere of cognitive warfare against member states; therefore, representatives of the academic community and analytical centers were also integrated into the process of establishing the conceptual framework.

According to the *NATO Cognitive Warfare Concept* (2025, p. 5), the term is defined as *"the fight for cognitive superiority. Contesting in this environmentcomprises deliberate, synchronized military and non-military activities throughout thecontinuum of competition designed to gain, maintain and protect cognitive advantage".* The document also highlights the relevance of cognitive warfare through the development of technologies such as the militarization of nanotechnologies, biotechnologies, and human augmentation, suggesting that the configuration of future conflicts will no longer belong exclusively to the informational domain.

### *China's Perspective*

Chinese strategists identified the value of the cognitive domain as early as the early 2000s. In recent years, China has devoted increased attention to the potential use of neuroscience and artificial intelligence, not only in the medical field, but also in the development of cutting-edge advanced technologies.

The *China Brain Project* (CBP) regained priority in 2021, despite having been postponed for five years due to ethical concerns regarding its application (Normile, 2022). Guo Yunfei (President of the Information Engineering University under the Strategic Support Force of the People's Liberation Army) argued that *"among the physical, informational, and cognitive domains, the cognitive domain will ultimately become the primary battlefield of military confrontation between major powers. Warfare in the cognitive environment directly affects the brain, influencing emotions, motivations, judgments, and actions – and may even control the enemy's brain."* (*The Future of China's Cognitive Warfare: Lessons from the War in Ukraine*, 2020).

### *Conceptual Deconfliction*

The innovative character of the term and the absence of a dedicated doctrine often leave room for interpretations or overlaps between cognitive warfare and other notions such as *psychological operations* (PsyOps) or *information warfare*.

Unlike PsyOps, which are used exclusively in the military domain and directed at a specific target audience, cognitive warfare proposes a broader approach that integrates PsyOps tactics but is not limited to them. Thus, cognitive conflict employs multiple instruments of power, supplemented by emerging technologies, neuroscience, and digital platforms, in order to control the behavior of large groups of individuals.

With regard to information warfare, NATO approaches it from the perspective of protecting access to sensitive information, intercepting and exploiting the adversary's information, destroying information infrastructures, and disrupting communication flows. Cognitive warfare, by contrast, expands the field of action, focusing not only on data or communication channels, but on how individuals perceive, process, and respond to information. Complementarily, the *NATO Cognitive Warfare Concept* (p. 4) states that the term *"should also not be misconstrued as StratCom by another name. InfoOps, PsyOps, and MilPA are only some of the capabilities and functions used in the daily contest for cognitive advantage".*

## THE INSTRUMENTALIZATION OF COGNITIVE WARFARE IN RUSSIA'S STRATEGY AGAINST UKRAINE

The Russian Federation's experience in employing forms associated with cognitive warfare is deeply rooted in the history of its relations with Western states, but especially in maintaining control over territories within the former Soviet space. Although the Putin regime was not the first to embrace expansionist visions centered on disinformation and the manipulation of reality in order to distort behavior, upon his accession to the presidency, the focus shifted toward controlling information and the ways in which it reaches citizens, specifically to serve regime interests. Such actions were initially directed at Russia's own population, with the Kremlin introducing new forms of information control on an annual basis starting in 2000. At present, any expression perceived as contradicting the Kremlin's agenda is subject to punishment, with censorship intensifying following the launch of the full-scale invasion of Ukraine (Bugayova, Stepanenko, 2025).Regarding the conduct of the war in Ukraine (2022), Russia has effectively employed a range of instruments associated with the cognitive component in order to compensate for gaps in conventional capabilities, making clear that the successes achieved would not have been possible through military means alone. To provide a more comprehensive picture of the behavioral influence ecosystem used by the Russian Federation against Ukraine, the evolution of this mechanism is analyzed both in the pre-conflict phase and after the outbreak of hostilities.

### *Before 2022: Preparing the Information Terrain*

Ukraine's orientation in the early 2000s toward transparent, Western-inspired governance was perceived by the Russian central authorities as a direct threat to the Putin regime. Consequently, Moscow intensified its external cognitive warfare efforts by launching information campaigns designed to undermine democratic processes and slow Ukraine's rapprochement with the West. Following the Orange Revolution, which resulted in the rerun of presidential elections and the appointment of a pro-European candidate despite Putin's preferred contender, Russia began constructing and disseminating narratives of separatism in Ukraine. These narratives were later strategically activated in 2014 during the hybrid operation to occupy eastern and southern regions of the country (Bugayova, Stepanenko, 2025). They were further reinforced by messaging that emerged in the aftermath of the Euromaidan protests (autumn 2013), with Russian media portraying the demonstrations as *"an unconstitutional coup endangering the Russian-speaking population"* (Hofirek, 2021, p. 11).

The effects included the organization of anti-Euromaidan protests from Odesa to the Luhansk regions and Crimea, ultimately culminating in the annexation of Crimea and the outbreak of the conflict in Donbas. The use of proxy groups (through protesters) and disinformation elements (via conspiratorial narratives such as the alleged abandonment of Ukraine – and implicitly Crimea – by the West;

the historical and spiritual unity between Ukraine and the Russian Federation; and Russia’s role as protector of abandoned states) aimed to foster among audiences in the affected regions the belief that annexation did not constitute aggression, but rather a historical restoration (Chiriac, 2021). Although the strategies employed in Crimea and Donbas were similar, the outcomes differed due to *“the lack of Russian regular forces’ timely decisive action (which) caused the conflict to transform into a frozen conflict”* (Hofirek, p. 2).

Following the military interventions of 2014, Russia recalibrated its national security paradigm, culminating in the adoption of the new Information Security Doctrine (December 2016). The document reflected a strongly defensive vision, portraying Russia as a *“besieged cyber fortress”.* It emphasized threats originating from foreign states – ranging from cyberattacks and digital espionage to ideological influence – while advocating stronger internal control over the Russian internet, reduced dependence on Western technologies, and the development of domestic IT capabilities (Pynnöniemi, Kari, 2016). Framing Russia as a victim of Western attacks served to justify the malign intentions the Kremlin intended to pursue.

Moreover, in the same year, Putin approved the Foreign Policy Concept of the Russian Federation, which reinforced the objective of *“strengthening the position of Russian media and communication outlets in the global information space and conveying Russia’s perspective on international processes to a broader international audience”.* Over the past decade, Moscow has relied on multiple channels to disseminate Russian propaganda internationally, including multilingual state-backed media outlets (RT, Sputnik, and TASS) as well as proxy websites (News Front, SouthFront, Geopolitica.ru, Strategic Culture Foundation), which, although not officially acknowledged by the Russian state, are indirectly controlled by it (Romanian Intelligence Service, 2020). State-controlled media entities have received substantial funding to broadcast Kremlin-favorable messaging in multiple languages and regions worldwide. The objective was **to construct a parallel reality** in which the West is depicted as morally declining, contrasted with an image of Russia as a defender of traditional values, sovereignty, and an *“authentic”* global order. Another key element of the strategy involved **delegitimizing Western media and cultivating informational ambiguity** aimed at eroding the public’s ability to distinguish between truth and disinformation, ultimately leading to the demoralization of civilian populations regarding the credibility of information disseminated by official authorities.

Between 2014 and 2022, Russia continued to test and refine instruments associated with cognitive warfare. Among the measures employed were: (1) ***plausible deniability***, through which Russia rejected direct involvement in the Donbas conflict, attributing actions to *"volunteers"* or *"local forces";* (2) ***informational*** fog, created by the deliberate dissemination of contradictory versions of events; and (3) ***influence campaigns*** conducted in the West, used to test cognitive manipulation techniques later applied in the Ukrainian context. This period marked the transition from fragmented actions to a coherent strategy in which the cognitive component became essential to achieving the Russian Federation's geopolitical objectives.

### *The 2022 Invasion: Escalation of Cognitive Warfare*

Russia employed cognitive warfare instruments to facilitate the war in Ukraine, such that in the days preceding the invasion, President Putin and Russian-affiliated media outlets consistently disseminated reassuring messages asserting that Russia had no intention of invading Ukraine - while, in reality, final preparations were being made for Russian forces to cross the border and occupy large portions of Ukrainian territory (Burke, Henschkel, 2022).

Another example of a cognitive attack explored in the prelude to the conflict (NATO Cognitive Warfare, June 2025, p. 6) was the dissemination of the narrative concerning the *"13 biological laboratories in Ukraine"*, suggesting that the United States was transforming Ukraine into a testing ground for biological weapons with the approval of the Ukrainian president. The Kremlin strategically amplified this narrative through platforms such as RT, Telegram, and other social media networks, using manipulated documents and distorted information to target international audiences, particularly in regions where skepticism toward Western institutions already existed. According to the NATO document, the campaign was designed to exploit cognitive biases such as distrust toward U.S. foreign policy and fear of biological threats – heightened in the aftermath of the COVID-19 pandemic – with the ultimate aim of undermining trust in the United States and NATO, justifying Russian aggression as a defensive measure, and creating confusion regarding the true nature of the conflict. The intended effect was not physical, but psychological: shaping perceptions, redirecting blame, and weakening international resolve.

The outbreak of the conflict itself was framed by the Russian president under the label of a *"special military operation"*, justified as an act of *"denazification"* of Ukraine and later as *"a struggle for the future, for the freedom of countries and peoples"* (Putin, 2023). The intensive use of messaging centered on the term

"Nazism" expanded its meaning to such an extent that it was incorporated into the latest version of the Foreign Policy Concept of the Russian Federation (2023), alongside other key terms such as *"Western hegemony", "neo-colonialism", "the collective West"*, and *"Russophobia"* in legitimizing the evolution of the war in Ukraine.

The dissemination of propagandistic messages through media channels – both within Ukraine and in other states supporting the Ukrainian side – was conducted in parallel with Moscow's investments in building a transnational network of pro-Russian journalists and influencers. This effort involved training programs, media partnerships, and the transfer of ideological *"know-how"* (Center for Countering Disinformation, 2025). Ultimately, this process formed part of a broader strategy aimed at imposing Russian narratives globally, implemented through both traditional media channels and digital platforms, social networks, online influencers, and coordinated disinformation campaigns.

The manner in which Moscow employed technology to propagate disinformation represented a novel element in the conduct of modern conflicts. The use of bots (computer programs operated within bot farms that generate targeted content for or against specific topics), trolls (individuals using false identities to disseminate propagandistic content), and artificial intelligence (a field of computer science focused on creating systems capable of mimicking human intelligence) significantly amplified the impact of messages on citizens' cognitive processes. The terms *"bot"* and "troll" are often incorrectly used interchangeably, yet their modes of operation differ: bots can rapidly disseminate messages at scale, while trolls intervene strategically to stimulate conflict, manipulate conversations, and lend credibility to disinformation. Maximum effectiveness – also leveraged by the Kremlin – is achieved when these tools are combined, creating the illusion of authentic consensus and amplifying the impact of desired narratives.

Their use was evident from the early stages of the conflict, with Ukrainian special services identifying over one and a half million accounts across various social networks and messaging platforms (…) *"created to spread falsehoods and pro-Russian propaganda"* (Ministry of Internal Affairs of Ukraine, December 2022). Bot and troll networks remain a persistent method of shaping the conflict, despite multiple countermeasures undertaken by security services and social media platforms. Their impact on influencing mass behavior is considerable, given that most individuals are not accustomed to verifying the authenticity of information and that attribution is difficult to establish. Furthermore, their proliferation in the information environment has increased due to the exploitation of artificial intelligence, whose increasingly sophisticated outputs are difficult to challenge even by domain experts.

As noted by F. Bechis in Playing the Russian Disinformation Game (p. 125), social media platforms have fundamentally reconfigured propaganda campaigns previously employed, granting states the ability to target adversaries in ways that were previously inconceivable. These platforms enable access to vast audiences within informal settings, embedded directly in users' everyday environments, thereby increasing the effectiveness of transmitted messages. Moreover, campaigns conducted through social media are difficult to detect and counter, requiring significantly fewer financial resources than conventional methods of psychological or kinetic influence.

These characteristics prompted the Kremlin to allocate substantial resources to the development of a coherent and advanced digital disinformation strategy. Unlike many Western states, Russia stands out for the scale and depth of its influence programs, which integrally mobilize state, media, and technological resources in a concerted effort of cognitive influence and information manipulation.

The dissemination of Russia's own perspectives through various overt and covert means, combined with the exploitation of **existing social, economic, and political cleavages** within target states, has supported Moscow's objectives of undermining international solidarity with Ukraine and instilling among the Ukrainian public the belief that Russia plays the role of a victim vis-à-vis the West and that of a liberator of Ukraine.

## PERSPECTIVES

Although Russia has not fully achieved its objectives in Ukraine, the use of instruments specific to the cognitive component of warfare has intensified in recent years, and their effects are increasingly evident. Within the information environment, concerns have grown regarding potential innovations that Russia may adopt in the future. These concerns also extend to the expanding cooperation between Moscow and Beijing, with the latter being widely recognized for its significant technological advances.

Another aspect requiring further examination in the near future is media literacy as a means of enhancing cognitive resilience. The cognitive warfare conducted by Russia in Ukraine and other areas of interest should serve as a lesson learned for strengthening interinstitutional cooperation, while also engaging multiple audience groups as an integral part of total defense (Solvita, 2022). In an information environment saturated with increasingly sophisticated cognitive influence campaigns, the active promotion of media literacy is not merely an educational necessity, but a vital strategy for national security and regional stability. Consequently, encouraging sustained citizen engagement and education in this field represents a fundamental pillar in effectively responding to the challenges posed by the cognitive component of conflict.

Approaching the conflict in Ukraine from the perspective of cognitive warfare on a global scale also entails questioning the ethics of this type of conflict, as it influences people's thinking and decision-making without their awareness. In a context where the boundary between peace and war is becoming increasingly blurred, and confrontations are often conducted within the cognitive domain, the effects on civilian populations can be profound and long-lasting. For this reason, security specialists must be prepared not only to identify and counter such threats, but also to manage the increasingly complex ethical challenges raised by the evolving nature of contemporary conflicts (Rusu, 2025).

## CONCLUSIONS

The Russian Federation is widely recognized for its extensive experience in the field of information manipulation. While its official rhetoric has remained consistent – portraying Russia as a victim of Western actions while simultaneously maintaining expansionist ambitions – the country has become a relevant example of the transition from classical propaganda to the integration of modern technologies in shaping mass behavior.

The conflict in Ukraine has been accompanied by an unprecedented intensification of cognitive warfare conducted by the Russian Federation, directly targeting the manipulation of perceptions and the disruption of the cognitive coherence of both the Ukrainian population and the international public. Through a combination of official narratives, disinformation campaigns, the use of affiliated media channels, influencers, and automated networks (bots and trolls), Russia has promoted themes such as Ukraine as a failed state, the "Nazification" of Ukrainian society, the historical legitimacy of territorial annexation, and the attribution of blame to NATO and the West for the outbreak of the conflict.

Cognitive warfare has also expanded into European states, aiming to divide public opinion and weaken political support for Ukraine. As a result, the cognitive domain has become an essential battlefield in which Russia has invested strategic resources, anticipating that informational victory may precede or even substitute for military success.

Against the backdrop of the intensification Russia's cognitive warfare efforts, NATO and Western states have become increasingly concerned with developing defensive capabilities within the information environment. In this context, NATO has explicitly acknowledged in recent strategic documents the importance of protecting the *"cognitive space"* of its citizens. Moreover, media literacy campaigns are becoming essential for strengthening societal resilience, as Russian cognitive interventions can undermine democracy from within, even in the absence of a conventional conflict.

## BIBLIOGRAPHICAL REFERENCES:

1. Anuța, C. (2016). *Old and New in Hybrid Warfare. Countering Hybrid Threats: Lessons Learned from Ukraine*.
2. Bechis, F. (2020). *Playing the Russian Disinformation Game Information operations from Soviet tactics to Putin's sharp power.* Democracy and Fake News.
3. Claverie, B., Cluzel F. (2020). *The Cognitive Warfare Concept*.
4. Bouwmeester, H. (2017). *Lo and Behold: Let the Truth Be Told –Russian Deception Warfare in Crimea and Ukraine and the Return of 'Maskirovka' and 'Reflexive Control Theory'*, în *Netherlands Annual Review of Military Studies*.
5. Bugayova, N. (2025). *A Primer on Russian Cognitive Warfare*, Institute for the Study of War, https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/, retrieved on 23 September 2025.
6. Burke, P., Henschke, A. (2022). *I Know My Truth… Now Tell Me Yours: From Active Measures To Cognitive Warfare In The Russian Invasion Of Ukraine*. Strategic Panorama.
7. Center for Countering Disinformation (2025). *How Russia Spreads Its Propaganda Worldwide Under the Guise of Education,* https://cpd.gov.ua/en/international-threats-en/europe/how-russia-spreads-its-propaganda-worldwide-under-the-guise-of-education/, retrieved on 23 September 2025.
8. Chiriac, O. (2021). *Cognitive Warfare in the 21st Century Great Power Competition – Framing of Military Activity in the Black Sea*, *Romanian Military Thinking International Scientific Conference Proceedings,* 3rd III.
9. Chotikul, D. (1986). *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study*. Naval Postgraduate School.
10. Deppe, C., Schaal, G-S. (2024). *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept*, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full, retrieved on 22 August 2025.
11. Embassy of the Russian Federation in Romania (2023). *Vladimir Putin: "Operațiunea Militară Specială este o luptă pentru viitor, libertatea țărilor și a popoarelor"*, https://

romania.mid.ru/ro/press-centre/arkhiv_novostey/vladimit_putin_opera_iunea_militar_special_este_o_lupt_pentru_viitor_libertatea_rilor_i_a_popoarelor/, retrieved on 25 September 2025.

12. Galeotti, M. (2019). *Active Measures: Russia's Covert Geopolitical Operations*, https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0, retrieved on 23 September 2025.
13. Gherasimov, V. (2016). *The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operation*, în *Military Review*, The Professional Journal Of The U.S. Army.
14. Hofirek, M. (2021). *Messing with their Minds: Maskirovka's Cognitive Effects in Crimea and Donbas*.
15. Morelle, M. et al. (2023). *Towards a Definition of Cognitive Warfare. Conference on Artificial Intelligence for Defense*, p. 3.
16. NATO Cognitive Warfare Concept (2025). Version 1.3.
17. Normile, D. (2022). *China bets big on brain research with massive cash infusion and openness to monkey studies*, https://www.science.org/content/article/china-bets-big-brain-research-massive-cash-infusion-and-openness-monkey-studies, retrieved on 23 September 2025.
18. Pynnöniemi, K., Kari, M. (2016). *Russia's New Information Security Doctrine: Guarding a besieged cyber fortress*. Finnish Institute of International Affairs.
19. Rusu, A. (2025). *Military ethics in the light of Cognitive Warfare*. International Conference RCIC`25, p. 49.
20. Serviciul Român de Informații (2020). *Tehnici de propagandă rusă*. Centrul de Excelență OSINT.
21. Solvita, D-L. (2022). *With Media Literacy Towards Cognitive Resilience: Updates from the Baltic States, and lessons learned*.
22. *Teoria controlului reflexiv în logica războiului hibrid* (2017), https://intelligence.sri.ro/teoria-controlului-reflexiv-logica-razboiului-hibrid/, retrieved on 23 Septembre 2025.
23. *The Future of China's Cognitive Warfare: Lessons from the War in Ukraine* (2020), https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine, retrieved on 24 Septembre 2025.
24. The Ministry of Foreign Affairs of the Russian Federation (2016), *Foreign Policy Concept of the Russian Federation*, /efaidnbmnnnibpcajpcglclefindmkaj/https://www.russiamatters.org/sites/default/files/media/files/Foreign%20Policy%20Concept%20of%20the%20Russian%20Federation%20(approved%20by%20President%20of%20the%20Russian%20Federation%20Vladimir%20Putin%20-on%20November%2030,%202016)%20-%20Asset%20Publisher%20-%20The%20Ministry%20of%20Foreign%20Affairs%20of%20the%20Russian%20Federation.pdf, retrieved on 24 September 2025.

25. The Ministry of Foreign Affairs of the Russian Federation (2023), *Foreign Policy Concept of the Russian Federation*, https://www.mid.ru/en/foreign_policy/fundamental_documents/1860586/, retrieved on 24 September 2025.
26. Zimmer, P. (2013). *Maskirovka: The Hidden Key to Soviet Victory*, Warfare History Network, https://warfarehistorynetwork.com/article/maskirovka-the-hidden-key-to-soviet-victory/, retrieved on 23 September 2025.