The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 3 (2024)

DOI: 10.62524/msj.2024.2.3.08

Cognitive Warfare in the Modern Architecture of Hybrid Warfare

Nataliia Semeniuk
Chief of Section
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh syl avenue, 28 B, Kyiv, Ukraine
e-mail: nataliia.semeniuk@gmail.com
ORCID: 0000-0001-5795-0021

Abstract. The experience of the Russian and Ukrainian war has proved that approaches to warfare have changed from purely conventional to hybrid wars with conventional actions and the inclusion of new elements. Mostly, combat operations are conducted simultaneously in all dimensions, which led to the coining of the term "operations in a multi-domain environment". Currently, the physical dimensions (space, air, sea and land) are intertwined with the virtual (cyber and information), which depend on the social conditions of individuals, their moral principles and cognitive perception. Dominance on the battlefield requires rapid adaptation to new realities and transformation of approaches to conducting operations in a multi-domain environment. In addition, the cognitive domain is a subsystem of new generation network-centric warfare in the modern architecture of hybrid warfare. A clear understanding of the interaction of elements of the modern architecture of hybrid warfare, their coordination and synchronisation during operations in a multi-domain environment will allow us to adapt to new armed conflicts and win them.

The author considers the current trends in the conduct of various types of warfare, takes into account best practices and presents the modern architecture of hybrid warfare. The author proposes a procedure for gaining a cognitive superiority.

The results of the proposed algorithm should be the introduction of a unified system of response to the challenges of modern hybrid warfare, including in the cognitive domain, at the state level.

Keywords: hybrid warfare, cognitive warfare, operations in a multi-domain environment, asymmetric warfare, network-centric warfare, conventional warfare, unconventional warfare, cyber warfare, cognitive superiority, cognitive domain.

Introduction

The experience of the Russian and Ukrainian war has proved that approaches to warfare have changed from purely conventional to hybrid wars with conventional actions and the inclusion of new elements [1-4]. Mostly, combat operations are conducted simultaneously in all operational areas (domains), which led to the introduction of the term "operations in a multi-domain environment" [5-6]. Currently, the domains (physical dimensions) (space, air, sea and land) are intertwined with the virtual (cyber and information) [1, 7], which in turn depend on the social conditions of individuals, their moral principles and cognitive perception [8-9]. Dominance on the battlefield requires rapid adaptation to new realities and transformation of approaches to conducting operations in a multi-domain environment. In addition, the cognitive sphere is a subsystem of new generation network-centric warfare in the modern architecture of hybrid warfare (Fig. 1).

A clear understanding of the interaction of the elements of the modern hybrid warfare architecture (see Fig. 1), their coordination and synchronisation in conducting operations in a multi-domain environment will allow us to adapt to new modern conflicts and win them.

Methodological Framework

Representing a paradigm shift for NATO, operations in a multi-domain environment integrate military activities across all operational domains. They encourage cooperation between military and non-military actors, stakeholders and subject matter experts, providing robust information sharing mechanisms, synchronisation of capabilities [10] that can reduce military risks and increase the likelihood of mission success, and enable Alliance decision-makers to achieve the desired results at the right time and place. This transformational approach aims to provide tailored options for action, strategically influencing adversary behaviour while protecting the freedom and security of NATO member states' populations in a fast-moving, volatile security environment.

The relevance of the study is to identify the methods and strategies used to influence people's perceptions and decisions to achieve goals in hybrid warfare. This may include information warfare, cyber and psychological operations, propaganda and other tactics [11] aimed at manipulating people's thoughts and behaviour.

An example of such warfare is the Russian and Ukrainian war, where Russia achieved its goals at the first stage through a combination of "unidentified" special forces, local armed groups, economic influence, disinformation and the use of socio-political polarisation in Ukraine, exerting cognitive influence.

The cognitive domain of network-centric warfare in the modern architecture of hybrid warfare (see Fig. 1) plays a key role that can be used both separately and as a combination with cyber, psychological and information means to achieve its goals [12].

From the point of view of psychology and pedagogy, the cognitive domain is defined as the area of human psychology associated with the cognitive process and consciousness, which includes human knowledge about the world and oneself.

Cognitive, which comes from the word "cognition", is a mental action or process of understanding that covers all aspects of the intellectual function, including subconscious and emotional aspects that guide most human decisions [13]. War, as the "experience" of war, originally referred to the general actions and characteristics of armed conflict between states, governments or organisations. In the modern dimension, there is less clarity about stakeholders, as varying degrees of organisational, cultural and social involvement are becoming more commonplace, as is the indirect extension of national interests.

Used together, these two words define cognitive warfare: activities carried out in sync with other instruments of power to change attitudes and behaviour by influencing, protecting and/or destroying individual and group cognition to gain advantage. These actions vary greatly and may involve supporting or conflicting cultural or personal components – social psychology, strategy and ethics are all contributing factors. However, the measures of modern warfare do not necessarily include a conventional component or directly tangible results such as the acquisition of territory or resources – as with other hybrid threats, adversaries wage cognitive warfare throughout the duration of the conflict and seek to remain in the "grey zone" below the threshold of armed confrontation.

In a recent example, Russia launched a military invasion of Ukraine, backed by unconventional (non-lethal) measures such as targeted propaganda, disinformation campaigns and support from its partners. Some of these unconventional (non-lethal) measures of cognitive warfare are obvious and direct: consumers of Russian disinformation experience a deterioration in their ability to distinguish fact from fiction, which reduces their mental resilience and can have long-term consequences, such as a loss of trust in the media.

Other examples are less obvious: China uses official and party influence to manipulate and control the domestic information environment, leading to the development of cognitive biases. The secondary effect is that citizens of other countries also develop cognitive biases against mainland Chinese citizens and their collective disconnection from external information, leading to two fundamentally opposite perceptions of reality. This form of "us versus them" polarisation can lead to increasing marginalisation and isolation of the population, as well as emotional exploitation, which fuels China's cognitive warfare strategy.

Cognitive superiority refers to actions: turning awareness and understanding of the situation into an actual advantage over the enemy in decision-making.

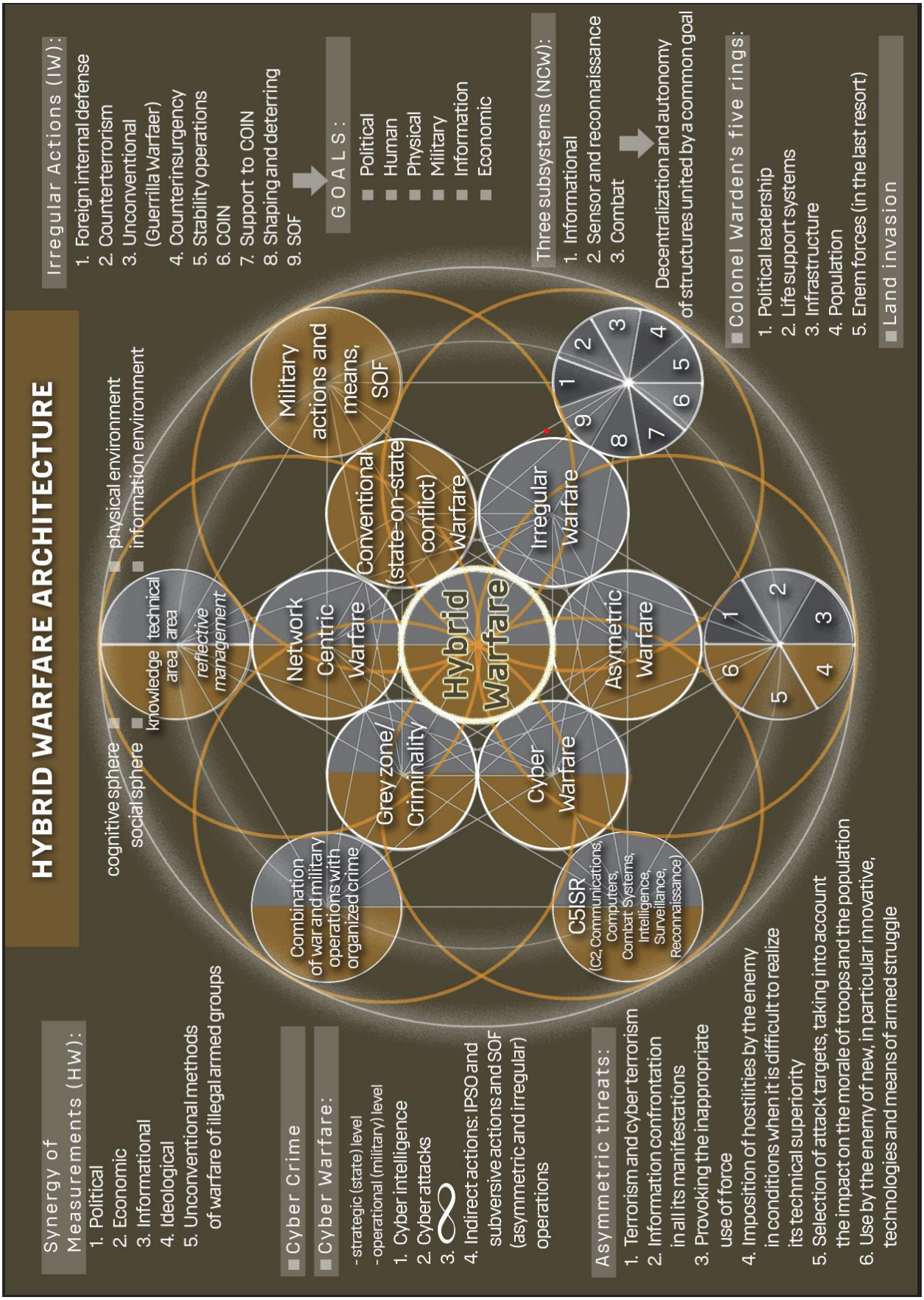

Figure 1. Modern architecture of hybrid warfare

Thus, the target audience against which cognitive influence is exerted includes both citizens of other countries and their own state. Particular attention is paid to high-ranking decision-makers at the strategic level – changing their behaviour to achieve their own goals – reflective management, which is adjacent (parallel) to cognitive warfare measures and is a subsystem of network-centric warfare (see Figure 1).

Thus, NATO has developed the Concept of Cognitive Warfare [14]. Cognitive warfare focuses on attacking and degrading rationality, which can lead to the exploitation of vulnerabilities and systemic weakening. Cognitive warfare integrates cyber, information, psychological capabilities and social engineering tools to influence attitudes and behaviour, protect or disrupt individual and group cognition to gain an advantage over the enemy, destroy unity, trust and democratic values.

The Concept of Cognitive Warfare has a dual purpose.

First, it forms a general framework for understanding the dynamics and mechanisms of cognitive warfare. It describes how an adversary uses social influence to manipulate public opinion, undermine decision-making processes and ultimately weaken military capabilities. The concept describes in detail the potential consequences of successful cognitive attacks, emphasising the vulnerability of national audiences, political structures and even military operations to disinformation and cognitive attacks.

Secondly, the Concept of Cognitive Warfare outlines NATO's path to strengthening its cognitive resilience and developing its capabilities to compete effectively in the cognitive domain. This includes protecting existing military capabilities and decision-making from manipulation, as well as exploring ways to strengthen public trust and understanding of NATO's role. By actively shaping the information environment and deterring foreign manipulation, NATO can ensure its freedom of action and continue to guarantee the security of its member states.

In cognitive warfare, the human mind shapes the battlefield. Cognitive warfare primarily targets cognition, which is "the mental process of acquiring and comprehending knowledge, as well as interpreting and perceiving information". Drawing on the psychological warfare of the past, which used propaganda to influence emotions, cognitive warfare uses modern technology to "build prejudices or mental automatons, causing distortions in perceptions, changing decisions or even inhibiting actions, and causing catastrophic consequences at both the individual and collective level". Unlike conventional (or kinetic) warfare, which uses physical violence, destruction and territorial conquest, cognitive warfare operates in the realm of ideas, emotions and perception. Referring to Sun Tzu, war seeks to use the human mind (which can be defined as cognitive warfare) as conventional forces and means that help to capture and hold territory by superior force, and can determine tactical or operational outcomes. Protecting the cognitive domain (the human minds) is essential to achieving lasting victory. Recent unconventional (non-lethal) conflicts have underscored the importance of this maxim.

Thus, cognitive warfare plays a key role in the modern architecture of hybrid warfare, using both individually and in combination cyber, psychological and information means to achieve its goals.

The development of the concept of "cognitive warfare" is a significant event in the field of warfare. It is aimed at more effective engagement, readiness, and maintaining trust and ability to deter adversaries in all areas of warfare. The key aspects of cognitive warfare are:

1. Importance and sphere of influence:

- the importance of gaining cognitive superiority can generally influence the outcome of a confrontation between adversaries;
- cognitive warfare involves actions conducted in sync with other instruments of power to influence attitudes and behaviour by influencing, protecting or destroying individual and group cognition;
- although most cognitive attacks remain below the threshold of armed conflict, their effects can span many domains, affecting all areas of warfare;
- cognitive effects are not always measurable in the typical sense, but they have a significant impact on how we think, feel and act. Brain-oriented technologies aim to destabilise structures (institutions), create distrust and weaken social cohesion;
-cognitive warfare can be a game changer.

2. Problems and individual approaches:

- insufficient development of cognitive influence measures, resulting in the lack of cognitive advantage;
- countries differ in cultural, social, technological and governmental structures, which affects their susceptibility to cognitive attacks;
- an individual approach is required to eliminate vulnerabilities and increase resistance to cognitive activities;
- countering cognitive attacks are a state task at the strategic level [15-16].

Currently, there is a tendency for the world's leading countries to develop an action plan to gain cognitive superiority [17]. For example, NATO:

cooperates with various organisations to combat cognitive warfare (Fig. 2) [18-19], namely

conducts international cooperation activities (works together with more than 20 member states, numerous NATO teams, academia and industry experts);

knowledge sharing (provides a forum for the exchange of research and information between member states and partner countries);

develops concepts (experts from many disciplines in NATO's Transformation Command develop concepts to protect the Alliance from cognitive warfare threats);

cooperates with the private sector to combat cognitive warfare in the following ways:

engages experts from industry to develop concepts and strategies;

organises joint working groups and workshops;

creates mechanisms to share information and synchronise capabilities, which can reduce military risk and increase the likelihood of mission success;

cooperates with academia to combat cognitive warfare in the following ways:

develops concepts (works with interdisciplinary experts to develop concepts aimed at protecting NATO against cognitive warfare threats);

organises educational events and training;

provides guidance on awareness, civil-military cooperation, societal resilience and data sharing;

promotes scientific research.

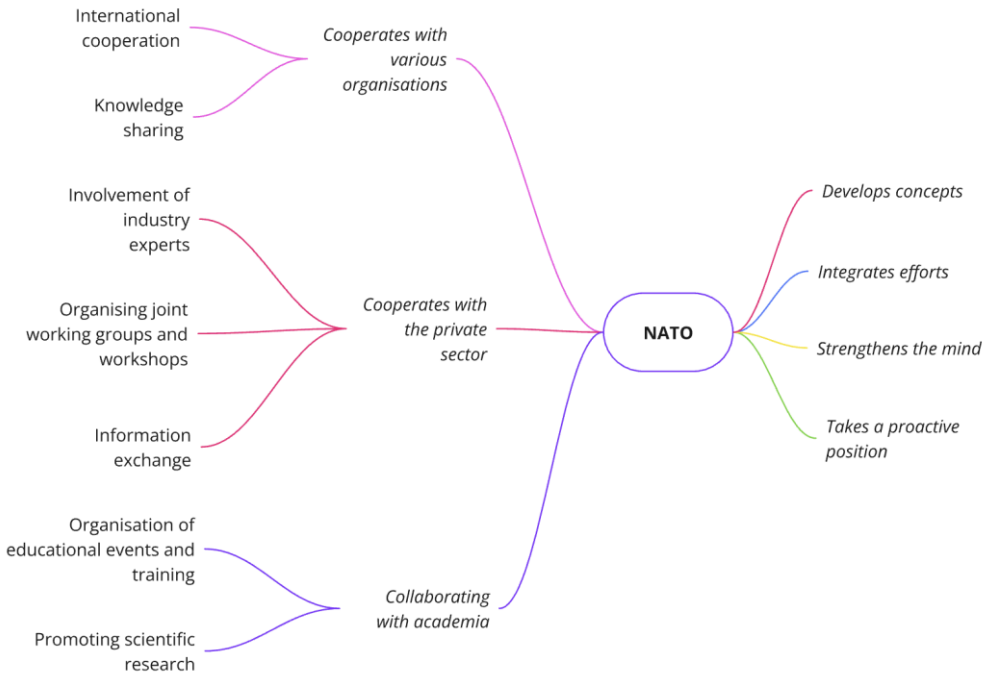

Figure 2. NATO measures to counter cognitive warfare threats

The rapid development of the latest information technologies and the introduction of artificial intelligence have brought hybrid warfare to a new level, and with it – operations in a multi-domain environment. The addition of cyberspace, asymmetric, network-centric and irregular actions to conventional warfare makes it much more difficult to conduct warfare in the classical style we know so well.

Today Ukraine is writing a new page in the history of warfare, needing not only weapons, but also detailed analytics and forecasting of existing threats in the information environment, especially in the cognitive domain.

In the current context of the restoration of the multipolar world, new actors are emerging to try to take their place in the geopolitical plane. The disguise of conquest is through the establishment of control and will not look like a classical war. The winner will be the one who manages to achieve a strategic advantage [2, 19], including through cognitive influence, without engaging in direct armed confrontation.

Results

Understanding the nature of cognitive warfare is the basis for good decision-making when it comes to their activities. They operate in a complex environment with a variety of threats, so it is important to develop a comprehensive approach to gaining cognitive superiority [20].

Cognitive warfare can include both separately and in combination the following components
disinformation: dissemination of false information to mislead;
propaganda: systematic dissemination of ideological messages to shape public opinion;
psychological operations: activities aimed at influencing people's emotions, motives and minds;
cyber warfare: the use of computer networks to gain a strategic advantage.

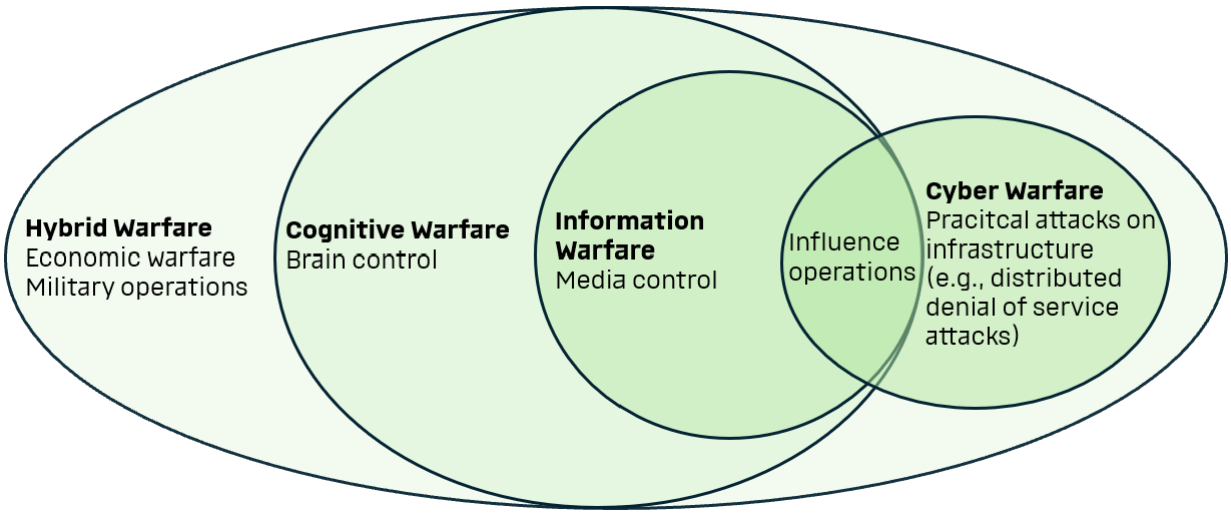

Figure 3. The relationship between cognitive warfare and modern technologies [20].

The following strategies can be used to avoid cognitive manipulation:
education;
critical thinking;
media literacy;
diversity of sources;
self-awareness.
The mass media also play an important role in preventing cognitive manipulation by:
*presenting facts (*the media should provide accurate and verified information);

*balance of opinions (*presenting different points of view to ensure objectivity);
*raising ethical standards (*adherence to high moral and professional standards);
*media literacy (*teaching the audience to critically perceive information).
The same applies to social media. To prevent cognitive manipulation, the following are necessary:
*content moderation (*detection and blocking of fake news and disinformation*)*;
*algorithms (*creation of algorithms that promote reliable content);
*cooperation with fact-checkers (*checking information for accuracy*);*
*educational campaigns (*training users to recognise manipulative content).
In view of the above, NATO countries are taking measures to counter cognitive influences:
concept development (creation of strategies to counter cognitive attacks);
integration of efforts (combining cyber, information, psychological and social engineering capabilities);
strengthening the mind (protecting and enhancing the cognitive capabilities of personnel);
a proactive posture (NATO is trying to be proactive in the cognitive dimension, recognising the threat of persistent cognitive attacks).
Such measures will allow NATO to:
shape the environment and counter the threats of cognitive warfare;
equip NATO countries to protect their core national democratic values;
improve its capabilities and strengthen its position in the field of cognitive warfare.
At the same time, artificial intelligence (AI) can be introduced into content moderation in the following ways:
develop algorithms - create algorithms that can recognise offensive and harmful content;
train models - use big data to train models to recognise patterns of disinformation;
test and optimise - to test the effectiveness of AI on real data and its continuous improvement;
integrate with human moderators - AI can perform initial analysis, while humans can evaluate more complex cases.
This combination can significantly improve the quality and speed of content moderation.
Education plays a key role in preventing cognitive manipulation by:
raises awareness - teaches people to understand how manipulation affects thoughts and behaviour;
develops critical thinking - helps to identify and analyse distorted information;
strengthens media literacy - teaches people to determine the reliability of sources and information;
promotes self-awareness - helps people to understand their own prejudices and emotional responsiveness.
Thus, education helps to create a society capable of critically evaluating information and resisting manipulative influences.

Conclusion

The main key to victory is understanding what it looks like. All elements in the modern architecture of hybrid warfare must be balanced with each other and optimised for the effects they produce. In combination with modern technologies, they will allow to gain an advantage in the information environment, including in the cognitive domain, when conducting operations in a multi-domain environment, to create a strong model of countering aggressor states at the state level that will meet modern realities, while maintaining unity, trust and national democratic values.
The analysis of research shows that in the near future, all modern technologies will be aimed at exerting influence without direct conventional confrontation.
Cognitive warfare will become increasingly widespread (important) in the modern architecture of hybrid warfare.
In general, cognitive warfare is a complex and multifaceted process that can have a serious impact on society during hybrid warfare. Both during armed conflicts and in peacetime, we can

protect ourselves from cognitive warfare by using critical thinking and information analysis and preserve our ability to think independently and objectively. Gaining Ukraine's cognitive superiority over Russia will be facilitated by the implementation at the state level of a comprehensive approach to responding to the enemy's armed aggression, taking into account the modern architecture of hybrid warfare.

References

1. Kogut, Y. (2023). *Hybrid warfare of a new type as a threat to the national security of states*. SIDCON Consulting Company; DAKOR Publishing House.
2. Sean McFate. (2023). *New Rules of War. Victory in an era of prolonged chaos*. (Transl. from English by Ihor Bihun). Nash format.
3. David Kilcullen. (2011). *The Accidental Guerrilla. Fighting small wars in the middle of a big one.* Hurst & Company.
4. *The Islamic State: the largest battle of our time*. (2nd edition). (2022). Mark Melnyk Publishing House (FOP Melnyk M.Y.)
5. *The US Army in Multi-Domain Operations 2028*. (2018, 6 груд.). TRADOC Pamphlet 525-3-1. Distribution Statement A.
6. *Multi-Domain Operations.* (2019, Sept.). Centre for Army Lessons Learned. Fort Leavenworth, KS 66027-1350. № 19-19. http://surl.li/rtnkr (accessed 14.10.2024).
7. Kogut, Y. I. (2022). Cyberwarfare, cyberterrorism, cybercrime (concepts, strategies, technologies): a practical guide.
8. *Happening in 2024: Advances in Cognitive Warfare, Multi-Domain Operations, Future Operating Environments, Sweden's Accession to NATO*. (2024, 8 Jan.). http://surl.li/dlvixk (accessed 14.10.2024).
9. *Allied Joint Doctrine for Strategic Communications*. (2023, March). NATO Standard AJP-10. NATO Standardisation Office (NSO): Edition A Version 1 with UK national elements (Change 1), © NATO/OTAN.
10. Joint Operations. Joint Publication No. 3-0. Washington DC: *Joint Staff, Incorporating change 1*, 22 (2022, Oct.).
11. Army Techniques Publication No. 3-13.1. *The Conduct of Information Operations*. (2018, Oct.). Headquarters, Department of the Army, Washington, DC, 04. http://surl.li/yjuove (accessed 14.10.2024).
12. Claverie, B., Prebot, B., Buchler, N. & Du Cluzel, F. (2021). *Cognitive Warfare*. *First NATO Scientific Meeting on Cognitive Warfare*. Bordeaux (France). (2021, 21 Jun.). Science and Technology Organisation. http://surl.li/wooshu (accessed 14.10.2024).
13. *Allied Command Transformation develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against "Cognitive Warfare"*. (2024). http://surl.li/dhaceu (accessed 14.10.2024).
14. *Workshop – Cognitive Warfare Concept*. (2022, 27 Sept.). http://surl.li/rtbtqv (accessed 14.10.2024).
15. *The 21st-Century Game Changer COGNITIVE WARFARE*. http://surl.li/ujxafu (accessed 14.10.2024).
16. *Cognitive Warfare – NATO's ACT*. http://surl.li/yweyeb (accessed 14.10.2024).
17. *Cognitive Warfare: Strengthening and Defending the Mind – NATO's ACT*. (2023, 5 Apr.). http://surl.li/jmcera (accessed 14.10.2024).
18. *Mitigating and Responding to Cognitive Warfare*. http://surl.li/zjhlju (accessed 14.10.2024).
19. *Countering cognitive warfare: awareness and resilience – NATO*. http://surl.li/piocap (accessed 14.10.2024).

20. Daniel Nikoula, Dave McMahon. (2024, 16 Jul.). *Cognitive Warfare: Securing Hearts and Minds.* Information Integrity Lab. http://surl.li/nvsbep (accessed 14.10.2024).

Когнітивна війна в сучасній архітектурі гібридної війни

Наталія Семенюк
начальник відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: nataliia.semeniuk@gmail.com
ORCID: 0000-0001-5795-0021

Анотація. Досвід російсько-української війни довів, що змінилися підходи до ведення війни від суто конвенційних на гібридні війни із конвенційними діями та включенням до них нових елементів. Переважно бойові дії ведуться одночасно у всіх вимірах, внаслідок чого було введено термін “операції в мультидоменному середовищі”. Наразі фізичні виміри (космічний, повітряний, морський та сухопутний) прошиті віртуальним (кібернетичним та інформаційним), які залежать від соціальних умов існування індивідів, їх моральних принципів та когнітивного сприйняття. Домінування на полі бою вимагає швидкої адаптації до нових реалій та трансформації підходів у веденні операцій в мультидоменному середовищі. Крім того когнітивна сфера є підсистемою мережоцентичних війн нового покоління у сучасній архітектурі гібридної війни. Чітке розуміння взаємодії елементів сучасної архітектури гібридної війни, їх координація та синхронізація під час проведення операцій в мультидоменному середовищі дозволить адаптуватися до нових збройних конфліктів та перемогти в них.

Авторкою взято до уваги сучасні тренди ведення війн різноманітного типу, враховано передовий досвід та представлено сучасну архітектуру гібридної війни. Запропоновано порядок дій для отримання когнітивної переваги.

Результатами запропонованого алгоритму має стати впровадження на державному рівні єдиної системи реагування на виклики сучасної гібридної війни, у тому числі в когнітивній сфері.

Ключові слова: гібридна війна, когнітивна війна, операції в мультидоменному середовищі, асиметрична війна, мережоцентрична війна, конвенційна війна, неконвенційна війна, кібер війна, когнітивна перевага, когнітивна сфера.