ANALYSIS OF APPROACHES AND TECHNOLOGIES FOR CONDUCTING COGNITIVE WARFARE IN MODERN CONDITIONS

Oleksandr Kin

Candidate of Technical Sciences, Senior Research Fellow, Associate Professor, e-mail: cubalibre1972@ukr.net,
ORCID ID: https://orcid.org/0009-0001-2196-7515

Hennadiy Udovenko Diplomatic Academy of Ukraine under the Ministry of Foreign Affairs, Kyiv, Ukraine

Received: November 24, 2025 | Revised: December 28, 2025 | Accepted: December 31, 2025

DOI: https://doi.org/10.33445/psssj.2025.6.4.4

Abstract

The article provides a military-political analysis of the cognitive dimension of modern hybrid warfare as a key element in the transformation of contemporary conflicts within the digital environment. The purpose of the study is to generalize approaches to the formation and implementation of the concept of cognitive warfare and to identify the main technologies and mechanisms of cognitive influence under current international confrontations. The methodological framework is based on doctrinal analysis, an interdisciplinary approach, comparative analysis of information and cognitive warfare concepts, and the examination of strategic documents and analytical materials of NATO and leading international institutions. The study demonstrates that cognitive warfare emerges at the intersection of military, informational, and psychological practices and is implemented through the deliberate construction of thinking patterns, causal relationships, and behavioral responses of individuals and social groups. Particular attention is paid to the influence of metamodern information reality, digital platforms, and artificial intelligence on the scale and intensity of cognitive operations. It is argued that the use of disinformation, manipulative narratives, and AI-driven technologies transforms the cognitive space into a distinct domain of confrontation aimed at undermining trust, political stability, and democratic processes. The article concludes that cognitive warfare has become a systemic factor of hybrid conflicts and requires further research, particularly regarding the disinformation aspects of artificial intelligence use.

Key words: Hybrid Warfare, Cognitive Warfare, Information Warfare, Cognitive Domain Operations.

Introduction

Contemporary armed conflicts increasingly extend beyond the boundaries of conventional warfare and acquire a multidimensional character, combining military, political, informational, and socio-psychological instruments of influence. Under these conditions, hybrid warfare has become the dominant form of modern conflict, in which decisive importance is attached not only to the physical destruction of the adversary but also to control over the perception, interpretation, and evaluation of reality by individuals and societies.

The rapid digitalization of the information environment, the expansion of social media, and the development of artificial intelligence and new media have significantly enhanced the capacity for targeted influence on mass consciousness. As a result, the cognitive dimension of confrontation is emerging as a critical element of modern conflicts, where the primary targets are thinking processes, belief formation, emotional responses, and behavioral patterns. Within this context, the concept of cognitive warfare has gradually taken shape and is increasingly reflected in academic discourse and military-strategic doctrines.

Despite the growing body of research on information and hybrid warfare, cognitive warfare as an independent and systemic dimension of confrontation remains insufficiently conceptualized.

Existing studies often conflate cognitive operations with information or psychological influence, which limits a comprehensive understanding of their nature, mechanisms, and strategic implications. At the same time, contemporary security practice—including the war in Ukraine and other international conflicts—demonstrates the expanding role of cognitive influence in achieving political and military objectives.

The purpose of this article is to provide a military-political analysis of the cognitive dimension of modern hybrid warfare by synthesizing theoretical approaches, doctrinal frameworks, and key technologies of cognitive influence. The study seeks to clarify the place of cognitive warfare within the structure of contemporary conflict and to substantiate its significance as a distinct domain that generates new challenges for international and national security systems.

Theoretical Background

The theoretical foundations of this study are situated at the intersection of hybrid warfare concepts, information warfare theory, and socio-philosophical analyses of mass consciousness. In contemporary security studies, cognitive warfare is increasingly viewed as an evolutionary stage of information warfare, where the object of influence extends beyond information flows to include perception, interpretation, and decision-making processes.

The conceptual origins of this approach can be traced to the works of **Marshall McLuhan**, who emphasized the decisive role of media in shaping mass consciousness and enemy images, framing information as a key weapon of future wars (McLuhan, 2014). These ideas laid the groundwork for subsequent studies that conceptualized the information environment as an independent domain of confrontation.

Further development of non-material dimensions of warfare is reflected in the works of **John Arquilla** and **David Ronfeldt**, who introduced the concepts of *noopolitik* and *noowar*, interpreting warfare as a struggle over meanings, knowledge, and narratives (Arquilla & Ronfeldt, 1999). Related perspectives are advanced by **Martin Libicki**, who systematized the forms and mechanisms of information warfare and highlighted its strategic nature (Libicki, 1995).

The contemporary stage of cognitive warfare theory is strongly influenced by doctrinal developments within NATO, particularly those advanced by Allied Command Transformation, where cognitive warfare is defined as coordinated activities synchronized with other instruments of power to influence attitudes and behavior (NATO Allied Command Transformation, 2023). Within this framework, the cognitive space is conceptualized as a distinct domain of confrontation alongside physical and digital domains.

Socio-philosophical interpretations of the changing information environment also play a significant role. **Alan Kirby** links the transition from postmodernism to metamodernism to changes in authorship and textual instability, directly affecting cognitive perception (Kirby, 2006). Similar ideas are developed by **Hanzi Freinacht**, who describes metamodern society as oscillating between truth and falsehood, creating favorable conditions for cognitive manipulation (Freinacht, 2017).

A separate strand of the literature focuses on digital phenomena such as post-truth, deepfakes, and cancel culture, analyzed as tools of cognitive influence in the context of social media and artificial intelligence (Oxford Dictionaries, 2016; Velasco, 2020; Thies et al., 2016). In this regard, reports by the **World Economic Forum** identify disinformation as a systemic risk to democratic processes (World Economic Forum, 2024).

Overall, the literature indicates a shift from information warfare toward cognitive confrontation as a systemic component of hybrid conflicts. However, existing studies remain fragmented, highlighting the need for an integrated theoretical framework.

Data and Methods

The study is theoretical and analytical in nature and is based on the analysis of open sources, strategic documents, conceptual materials, and academic publications addressing hybrid, information, and cognitive warfare. No empirical statistical data are employed, as the research objective focuses on the conceptual understanding of the cognitive dimension of modern conflicts.

The data set includes official NATO documents and analytical reports, particularly materials developed within the framework of Allied Command Transformation, NATO strategic concepts, as well as publications by leading international institutions and research centers. In addition, the study draws on academic works by domestic and international scholars in the fields of information security, strategic communications, postmodern and metamodern philosophy, and studies on disinformation, artificial intelligence, and digital media.

The methodological framework is based on an interdisciplinary approach combining military-political analysis, information security studies, and socio-philosophical concepts. The research applies doctrinal analysis to examine official approaches to cognitive warfare, comparative analysis to distinguish between information, cognitive, and hybrid warfare concepts, and logical-analytical methods to identify cause-and-effect relationships between transformations of the information environment and changes in contemporary forms of confrontation. The analysis of digital phenomena such as post-truth, deepfakes, cancel culture, and the metaverse is used to conceptualize mechanisms of cognitive influence within the metamodern information reality.

Results

The concept of cognitive warfare emerged at the intersection of military, information and psychological research. Its roots can be found in various military doctrines and strategic approaches to information and psychological warfare, but as a separate term it has become widely used in recent decades. One of the first official military documents that directly refers to cognitive warfare appeared in NATO, specifically within the framework of Allied Command Transformation (ACT), which actively researches new threats, in particular those related to information and cognitive influences (NATO ACT, 2023). Allied Command Transformation guides the concept of cognitive warfare research, which is part of a wider agenda for the development of military strategies (NATO Allied Command Transformation [NATO ACT], 2023). Understanding the conceptual framework, definitions, consequences and risks of such warfare, according to experts, contributes to better political decision-making, the development of military capabilities, and the overall security of the Alliance. The Allied Transformation Command conducts training, cooperation, protection and capability development for NATO in the field of cognitive warfare, providing recommendations on awareness raising, civil-military cooperation, societal resilience and information sharing to ensure the Alliance's current and future security.

Aimed at changing perceptions of reality, societal manipulation has become the new standard, and human cognition is becoming a critical area of warfare. The definition of cognitive warfare proposed in NATO's ACT research concept is as follows: "Activities conducted in synchronisation with other instruments of power to influence attitudes and behaviour through manipulation, protecting or violating the cognition of individuals and groups to gain an advantage over the enemy" (NATO ACT, 2023).

The relevance of this concept arises from the challenges NATO has faced in recent years and has introduced into the concept, namely (NATO ACT, 2023): technological progress and changes in information consumption provide opponents with greater opportunities to collect and manipulate data, influence emotions, and shape beliefs and behaviour. It makes possible to exploit the differences in society through the latest technologies, such as artificial intelligence, emerging and disruptive technologies (EDTs), and data collection. In addition, the spread of social media contributes to influencing the thoughts, emotions, and actions of individuals.

As the authors of the concept note, it reflects the tactics of hybrid warfare, where society is used as a vector of influence on key targets – political and military leaders. The effectiveness of information campaigns depends on the targeted manipulation of emotions and cognitive biases, which causes large-scale changes in attitudes and behaviour. Such changes are often subtle and inconspicuous, blurring the line between genuine public discourse and hostile cognitive attacks that exploit social divisions.

Although cognitive attacks are not a new phenomenon, the concept defines them as deliberate offensive manoeuvres aimed at influencing perceptions, beliefs, interests, decisions, and behaviour through a direct attack on human consciousness. The innovative aspect of this approach is that enemies can now quickly and anonymously conduct cognitive attacks in the information environment using digital platforms and breakthrough AI technologies.

Cognitive warfare today fully reflects the system of principles of the meta-modern philosophical era, for which categories such as truth and reality are entirely relative. If postmodernism was marked by the growing influence of the media on the formation of new principles of individual perception of reality and a new type of inter-state communication, and television contributed to the cultivation of mass pop culture, then the beginning of the 21st century gave rise to a new phenomenon, namely the Internet, which transformed horizontal "subject-object" relationships, in the case of spiritual and informational exchange – "author–recipient". For example, voting for participants in various TV shows is becoming an insufficient act of communication for people in the new information age, since its purpose is not only to be on the side of the object or subject of this communication, but to fulfill both roles at the same time. This radical change in the function of the producer is noted by A. Kirby: "The author now has the status of one of those who sets the parameters without which other operators become simply irrelevant, unknown, out of line. These changes also apply to the "text" itself, which is characterized by hyper-ephemerality and instability" (Kirby, 2006).

Currently, the Metamoderna.org project is gaining popularity in Europe – a collaboration between Swedish cultural theorists and sociologists Emil Friis and Daniel Gortz to create a virtual "philosopher, historian and sociologist Hanzi Freinacht, who "lives" alone in the Swiss Alps. Combining age psychology and cultural studies, Emil Friis and Daniel Gortz, on behalf of Hanzi Freinacht, have recently published a book entitled "The Listening Society", in which they reveal the secrets of "memes of metamodern significance" (Freinacht, 2017). Modern people are surrounded by an overload of information, facts, events, knowledge, and things, and at this time, it is difficult and no longer necessary to strive for stability or a final system as the truth. The world of post-truth, fake news and information manipulation detracts from the sense of stability and understanding of the essence of reality.

Metamodernism gave rise to a new wave of informatisation of society with the establishment of the Internet, and later artificial intelligence, expanding access to these technologies to members of society with varying levels of wealth, as well as the formation of so-called new media in social networks (blogs, public pages, etc.). Internet communication has led to the transformation of interpersonal, interinstitutional and intergovernmental information exchange. At this time, thanks to the global online network, concepts are emerging and becoming established that are actively used in cognitive warfare:

"post-truth" – it emerged as a phenomenon of the postmodern era, but in the metamodern era it is being perfected and becoming a marker of the information age. According to the Oxford English Dictionary, post-truth is an information flow which is deliberately constructed in modern society with the help of the media to create a virtual reality that differs from the real one, with the aim of manipulating public consciousness (Oxford Dictionaries, 2016). In 2016, this word was named word of the year by dictionary editors;

"cancel culture" – a modern form of ostracism, which Michigan State University professor Lisa Nakamura described as an attempt to control freedom of thought using the power given by social networks (Velasco J., 2020). This refers to the bullying of public figures in the information space for their present or past actions and deeds, in the context of the general right to self-expression and the expression of one's own position in the network. Thus, the presumption of innocence ceases to apply at the level of public discussion. Such online information campaigns are also sometimes referred to as "cancelling".

"deepfake" is a method of synthesising human images based on artificial intelligence. It is used to combine and superimpose images and videos onto original images or videos. Methods for detecting gestures and converting the original video into a video with a face similar to the target person were presented in 2016 and enable real-time calculation of fake facial expressions in 2D videos (Thies et al., 2016). Deepfakes can be used to create fake news, malicious deceptions, including the compromising of celebrities and public figures and the destruction of political reputations.

"metaverse" is a term that originated in science fiction novels in the 1990s. In the autumn of 2021, Mark Zuckerberg revived it by presenting a course of conceptual rebranding for the company Facebook, which will now work on creating a new cyber reality in which simulators become a tool for accurately reproducing reality in cyberspace. According to the concept, the metaverse is a permanent live virtual space in which people can interact with each other and with digital objects through their avatars, using virtual reality technologies.

Metamodern consciousness is in a state of constant oscillation (swinging). It is about radical openness, about universal acceptance. At this time, cognitive wars are reaching their peak, as the Internet, AI and social networks as the main marker of new informational and spiritual exchanges have led to the appearance of the meta-modern author and the meta-modern recipient, who often switch roles (this can be represented as a post with certain information on social networks, which other users reproduce on their pages, decorating it with numerous comments and accompanying texts). Human consciousness begins to constantly exist in a state of "meta" – "between" the usual reality and the network reality, which duplicates objective reality as much as possible; between truth and falsehood, trust and distrust.

Considering the rapid emergence of a new information reality based on cyber technologies, in particular AI, it can be assumed that humanity is in the process of forming a new type of metamodern society – an information networked society that is permanently in a state of cognitive and conscientious warfare. Manipulation of consciousness through information has gradually replaced violence, which for a long time was considered the only means of governance. That is why modern media of this type are becoming an effective tool for political propaganda, the spread of disinformation as a source of destabilising social processes, and also a direct information weapon used in hybrid warfare. During such cognitive warfare, modern cyber technologies, in particular artificial intelligence, are actively used.

Virtual space protection against cognitive attacks is a new stage in the development of information security, which is aimed specifically at the digital environment. In the late 1990s, experts from the RAND analytical centre of the US administration, J. Arquilla and D. Ronfeldt highlighted the problems of information strategy, cyber warfare, network warfare, and information warfare. In their opinion, the concepts of cyberspace and the information sphere should be combined as a combination of cyberspace and the mass media into a single "noosphere" – a new based on ideas, spiritual values, ethics, and an epistemological paradigm in which traditional politics of "brute" force with its emphasis on the material component of opposition is replaced by a new one based on “soft power”. The modern “noowar” as a war of meanings and knowledge corresponds to a special term for the new politics – “noopolitik” (Arquilla & Ronfeldt, 1999). Such politics are implemented both in real and virtual space, using various platforms for their implementation, as well as various instruments.

Disinformation supported by foreign states may be aimed at creating confusion, exacerbate political polarisation, undermine democracy or create mistrust in societies. Although research shows that disinformation can influence beliefs, the degree to which it leads to behavioural change or has a real impact remains uncertain and difficult to measure. In January 2024, the World Economic Forum named disinformation as the greatest short-term risk in the world due to its potential to undermine democratic elections, causing social unrest and increasing censorship through initiatives to counter disinformation (World Economic Forum [WEF], 2024).

The digital space is becoming a specific platform for information terrorism, cognitive and conscientious attacks, simulated wars, Gibson’s wars. While the first category is the most common type of information aggression in the digital space, the second consists of preserving the functioning of the information system in its correct form, but with a certain distortion, a change in the information flow that changes the principle of information perception, and subsequently the ability to analyse it correctly, in intimidation with a certain type of weapon with the corresponding information accompaniment, which has special technical characteristics. Gibson’s wars exist more as a concept, which consists of waging war in virtual space using intelligence (including humans directly in the Internet network) (Libicki, 1995). Thus, artificial intelligence technologies are integrated into so-called noopolitik.

It should be noted that artificial intelligence in the field of cognitive warfare can significantly increase the scale of the threat of mass consciousness change. As it is known, one of the three pillars of a functioning democracy is representativeness. In order for elected representatives to respond effectively to the requests of their voters, they need to know exactly what they think. However, information warfare, controlled by AI, can manipulate social networks, creating confusion and spreading disinformation that distorts politicians’ perception of public opinion. Thus, if the populations of democratic countries are deceived into believing that, for example, Ukraine and Taiwan are not worth defending, the world will become critically vulnerable to aggressive tyranny.

Within the framework of the Munich Security Conference 2024, a document entitled “The Battle for the Mind: Understanding and Addressing Cognitive Warfare” (Centre for Governance and Change, 2024) was approved, which summarises the discussions that took place during a high-level Round Table on Cognitive Warfare organised by the Centre for Governance and Change (CGC) at IE University. The event was attended by Margrethe Vestager, Arancha González Laya, Anne Marie Slaughter and other well-known politicians and industry leaders. The document analyses the establishment of cognitive space as the sixth dimension of warfare – after land, sea, air, space and cyberspace – in the context of multi-domain theory.

Discussion

The findings of this study confirm that cognitive warfare has evolved into a systemic and autonomous dimension of modern hybrid warfare rather than remaining a subsidiary element of information or psychological operations. The analysis demonstrates that contemporary cognitive confrontation targets not merely information flows but the underlying mechanisms of perception, interpretation, and decision-making, thereby reshaping the strategic logic of conflict. This result supports theoretical assumptions that modern warfare increasingly prioritizes non-material forms of influence over traditional kinetic means.

The conceptualization of cognitive warfare presented in the article aligns with and extends NATO’s doctrinal approach, particularly the framework developed by Allied Command

Transformation, which defines cognition as a critical domain of competition. However, the discussion highlights that cognitive warfare should not be understood solely as an extension of information warfare. Instead, it represents a qualitative shift toward influencing causal reasoning, emotional responses, and behavioral patterns at both individual and societal levels. This distinction clarifies one of the central research questions by demonstrating that cognitive warfare operates on a deeper level than information dissemination or persuasion.

The results also resonate with earlier theoretical contributions that frame warfare as a struggle over meanings and narratives rather than material resources. The concepts of *noopolitik* and *noowar* are particularly relevant in interpreting the findings, as they provide an analytical lens for understanding cognitive space as a battlefield where values, identities, and interpretations of reality are contested. In this regard, the study confirms that contemporary hybrid conflicts increasingly rely on the manipulation of symbolic and cognitive resources to achieve strategic objectives.

A significant contribution of the discussion is the integration of socio-philosophical perspectives on metamodernism into the analysis of cognitive warfare. The findings suggest that the metamodern information environment—characterized by oscillation between truth and falsehood—creates structural vulnerabilities that can be systematically exploited through cognitive operations. Phenomena such as post-truth narratives, deepfakes, and cancel culture are not isolated media effects but components of a broader cognitive ecosystem shaped by digital platforms and artificial intelligence. This interpretation deepens the understanding of how technological and cultural transformations amplify the effectiveness of cognitive influence.

The discussion further underscores the growing role of artificial intelligence as a force multiplier in cognitive warfare. AI-driven tools enable the rapid personalization, scaling, and automation of manipulative narratives, thereby increasing both the reach and subtlety of cognitive attacks. At the same time, the study acknowledges the limitations identified in the literature regarding the measurement of the actual behavioral impact of disinformation. While cognitive influence can shape beliefs and perceptions, its translation into concrete political or military outcomes remains difficult to quantify, which represents an important methodological challenge for future research.

From a military-political perspective, the findings imply that cognitive warfare poses a direct challenge to democratic systems, where openness, pluralism, and freedom of expression can be exploited as vectors of influence. The discussion highlights that the erosion of trust in institutions, combined with the attention economy and societal polarization, increases the susceptibility of liberal democracies to cognitive manipulation. This observation is consistent with recent assessments by international organizations that identify disinformation as a systemic security risk.

Despite its contributions, the study has several limitations. First, its theoretical and doctrinal focus precludes empirical testing of specific cognitive operations or case-based measurement of their effectiveness. Second, the reliance on open-source documents and analytical reports limits the ability to assess classified or covert dimensions of cognitive warfare. These limitations suggest that future research should incorporate empirical case studies, experimental designs, or comparative analyses across different conflict contexts.

Overall, the discussion reinforces the central argument that cognitive warfare has become a defining feature of modern hybrid conflicts. By conceptualizing the cognitive domain as a distinct space of confrontation, the study contributes to a more nuanced understanding of contemporary warfare and highlights the need for integrated policy responses that combine military, informational, technological, and societal resilience measures.

Conclusions

Today, both government and non-government actors have the tools and stimuli to manipulate our thoughts and destroy our common understanding of reality – from interfering with specific military manoeuvres to destabilising societies and multilateral cooperation. Contemporary society has entered a hyperrealistic dream in which everything is true and false at the same time, and those who generate meaning and information themselves fall into its trap, becoming consumers rather than producers. The increased use of artificial intelligence in all areas of activity not only has a constructive impact on the development of high technologies and improves the possibilities for ensuring individual and national security, but also becomes an instrument of destabilisation processes, both within the microcosm of an individual, influencing the processes of information processing, but also in the geopolitical macrocosm, even transforming the understanding of the established world order.

The growth in the use of deceptive narratives and manipulative AI in democratic processes, the war in Ukraine and the conflict between Israel and Hamas demonstrate a growing geopolitical interest in controlling people's perception. Citizens of liberal democracies are particularly vulnerable to cognitive manipulation, as the economy of attention negatively affects our ability to think critically, trust in institutions is at an all-time low, and the polarisation of society has reached its peak.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Arquilla, J., & Ronfeldt, D. (1999). *The emergence of noopolitik: Toward an American information strategy*. RAND Corporation.

Centre for Governance and Change. (2024). *The battle for the mind: Understanding and addressing cognitive warfare and its emerging technologies*. IE University. https://static.ie.edu/CGC/CGC_TheBattleofTheMind_2024.pdf

Freinacht, H. (2017). *The listening society: A metamodern guide to politics*. Metamoderna.

Kirby, A. (2006). The death of postmodernism and beyond. *Philosophy Now*, (58), 34–37. https://philosophynow.org/issues/58/The_Death_of_Postmodernism_And_Beyond

Libicki, M. C. (1995). *What is information warfare?* National Defense University Press.

McLuhan, M. (2014). *Media research: Technology, art and communication*. Taylor & Francis.

NATO Allied Command Transformation. (2023). *Cognitive warfare exploratory concept*. NATO ACT.

Oxford Dictionaries. (2016). *Post-truth*. https://www.lexico.com/en/definition/post-truth

Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., & Niessner, M. (2016). Face2Face: Real-time face capture and reenactment of RGB videos. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2387–2395. http://www.niessnerlab.org/papers/2016/1facetoface/thies2016face.pdf

Velasco, J. (2020). You are cancelled: Virtual collective consciousness and the rise of cancel culture. *Rupkatha Journal on Interdisciplinary Studies in Humanities*, 12(5). https://rupkatha.com/V12/n5/rioc1s21n2.pdf

World Economic Forum. (2024). *Global risks report 2024*. https://www.weforum.org/publications/global-risks-report-2024