

### National Defence Academy of Latvia Centre for Security and Strategic Research

# The Cognitive Battlefield: Exploring the Western and Russian Views





CSSR Paper no. 05/2023

# The Cognitive Battlefield: Exploring the Western and Russian Views

Dr. oec. Jānis Bērziņš

Senior Researcher at the Centre for Security and Strategic Research

National Defence Academy of Latvia Centre for Security and Strategic Research Ezermalas 8B LV-1014 Riga Latvia http://www.naa.mil.lv

© 2023 by Centre for Security and Strategic Research September 2023

The views expressed here are solely those of the author in his private capacity and do not in any way represent the views of the Latvian National Armed Forces, the Ministry of Defence of Latvia, or any other entity of the Latvian government.

#### About the Author

Dr. Berzins is a senior researcher and formerly served as the director of the Centre for Security and Strategic Research (CSSR) at the National Defence Academy of Latvia. He is also a non-resident researcher fellow and advisor at the Swedish Defence University, and a senior fellow at the Center for the Study of New Generation Warfare. His work primarily focuses on the intersection between the theoretical developments of Russian Military Thought and the operational realities on the ground. This encompasses both the hybrid and conventional aspects of warfare, including influence, information, and psychological operations. He has been a guest lecturer in various countries, including the United States, Sweden, Norway, the Netherlands, Singapore, Belgium, Brazil, Estonia, and Lithuania, at numerous academic and defense institutions. These institutions include the New York University, the Johns Hopkins University, the George C. Marshall Center European Center for Security Studies, the Swedish Defense University, the Swedish Defense Research Agency, the Norwegian Military Academy, the US Army's Asymmetric Warfare Group, NATO's Special Operations Command Europe, NATO/SHAPE Brunssum Headquarters, the Center for European Policy Analysis (CEPA), the Jamestown Foundation, the Atlantic Council, among others. Dr. Berzins has collaborated with various governmental bodies, including the United Kingdom House of Commons Defense Select Committee, the Parliament of Singapore, the Swedish Government, and the Polish Government. He has also offered his expertise to the Ministry of Defense of Singapore on matters related to Strategic Communications, influence, information, and psychological operations. Additionally, he has provided insights into Russia's doctrine to the US Department of Defense and offered strategic guidance on Russia's issues to the private sector.

## The Cognitive Battlefield: Exploring the Western and Russian Views

Dr. oec. Jānis Bērziņš

National Defence Academy of Latvia's Centre for Security and Strategic Research Email: Janis.Berzins01@mil.lv

#### Abstract

This paper explores the concept of cognitive warfare, a multifaceted approach to achieving strategic objectives by manipulating the cognitive mechanisms of adversaries. Drawing on historical examples and contemporary developments, it delves into the increasing focus on the "hearts and minds" aspect of modern conflict. The analysis encompasses two principal components of cognitive warfare as presented in Russian military literature: Reflexive Control and Mental Warfare. While Reflexive Control has been previously discussed in Western literature, Mental Warfare is a recent and lesser-known concept. The paper examines the theoretical and philosophical foundations underlying these components, highlighting their shared emphasis on the cognitive process. Mental Warfare, as an integral part of the strategy of Controlled Chaos, seeks to occupy the adversary's consciousness and induce changes in collective mindsets, while Reflexive Control aims to influence opponents through tailored information. The implications of cognitive warfare for NATO and Western countries are also discussed, emphasizing the importance of proactive measures and enhanced cognitive defense in countering adversarial attempts to exploit systemic vulnerabilities. Ultimately, the paper underscores the critical need to protect the human mind, which has become the primary battleground in the pursuit of political objectives in contemporary warfare.

#### 1 Introduction

Information, psychological, and influence operations have been employed during both peace and conflict periods to achieve objectives at multiple strategic levels. While there are arguments suggesting that the French military was the first to engage in information operations during the First World War through the interception of radio and telephone communications (Bailey, 2001), Sun Tzu had already discussed the importance of comparing the unity and morale of the home front and army with that of the enemy (Sun Tzu & von Clausewitz, 2000). Additionally, Frederick the Great, known for his impressive intelligence system, utilized deception to mislead opponents about his forces' capabilities and intentions, strategically targeting their informational and cognitive processes (Duffy, 1974).

The technological advancements of the past 50 years, particularly in information and communication technologies, have made it possible to employ well-established methods of warfare in innovative ways. As warfare's primary objective is political, with military instruments serving as a means to that end, the struggle for "hearts and minds" has become a crucial aspect of contemporary warfare. This holds significant implications for the West, given the high credibility of NATO's military deterrent. Rather than relying solely on conventional military instruments, adversaries have increasingly focused on

<sup>&</sup>lt;sup>1</sup>The author does not intend to propose a new buzzword. Contemporary warfare should be understood as the way in which warfare is being conducted at the present moment.

exploiting the West's systemic vulnerabilities to achieve political victories by gaining control over the cognitive processes of adversaries, influencing perceptions, behavior, and decision-making at both individual and collective levels. In essence, the human brain has become the battlefield, and society, as a whole, serves as the primary target.

While NATO, its members, and allies have been developing their understanding of the meaning and implications of cognitive warfare, the Russian military literature presents a distinct body of analysis on similar phenomena. The Western approach to cognitive warfare does not differentiate between levels of effect. In other words, cognitive warfare may refer to operations targeting individuals, groups, or the entire society. Conversely, the Russian military literature divides the cognitive factor in warfare between Reflexive Control and, more recently, Mental Warfare.

Reflexive Control, extensively discussed in Western literature, primarily concentrates on the manipulation of cognitive processes within individuals or groups by inducing shifts in their perceptions of reality. In contrast, Mental Warfare seeks to reshape the cognitive processes of individuals and social collectives, with the aim of altering their social consciousness. This is achieved through the undermining of spiritual and moral values, traditions, and the cultural and historical foundations of the state (Ilnitsky, 2022).

Consequently, this paper's objective is to conduct an analysis of the contemporary advancements in cognitive warfare within both Western and Russian contexts, with a particular focus on identifying the central theoretical and conceptual underpinnings, prevailing trends, and the instrumentalities employed. Given that this field is still evolving, it prompts more questions rather than providing definitive answers. Therefore, this paper serves as an introductory exploration into the ongoing discourse surrounding cognitive warfare in the West and in Russia. The first section offers insights into the Western perspective, while the subsequent section delves into Russian developments, followed by conclusions.

#### 2 Cognitive Warfare in the West

The term "Cognitive Warfare" has been employed in the United States since 2017 to describe the specific modes of action that a state or influential group may employ to manipulate the cognitive mechanisms of an enemy or its population. The objective of cognitive warfare is to weaken, infiltrate, influence, and potentially subjugate or destroy the target entity. (Stuart, 2017). Cognitive warfare integrates the various components of information warfare, combining psychological operations and influence operations targeting intangible assets with cyber operations aimed at disrupting or damaging physical information systems.

According to Claverie and du Cluzel (2022) cognitive warfare strategies typically encompass the deliberate manipulation of reality through the presentation of biased information, often digitally altered, with the aim of advancing one's own interests. The advent of new communication tools has exponentially expanded the range of possibilities, giving rise to novel methods and objectives within this domain. However, this increased complexity underscores the importance of potential targets adopting a continuous stance of resilience, since victims may only become aware of the attacks after they have already occurred. This emphasizes the need for proactive measures for effectively countering cognitive warfare threats.

As illustrated in Figure 1, Cognitive Warfare occupies a pivotal position where two traditionally separate operational domains intersect: Psychological Operations (PSY-OPS) and influence operations, often linked with the concept of soft power on one side, and cyber operations, primarily geared toward the defense and disruption of physical information assets, on the other. While its technical aspects, particularly those involving cyber capabilities, diverge from conventional Psychological Operations, Cognitive Warfare can be seen as a complementary endeavor, characterized by shared goals and strategies within the realm of psychological influence (Claverie & du Cluzel, 2022). Consequently, the principal objective of Cognitive Warfare transcends being merely an adjunct to strategic planning or the achievement of victory without direct confrontation. Instead, it involves engaging in a profound conflict that addresses the thoughts, affiliations, and convictions of adversarial communities, ultimately reshaping their perceptions of reality (Claverie & du Cluzel, 2022).

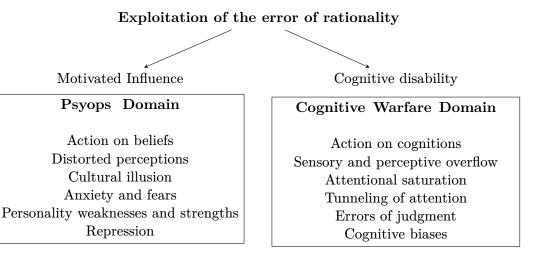


Figure 1: Differences Between Cognitive Warfare and PSYOPS (Including, in Broad Terms, Actual Psychological Operations and Other Non-Kinetic Actions such as Influence Operations and Civil-Military Cooperation). Adapted from Claverie and du Cluzel (2022).

Cognitive warfare goes beyond being a mere supplementary strategy or a means to achieve victory without physical combat. Its fundamental goal is to wage war on an adversary community's core beliefs, values, and sentiments by manipulating their perception of reality. This type of warfare specifically targets the thought processes, cognitive frameworks, and overall worldview of the enemy, influencing how they perceive the world and formulate their conceptual thinking. The intended effects of cognitive warfare include the alteration of worldviews, which can disrupt the adversary's peace of mind, undermine their certainties, reduce their competitiveness, and hinder their prosperity (Claverie & du Cluzel, 2022).

In essence, cognitive warfare is a form of conflict that employs information, technology, and psychological operations to sway the perceptions, beliefs, and decision-making of adversaries. Its ultimate objective is to interfere in the process of reality construction to undermine mental self-confidence, trust in processes, and the mechanisms crucial for the smooth functioning of groups, societies, and even nations (Claverie & du Cluzel, 2022). Thus, the objective of cognitive warfare is to disrupt or exploit an opponent's decision-making abilities, manipulate their perceptions, and ultimately gain a strategic advantage. It can include psychological operations like propaganda or disinformation, cyber-attacks, and spreading false information through digital communication. Both

state and non-state actors can engage in cognitive warfare and it can have significant impacts on the decision-making abilities of opponents.

Cognitive warfare integrates new technologies with human factors and systems, including Artificial Intelligence (AI), Machine Learning (ML), Information Communication Technologies (ICT), neuroscience, biotechnology, and processes of human enhancement. This integration poses a high risk to security as a broad concept, encompassing economic, social, and cultural issues (Masakowski et al., 2020). Consequently, the domains of warfare have expanded from the traditional three (land, sea and air) to the six currently recognized by NATO (land, air, sea, space, cyber and cognition) (Guyader, 2022).

The preceding discussion should not be misconstrued as NATO or any European Union country preparing to engage other actors with the instruments of cognitive warfare. On the contrary, the aim is to gain a better understanding of cognitive warfare and its instruments for self-defense purposes. There have been instances of malign actors employing cognitive warfare against the West. Clear examples of this can be seen in Russia's meddling in American elections, spreading disinformation to discredit the media, public institutions, politicians, and civil servants, as can be observed with false claims about COVID-19 vaccines, climate change, 5G technology, among others.

Russian analysts are acutely attentive to the recent developments in cognitive warfare in the Western world. A recent article featured in the academic journal of the Russian General Staff, *Voennaia mysl'*, asserted with a discernible sense of apprehension, that Western governments are placing significant emphasis on the advancement of cutting-edge cognitive technologies. These technologies empower them to exercise influence over the cognitive realm of individuals, social collectives, and the entire state apparatus. This capacity forms the bedrock upon which developed nations across the globe base their pursuit of comprehensive cognitive warfare strategies for accomplishing their geopolitical objectives (Zhdanov et al., 2023).

#### 3 Cognition in Russian Warfare

The Russian approach to cognitive warfare diverges from the understanding utilized in Western contexts. Instead, it delineates two fundamental components, contingent upon the source of the action. When the source originates from Russia, it is termed "Reflexive Control," whereas when the source is from the West, it is referred to as "Mental Warfare." Although "Reflexive Control" has been extensively discussed in Western literature, the concept of "Mental Warfare" is comparatively recent and warrants further analysis and discussion. Thus, this paper will focus primarily on the principles of "Mental Warfare." Both concepts share a common theoretical and philosophical framework, linking them with cognitive processes. Furthermore, "Mental Warfare" also shares the principle of "reflectiveness" with "Reflexive Control."

The most important theoretical concept underlying the reflexive process is Marxist dialectics. Marx inverted Hegelian dialectical logic, which posited that the human mind determines the material world. In contrast, Marx argued that the material world, particularly the way humans produce their means of subsistence, shapes their social, political, and cultural structures. Consequently, cognition emerges from the reflection of the material world in the human mind, influencing social consciousness. As such, intelligence

and cognitive processes become dependent on an individual's sensory awareness of the external world, thereby determining the content and dimensions of their consciousness.

Thus, Reflexive Control entails the technique of providing the opponent (controlled) with specialized enemy information to induce them to voluntarily undertake a predetermined action desired by the controller. This can occur through altering the enemy's information processing (cognitive) or selectively disseminating messages (informational). It can further be categorized into constructive reflexive control when the opponent is influenced to voluntarily make decisions favorable to the controller, and destructive reflexive control when the objective is to disrupt, paralyze, or neutralize the opponent's decision-making processes and algorithms. This manipulation leverages moral, psychological, and other factors, including the personal characteristics of the opponent, exploiting psychological vulnerabilities in deception operations.

Instead of viewing conflict as a mere interaction between two military forces, it is essential to consider conflict as a dynamic occurring within the decision-making processes of the opposing parties. Each adversary's choices are shaped by their perception of both themselves and their opponent, resulting in a reflective interaction between the two. Reflexive Control encompasses a process in which one side presents reasoning or information to the enemy, leading them to logically infer and ultimately make a decision predetermined by the initiating party. A more contemporary definition describes it as a method of conveying specially prepared information to a partner or opponent, with the aim of influencing them to voluntarily make a decision desired by the initiator of the action. The primary instruments employed in Reflexive Control are (Komov, 1997):

- Exhaustion: This tactic aims to compel the enemy to undertake unwise or futile actions, depleting their resources and reducing combat readiness. It may involve limited combat or diversionary operations.
- Decoy: This strategy involves information counteraction to expose the enemy to a perceived threat in vulnerable areas (rear, flanks, etc.) that does not require special countermeasures. Its purpose is to divert the enemy's attention from the real threat and lull their vigilance.
- Disintegration: Primarily a diplomatic weapon, this tactic employs information counteraction to instill the idea of acting against the coalition's interests in the enemy's minds. It can include misleading public opinion or implanting false notions about the military-political situation among the involved states' leaders. Additionally, it may encompass actions to create tension within the enemy country or exacerbate existing contradictions, weakening their military and economic strength.
- Appeasement: It is used to persuade the enemy that their opponent holds neutral or friendly intentions. It involves measures of information counteraction that create an impression of routine combat training rather than preparations for hostilities. The aim is to convince the enemy that the opponent is peaceful and non-threatening, leading them to lower their guard. Any planned attack is kept under deep secrecy.
- Intimidation: The aim is to inform the enemy of their opponent's real or imagined superiority.
- Provocation: The objective is to induce the enemy to take actions that the opposing side can exploit to their advantage.

- Overload: It requires inundating the enemy with a vast amount of information during preparations and hostilities. This strains their command system and forces them to make decisions in an uncertain and confusing situation.
- Suggestion: This tactic involves shaping and exploiting the opposing side's behavioral patterns. During the preparatory stage, the enemy is provided with information of a legal, moral, ideological, or other nature that might prompt them to act in favor of their opponents.
- Distraction and paralysis: It creates a real or imaginary threat against one of the most vital places for the enemy, such as the flanks and rear, during the preparatory stages of combat operations. It forces them to reevaluate their decisions about the axis on which to operate.

Although one might be skeptical about Reflexive Control, its distinct advantage is that it forces the potential user to develop a mindset in which understanding the enemy, thinking through moves and countermoves, and attempting to develop a rigorous methodological approach to analyzing strategic problems and making optimal decisions are of utmost importance. Therefore, Reflexive Control aims to alter the subject's perceptions of the material world to affect social consciousness and change their cognitive process. Reflexive control can be understood as a strategy used to influence a partner or opponent by providing them with carefully tailored information, leading them to voluntarily make a decision that aligns with the initiator's desired outcome. Therefore, it is one of the main instruments employed by Russia to affect cognition, aiming to influence the opponent's process of decision-making. It has many similarities with NATO's previously discussed concept of Cognitive Warfare.

The concept of Mental Warfare is primarily linked to the Russian belief that they are facing a civilizational war initiated by the West by means of color revolutions to achieve a state of what is called *Controlled Chaos* in the Russian military literature. According to Zhdanov et al. (2023), Russia's pursuit of safeguarding its national interests has transformed into a civilizational confrontation, manifesting itself as a hybrid war against the entire Western world, which encompasses not only the existence of the country as a sovereign state, but also the preservation of the entire Russian civilization. In this sense, it is the development of a previous discussion, which already started around the beginning of the 2010s, when A. A. Bartosh, I. N. Vorobyov, V. A. Kiselyov, S. G. Chekinov, S. A. Bogdanov, and other Russian military scholars began to develop the discussions about what became known in the Russian military literature as *Voyna novogo pokoleniya* or New Generation Warfare. In this sense, Mental Warfare is one of the main components of the strategy of Controlled Chaos, which is part of New Generation Warfare.

Controlled Chaos represents a geopolitical model aimed at causing destruction in a targeted victim state, selected by another country (the customer country). This "destruction" entails a series of measures designed to neutralize the victim state's geopolitical advantages, including its territorial size, total population, international standing, economic potential, military strength, and overall capabilities by creating an artificial crisis (Serzhantov et al., 2022). It is also closely related to the Russian concept of Hybrid Warfare (gibridnaya voyna), which is defined as the coordinated use, by the aggressor country, of numerous types (tools) of violence aimed at exploiting the vulnerabilities

of the target country, covering the full range of social functions, to achieve a synergistic effect and subordinate the enemy to its will (Bartosh, 2022). In this context, the seizure of territory is supplanted by the overthrow of objectionable governments and the empowerment of loyal political forces, thereby depriving the target of sovereignty and placing it under external control.

As articulated by Vorobyov and Kiselyov (2014), the Russians are convinced that the West is employing a subversive ideological weapon known as Westernization, which involves imposing a social system, economics, ideology, culture, and way of life similar to those in Western countries, on Russia (or other countries). This strategy seeks to discredit the existing social system in Russia, sow division among the population, and to garner support for opposition movements. Essentially, this refers to Color Revolutions, which the Russians firmly believe to be the primary instrument utilized by the West in their pursuit of Hybrid Warfare.

From the Russian perspective, Hybrid Warfare remains an exclusive tool utilized by the West and is foreign to Russian military doctrine. According to the Russian literature, the process of Hybrid Warfare unfolds in three stages (Vorobyov & Kiselyov, 2014): the first stage involves instigating crises, promoting destabilization, and fostering internal conflicts within the victim state; the second stage centers on causing degradation, impoverishment, and ultimately pushing the victim state towards disintegration, effectively transforming it into what is commonly referred to as a "failed state"; finally, the West portrays itself as a benevolent savior, intervening in the situation and facilitating a change in political power. If necessary, the U.S. Armed Forces stand ready to execute an invasion, followed by a so-called "stabilization" operation. The main instruments used in Hybrid Warfare are (Karavaev, 2022):

- Aggressive actions (attacks) commence without declaration. They possess an evolutionary, permanent nature, occur in gray zones, and often result in the defeat of the victim state due to its inability to effectively counter them.
- The defeated nation-states are dismantled, often without their territory being occupied, or they lose not only their population and resources but also their political will and self-governance opportunities.
- The population of the victim state often finds itself administered by external and internal entities, losing the ability to influence its own fate. A battle is waged for minds, knowledge, and will, shaping the world outlook of individuals and society at large.
- The national history, culture, traditions, way of life, and priorities of the population are ignored and replaced with different ones imposed from outside, often with the tacit acquiescence of the local population.
- Victory is deemed absolute when the spiritual space and public consciousness have been occupied, leading the vanquished not only to lose the ability to defend their values but also to fully assimilate the alien, false guidelines imposed by the victorious adversary.
- Blitzkrieg in this war involves paralyzing the adversary's will by targeting its elite and media, subsequently dismantling state institutions and disintegrating the army, military, and security agencies from within.

• Attacks against the victim country are not only conducted from the outside but also from the inside, marking a fundamental distinction from traditional "from the outside - in" methods of warfare. As a result, the fronts and battles of this war vary in scale but are synchronized and systemic.

The role of Mental Warfare in this process is to defeat social consciousness by the use of a system of methods and means of influence with a strategic combination of activities and operations of different scale with the objective of "occupying" the adversary's consciousness, leading to the paralysis of its will and inducing changes in the individual and collective mindset of the population (Karavaev, 2022). Hence, mental warfare is defined as the "coordinated sum of variously scaled activities and operations aimed at "occupying" the consciousness of the adversary. This is done to paralyze its will and change the individual and mass consciousness of the population, to demoralize the army and society, to destroy its spiritual and moral values, traditions, and the cultural and historical foundations of the state and erase the national identity of the people (Ilnitsky, 2022). It has seven main tenets:

- Informational: Complex impact on the state and military command system and control of the opposing side, which leads to the adoption of the required decisions and paralyzes the functioning of infrastructure management.
- Psychological: Implies the deliberate use of propaganda and other means (diplomatic, military, economic, etc.) for direct or indirect influence on opinions, moods, feelings of the enemy and, as a result, on its behavior and cultural installations.
- Cybernetic: Aimed at undermining information security and disrupting the functioning of computer systems, data theft, covert surveillance and search compromising evidence.
- Political: Based on creating the conditions for political isolation with all the ensuing consequences;
- Economic: The creation of artificial trade barriers and restrictions, introduction of a moratorium on investment assets.
- Financial: The closure of capital markets making borrowing, financial services, intermediation and settlement impossible.
- Hybrid: Using a combination of covert operations, sabotage and cyber warfare, as well as providing support to insurgents operating in enemy territory.

The targets are the mentality, identity, historical traditions, and values of the opposing side, both in peacetime and during military conflict. Its goal is the destruction or transformation of the object of influence: the destruction of public consciousness, public institutions, the state, the Armed Forces and others. The main forms of Mental Warfare include multi-way information operations, during which specific information operations are used to influence human consciousness (attitudes, infection, imitation, persuasion, influence, suppression and suggestion) targeting the following areas (Ilnitsky, 2022). The following techniques are used in Mental Warfare (Karavaev, 2022):

Concealment of critical information about the situation in various areas of society.

- Immersion of valuable information in an array of "information garbage" in accordance with the principle of "hiding a sheet in the forest."
- Substitution of concepts or distortion of their meaning.
- Distraction of attention to insignificant events.
- The application of concepts constantly used in the media space, the meaning of which has undergone qualitative changes.
- Presentation to the audience of negative information that is perceived better than positive news.
- Discussion of events of no real social value and the use of the results of incorrectly conducted sociological research to create a distorted picture of the situation in society.
- Introduction of prohibitions on certain types of information and news sections in order to prevent broad public discussion of issues and topics critical to certain power structures.
- Outright lies in order to misinform the population about their country and the foreign public.

In this case, the operational focus is on gaining control over an adversary's cognitive processes to influence perceptions, behavior, and decision-making at an individual or collective level. The objective is to align the population of the country/ies under attack with the attacker's political, social, economic, and military/tactical objectives. This is achieved by employing social engineering tools and techniques aimed at confusing the political debate and paralyzing the process of decision-making. The technological development of the last thirty years and the growth of the internet and the importance of networks and cyber assets have increased opportunities for altering and filtering the flow of information. As the target is the process of transforming information into knowledge, information has become a weapon (Ilnitsky, 2022), and society, therefore, has becomes a fair target in warfare.

#### 4 Conclusion

The enduring principles articulated by Clausewitz emphasize that warfare, at the grand strategic level, revolves around political objectives. The advent of new technologies has ushered in novel forms of engagement, encompassing both kinetic and non-kinetic approaches. These multifaceted strategies are tailored to elicit transformative changes in the cognitive processes of individuals and collectives, with the ultimate goal of achieving strategic objectives, traditionally pursued through kinetic means, but now accomplished through non-kinetic instruments. In recent years, this has led to the prominence of the concept of cognitive warfare, which aims to manipulate the cognitive mechanisms of enemies or populations to weaken, influence, or subjugate the target entity. This form of warfare employs psychological operations, influence operations, and cyber-attacks to alter the perceptions, beliefs, and decision-making processes of adversaries. In this context, NATO and Western countries have been grappling with the complexities of

cognitive warfare and the challenges posed by adversaries exploiting systemic vulnerabilities. Moreover, the order of battle has shifted from physical, emotional, and intellectual aspects in the past, to an emphasis on intellectual, emotional, and physical factors nowadays.

In comparison to the current Western approach, the Russian military literature presents a more nuanced and distinctive viewpoint, introducing two principal components: Reflexive Control and Mental Warfare. While the concept of Reflexive Control has received attention in Western literature, the notion of Mental Warfare is a more recent addition. Both Reflexive Control and Mental Warfare share a theoretical and philosophical foundation centered around the cognitive process. While Reflexive Control aims to influence an opponent by providing them with tailored information, Mental Warfare targets the mentality, identity, historical traditions, and values of the opposing side.

Notably, Mental Warfare serves as an integral part of the context of Controlled Chaos and color revolutions. According to the Russian literature, the objective of Mental Warfare is to occupy the adversary's consciousness, paralyze their will, and induce changes in the individual and collective mindset of the population. It seeks to destroy or transform social consciousness, public institutions, the state, the armed forces, and other critical aspects of the target country. Employing a combination of multi-way information operations, Mental Warfare utilizes specific techniques to influence human consciousness, including attitudes, infection, persuasion, and suppression. It is important to note that Russia considers Mental Warfare as an instrument employed by the West against unaligned countries, including Russia itself.

In this sense, Russia positions itself as a victim of a civilizational war instigated by the West. Rather than acknowledging its own potential deficiencies, Russia attributes the appeal of Western values and political, social, and economic models to external manipulation, unwilling to accept that its own elite's values and policies may lead to idiosyncratic vulnerabilities and challenges. As a consequence, it seems more convenient for Russia to place blame on external actors, such as the West, rather than introspectively addressing its own shortcomings and seeking to develop more attractive alternatives.

Simultaneously, Russia employs the same tactics that they believe the West is using against them, targeting the West itself in what can also be called a "civilizational war". Their aim is to exploit the West's own systemic fragilities with the objective of overthrowing objectionable governments and bringing loyal political forces to power instead of seizing territory. As such, since the objective is political, they exploit gaps between society and political, governmental, economic, military, and other institutions. Thus, the narratives are not pro-Russia but rather anti-West, anti-systemic, pro-populist, and aimed at a broader social spectrum.

Although cognitive warfare does not replace kinetic warfare, the West must remain vigilant in countering it, as adversaries continue to employ innovative and sophisticated methods to achieve their political objectives. By investing in proactive measures, including enhanced resilience, information security, and cognitive defense, NATO and its member states can better safeguard their societies and uphold democratic values in the face of evolving threats. Politicians, civil servants, and other stakeholders must also understand that their actions influence the level of confidence in the State. The lower the level of confidence, the higher is the chance of cognitive operations being successful.

#### References

- Bailey, J. (2001). The first world war and the birth of modern warfare. In W. Murray & M. Knox (Eds.), *The dynamics of military revolution* 1300–2050 (pp. 132–154). Cambridge University Press.
- Bartosh, A. A. (2022). Vzaimodeystviye v gibridnoy voyne [Interaction in hybrid war]. *Voennaia mysl'*, (4), 6–23.
- Claverie, B., & du Cluzel, F. (2022). Cognitive warfare: The advent of the concept of "cognitics" in the field of warfare. In B. Claverie, B. Prébot, N. Buchler, & F. du Cluzel (Eds.), Cognitive warfare: The future of cognitive dominance. NATO STO CSO.
- Duffy, C. (1974). The army of Frederick the Great. Hippocrene Books.
- Guyader, H. L. (2022). Cognitive domain: A sixth domain of operations? In B. Claverie, B. Prébot, N. Buchler, & F. du Cluzel (Eds.), Cognitive warfare: The future of cognitive dominance (pp. 3-1 3-5). NATO STO CSO.
- Ilnitsky, A. M. (2022). Strategiya mental'noy bezopasnosti rossii [Russia's mental security strategy]. *Voennaia mysl'*, (4), 24–35.
- Karavaev, I. N. (2022). Kontseptsiya mental'noy voyny kak sostavnaya chast' ucheniya o voynye i armii [The concept of mental warfare as an integral part of the doctrine of war and the army]. *Voennaia mysl'*, (3), 35–42.
- Komov, S. (1997). O sposobakh i formakh vedeniya informatsionnoy bor'by [On the methods and forms of information warfare]. *Voennaia mysl'*, (4), 18–22.
- Masakowski, Y. R., Blatny, J. M., Knox, B., Lauder, M. A., Sivertsen, E. G., & Grigsby, C. C. (2020). Executive summary. In *Mitigating and responding to cognitive war-fare*. STO-TR-HFM-ET-356, NATO STO HFM Panel.
- Serzhantov, A. V., Smolovy, A. V., & Terentyev, I. A. (2022). Transformatsiya soderzhaniya voyny: Kontury voennykh konfliktov budushchego [Transformation of the content of war: Outlining military conflicts of the future]. *Voennaia mysl'*, (6), 19–30.
- Stuart, V. R. (2017). Lt. Gen. Vincent Stewart's remarks at the Department of Defense Intelligence Information System 2017 Worldwide Conference. https://www.youtube.com/watch?v=Nm-lVjRjLD4.
- Sun Tzu & von Clausewitz, C. (2000). The book of war: Includes The Art of War by Sun Tzu and On War by Carl von Clausewitz. Random House Publishing Group.
- Vorobyov, I. N., & Kiselyov, V. A. (2014). Strategii sokrusheniya i izmora v novom oblike [Strategies of destruction and attrition: A new version]. *Voennaia mysl'*, (3), 45–57.
- Zhdanov, M., Sidorov, M., & Lukashin, A. (2023). Rol' natsional'nogo samosoznaniya v dostizhenii prevoskhodstva nad zapadom v usloviyakh kognitivnoy voyny [The role of national identity in achieving superiority over the west in terms of cognitive war]. Voennaia mysl', (6).

## CSSR Paper 05/23 September 2023

The views expressed here are solely those of the author in his private capacity and do not in any way represent the views of the Latvian National Armed Forces, the Ministry of Defence of Latvia, or any other entity of the Latvian government.

The Centre for Security and Strategic Research (CSSR) is a scientific institute at the National Defence Academy of Latvia (NDA). Its aim is to support the NDA's scientific activities, promote the development of military science in Latvia, and carry out research projects in line with Latvia's security and defence priorities. CSSR conducts research for the needs of the defence industry, participates in national and international research, provides consultations and support to defence sector organisations, organises conferences, seminars, and lectures, publishes research results and informative materials, participates in public discussions on important issues related to Latvia's security and defence, and contributes to the development and implementation of NAA study programmes.

National Defence Academy of Latvia Centre for Security and Strategic Research

Ezermalas 8B LV-1014 Riga Latvia http://www.naa.mil.lv