



INFORMATION AND COMMUNICATION TECHNOLOGIES


ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

DOI: 10.22363/2313-0660-2025-25-2-236-250

EDN: MQQFIS

Research article / Научная статья

Information Warfare in a Multipolar World

Sergei V. Bazavluk¹ , **Andrei A. Kovalev²**  ¹National Research Institute for the Development of Communications, Moscow, Russian Federation²North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration, St. Petersburg, Russian Federation kovalev-aa@ranepa.ru

Abstract. The formation of a new world order in the 21st century is in its infancy, and the growing contradiction between international actors continues to intensify. In an effort to preserve unipolarity and counteract multipolarity, the United States adheres to the concept of information warfare, involving the rest of the world in this process. Conflict remains a prevalent feature of international relations, and dialogue is frequently perceived either as a sign of weakness or as a planned maneuver by an opponent. The purpose of the study is to identify the features of the axiological and technical aspects of information warfare in a multipolar world. Two key aspects of information warfare are examined separately: the information-psychological and the information-technical. The analysis of the use of information warfare tools enables the identification of the direction of actions by global actors, the main methods employed, the goals pursued and the results achieved. The research methodology is based on systematic and axiological approaches, which have facilitated the conceptualization of information warfare as a form of non-kinetic influence on the value and institutional foundations of the enemy. The present study employs a hermeneutical analysis of sources, incorporating elements of lexico-semantic analysis, as a methodological approach. The main conclusion of the study asserts that information warfare, in which the United States remains the main actor, poses a serious threat to the emerging multipolar world and the security of its supporters, while acknowledging their potential for resistance, which is likely to emerge in the future. In conclusion, the following directions for further research are proposed: firstly, the practice of interaction between the allied states that prevent the restoration of a unipolar world; secondly, the information pressure from the United States and the collective West; thirdly, Russia's transition from defensive to offensive actions in the information warfare; and fourthly, the analysis of new tools and methods of conducting information warfare, as well as other relevant topics.

Key words: cognitive warfare, mental security, strategic propaganda, artificial intelligence technologies, deepfake, decoupling, technological sovereignty, digital manipulation, hybrid threats, psychosphere, value impact, information destabilization



Conflicts of interest. The authors declare no conflicts of interest.

Authors' contributions. S.V. Bazavluk: conceptualization, development of research methodology, analysis, writing and preparation of a draft manuscript. A.A. Kovalev: theoretical and analytical study of the material, text editing, bibliography design, validation of sources. Both authors have read the final version of the article and approved it.

For citation: Bazavluk, S. V., & Kovalev, A. A. (2025). Information warfare in a multipolar world. *Vestnik RUDN. International Relations*, 25(2), 236–250. <https://doi.org/10.22363/2313-0660-2025-25-2-236-250>

Информационное противоборство в многополярном мире

С.В. Базавлук¹, А.А. Ковалев²✉

¹Национальный исследовательский институт развития коммуникаций, Москва, Российская Федерация

²Северо-Западный институт управления — филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Санкт-Петербург, Российская Федерация
✉kovalev-aa@ranepa.ru

Аннотация. Формирование нового миропорядка в XXI в. находится в стадии становления, а нарастающее противоречие между международными акторами продолжает усиливаться. США, стремясь сохранить однополярность и противодействуя многополярности, придерживаются концепции информационного противоборства, вовлекая в этот процесс остальной мир. Конфликтность в международных отношениях сохраняется, а диалог часто воспринимается либо как проявление слабости, либо как спланированный маневр оппонента. Цель исследования — выявление особенностей аксиологического и технического аспектов информационного противоборства в многополярном мире. Отдельно рассмотрены два ключевых аспекта информационного противоборства: информационно-психологический и информационно-технический. Анализ применения инструментов информационного противоборства позволяет установить направленность действий глобальных акторов, основные используемые методы, преследуемые цели и достигнутые результаты. Методология исследования основана на системном и аксиологическом подходах, позволивших информационное противоборство как форму некинетического воздействия на ценностные и институциональные основы противника. В качестве метода применен герменевтический анализ первоисточников с элементами лексико-семантического разбора. Авторами сделан вывод, что информационное противоборство, главным субъектом которого остаются США, представляет серьезную угрозу формирующемуся многополярному миру и безопасности его сторонников, при этом отмечается наличие у них потенциала к сопротивлению, который, вероятно, будет раскрываться в будущем. В заключении приводятся возможные направления для дальнейших исследований, такие как практика взаимодействия союзных государств, препятствующих восстановлению однополярного мира и информационному давлению со стороны США и коллективного Запада; переход России в информационном противоборстве от оборонительных действий к наступательным; анализ новых инструментов и методов ведения информационного противоборства и другие актуальные темы.

Ключевые слова: когнитивная война, ментальная безопасность, стратегическая пропаганда, технологии искусственного интеллекта, deepfake, декаплинг, технологический суверенитет, цифровая манипуляция, гибридные угрозы, психосфера, ценностное воздействие, информационная дестабилизация

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Вклад авторов. Базавлук С.В.: концептуализация, разработка методологии исследования, проведение анализа, написание — подготовка черновика рукописи. Ковалев А.А.: теоретико-аналитическая проработка материала, редактирование текста, оформление библиографии, валидация источников. Оба автора ознакомлены с окончательной версией статьи и одобрили её.

Для цитирования: Базавлук С. В., Ковалев А. А. Информационное противоборство в многополярном мире // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2025. Т. 25, № 2. С. 236–250. <https://doi.org/10.22363/2313-0660-2025-25-2-236-250>

Introduction

The contemporary world is undergoing profound transformations, with the unipolar structure being replaced by a multipolar configuration, characterized by a redistribution of centers of power. Nevertheless, states that have openly proclaimed their commitment to a polycentric world order are facing active resistance from the United States. Rather than resorting to direct military confrontation, the focus is increasingly shifting toward concealed forms of struggle, especially information confrontation.

The term ‘information confrontation’ possesses a complex etymology and consists of two components: ‘information’ (from the Latin *informatio* — “explanation, presentation, communication”) and ‘confrontation,’ which itself is composed of “contra” (from Old Church Slavonic *prětivŭ*, meaning “opposing, hostile”) and “struggle” (the root “bor-” traces back to Old Russian *boroniti* — “to defend, to resist”). Thus, the term ‘information’ encompasses the processes of transmitting, processing, and receiving data, while ‘informational’ refers to the exchange of information or the application of technologies. In turn, ‘confrontation’ implies active resistance and struggle between parties seeking to achieve their objectives by overcoming the will of their opponent. Therefore, information confrontation should be understood as active operations within the information domain aimed at achieving strategic objectives by employing information as a resource or an instrument. Information confrontation is conducted in both offensive forms, such as the dissemination of disinformation, and defensive forms, aimed at protecting against informational threats.

In the 21st century, the arena of state rivalry has increasingly shifted to the informational domain, thus making information confrontation

an integral part of national security strategies and military doctrines. It involves interactions between states in various fields, including political, economic, military, etc., where influence is exerted on the adversary’s information sphere to expand one’s zone of influence (Vykhodets & Pantserev, 2022, p. 139). In their joint work dedicated to the methodological foundations of building a theory of information confrontation, A.I. Pozdnyakov and V.S. Shevtsov emphasize that the notion of “information war” should be understood only metaphorically; therefore, the term “information confrontation” (or “struggle”) is more appropriate (Pozdnyakov & Shevtsov, 2017, p. 245). The authors also observe that the informational influence exercised within the framework of information confrontation can be divided into two major categories: information-technical and information-psychological. It is important to highlight that information-technical confrontation is embodied in the concept of cognitive warfare, which focuses on the technical aspects based on the advances of cognitive science. These advances enable the manipulation and control of human information consumption processes, whereas information-psychological confrontation is articulated through the concept of mental warfare, which primarily concentrates on altering the value and worldview orientations of individuals and societies. It is essential to understand that information-psychological confrontation is carried out through information-technical systems.

Consequently, there are a number of contemporary theories of information confrontation, which can be divided into two broad and interconnected groups.

In the context of analyzing *information-technical confrontation*, particular attention can be given to the concepts of *netwar*, *network-centric warfare*, and *cyber warfare*. The theory of *netwar* was articulated in the work

of J. Arquilla and D. Ronfeldt (1996),¹ in which the authors posited that the network-based principle of organizing contemporary confrontation has become predominant in modern warfare. Disrupting the adversary's communications and information networks through the use of advanced technologies is, therefore, emerging as a primary means of achieving military objectives.

At the turn of the 21st century, the United States developed the theory of network-centric warfare,² in which personnel, military equipment, and command structures were integrated into a unified information network. The purpose of such integration was to enhance the synchronization of actions between different combat units and to increase the speed of operational control on the battlefield. Consequently, the hierarchical mode of organizing and coordinating military operations began to give way to the network-based principle. In turn, the concept of cyber warfare encompasses knowledge of how to inflict damage on an opposing side through the use of computers and the Internet, with cyberattacks making it possible to do so remotely, without regard to national borders (Clarke & Knake, 2010).

The information-technical dimension is currently exerting a significant influence on the formation of a multipolar world order, with the leading global powers (the United States, China, Russia, and several others) acting as its main actors. The methods of confrontation within the framework of the information confrontation are constantly being refined and becoming more complex. In this study, particular attention is paid to the decoupling and the competition in the

development of technologies related to Industry 4.0 (the Fourth Industrial Revolution) as effective methods of the information-technical confrontation and as key factors in the sanctions policy.

Information-psychological confrontation is a type of information confrontation and is considered from the perspective of an axiological approach to the security system as a whole. In contemporary warfare, the human psyche becomes a target of informational influence and sustains significant damage (Hoyle et al., 2021, p. 150), which is why ensuring mental (cognitive) security constitutes an important objective within national security strategies. Through the manipulation of the adversary's population consciousness, the objectives of information-psychological confrontation are pursued (Manoylo, 2019, p. 39). Possessing knowledge of the mechanisms of influencing public opinion, the conditions of its formation, and the ways in which information is perceived and processed by individuals enables the effective conduct of information-psychological confrontation. The possibility of applying psychological research to the military sphere had been previously explored by the American scholar P. Linebarger as early as 1954 (Linebarger, 1962).

Thus, information-psychological confrontation is carried out within the framework of mental warfare. This particular type of confrontation is explored in the works of the Russian military expert A.M. Ilnitsky, who identifies the self-consciousness of the individual (or the nation), the national mentality, and the civilizational foundations of the adversary's existence as the primary targets of influence (Ilnitsky, 2021). Essentially, the term mental warfare can be defined as hostile actions in which the values, ideals, way of life, and other elements (attributes) of one nation are transferred to another. Accordingly, it may be assumed that, in accordance with the perspective of A.M. Ilnitsky,³ if the characteristic traits and

¹ Arquilla J., Ronfeldt D. *The Advent of Netwar*. Santa Monica, CA : RAND Corporation, 1996. (The activities of *RAND Corporation* are considered undesirable in the territory of the Russian Federation (*Editor's note*)).

² Cebrowski A. K., Garstka J. H. *Network-Centric Warfare — Its Origin and Future* // *Proceedings*. 1998. Vol. 124, no. 1. URL: <https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future> (accessed: 06.01.2025).

³ Ilnitsky A. M. *Mental War for the Future of Russia* // *Zvezda*. April 21, 2021. (In Russian). URL:

features of one nation (the subject of influence) become evident within another nation (the object of influence), a mental intrusion has taken place. In other words, the existence of mental warfare can be inferred from its outcomes.

In recent years, there has been a notable development and application of methods of cognitive warfare in the context of information confrontation. The North Atlantic Treaty Organization (NATO), under the leadership of the United States, has identified the following key domains in its core concept of military operations: land, maritime, air, space, information (cyberspace), and cognitive.⁴ Increasing attention is being paid to the cognitive domain in wars of the new type, particularly with regard to the development and implementation of methods for conducting military operations. This domain is regarded as a promising direction for further advancements. “Hacking the individual” is both a core principle and an instrument of cognitive warfare, the essence of which is the manipulation of human consciousness and the direct control of individual actions.⁵ In this case, destabilization and external influence serve as the primary objectives of cognitive confrontation.⁶

The development of cognitive warfare is largely based on advances in the neurosciences, which provide opportunities for deeper influence over psychophysiological processes. In this

regard, the neurosciences are becoming an instrument of political struggle, facilitating the achievement of large-scale strategic objectives. The battle for the human mind is radically transforming conceptions of security, which is increasingly perceived as a zero-sum game (Ördén, 2024, p. 614).

Information confrontation, in which the United States plays an active role, is regarded as a non-traditional security threat in the context of a multipolar world. Information-psychological confrontation, based on “soft power” methods, unfolds in the cultural space with the aim of transforming the consciousness of a political opponent, who may not even be aware of such influence. The targets of such attacks include value systems, traditions, historical and cultural identity of states (Goncharova, Nicevich & Sudorgin, 2024, p. 21), as well as critical infrastructure, military facilities, and other key elements of the state, thereby endangering the information-psychological sphere.

The dynamic development of international processes, driven by rapid advances in information and communication technologies (ICT) and the growing global tensions, has served as the foundation for this study. Particular concern in the context of information confrontation is raised by issues of information-psychological security. The present study is devoted to the analysis of information confrontation in a multipolar world. The aim of the research is to identify the specific features of the axiological and technical dimensions of information confrontation in the context of an emerging multipolar world.

The authors adopt a critical-analytical approach that interprets information confrontation as a form of non-kinetic influence aimed at transforming the mental and institutional resilience of the adversary. This perspective distinguishes the present study from technocratic and infrastructural models focused on the control of the ICT environment, as well as from the neo-Marxist interpretation (particularly characteristic of the works of M. Castells), which

<https://zvezdaweekly.ru/news/20214211636-jxgHZ.html> (accessed: 19.04.2025).

⁴ Tammen J. The NATO Warfighting Capstone Concept: The Changing Character of Warfare Ahead // NATO Review. July 9, 2021. (In Russian). URL: <https://www.nato.int/docu/review/ru/articles/2021/07/09/bazovaya-kontseptsiya-boevykh-deystvij-nato-v-perspektive-menyayushchisya-harakter-vojny/index.html> (accessed: 06.01.2025).

⁵ Du Cluzel F. Cognitive Warfare, a Battle for the Brain. NATO Innovation Hub. 2020. URL: <https://archive.org/details/mp-hfm-334-kn-3> (accessed: 19.01.2025).

⁶ Wanyana R. Cognitive Warfare: Does it Constitute Prohibited Force? // EJIL: Talk. January 30, 2025. URL: <https://www.ejiltalk.org/cognitive-warfare-does-it-constitute-prohibited-force/> (accessed: 02.02.2025).

emphasizes the role of digital networks within the global system of communication, power distribution, and economic influence (Castells, 2000). The chosen approach facilitates an examination of the humanitarian aspects, and the value-based vulnerability of actors engaged in geopolitical interaction.

The methods employed in the study included systematization, through which the broad definition of “information confrontation” was differentiated on the basis of a more localized and specific aspects of this confrontation within the functioning of the international system. The systemic approach made it possible to identify the underlying causes and meanings behind the restructuring of the world order and the chosen methods of its implementation. In addition, the systemic-activity approach and its axiological component were applied to explore the selected topic, along with hermeneutic analysis of primary sources incorporating elements of lexical-semantic analysis. These methods enabled the study of the potentials of the information-technical and information-psychological dimensions of the information confrontation, the identification of possible uses of artificial intelligence (AI) technologies for both offensive and defensive purposes, and the examination of Russia’s capabilities in maintaining its sovereignty in the contemporary multipolar world.

Information Warfare in the Contemporary World

The term ‘information war’ was first mentioned in a report by scholar Thomas Rona, prepared for the U.S. Department of Defense in 1976.⁷ This report identified the information sphere as a vulnerable target for potential enemy attacks. At that time, information attacks were

considered primarily within the economic sphere; however, over time, their impact expanded to encompass virtually all areas of human activity. The authorship of the term is often contested, as journalist Dale Minor had already published the book *Information War* in 1970 (Minor, 1970). Nevertheless, it was T. Rona’s work that contributed to the popularization of the concept as a significant phenomenon.

The evolution of information confrontation in recent decades has moved from the technical to the axiological and anthropological sphere. In the contemporary world, there is an increasing emphasis on the mentality of peoples, their identity, self-consciousness, collective memory (including collective trauma), and ideology. In this regard, in the twenty-first century, information-psychological confrontation has become an important instrument of interstate interaction, employed to achieve objectives through non-kinetic (non-physical) forms of influence characteristic of modern warfare.

Within the framework of information-psychological confrontation, information-ideological confrontation is employed, wherein the uniqueness of a nation and the foundation of its spiritual existence become key targets of influence. According to I.F. Kefeli and N.A. Komleva, the information-ideological space has now become the primary arena of struggle, as such actions are covert in nature and are not perceived by society as acts of aggression. On the contrary, the aggressor nation “gently encourages” the target nation to transform itself and to follow an ascending path of development. In Western rhetoric, the terminology of the “Second” and “Third World” is still used, implying the backwardness of the rest of the world and the necessity of adhering to Western models of development. This approach is increasingly criticized even within the West itself as a form of perpetuating colonial thinking.⁸

⁷ Rona T. *Weapon Systems and Information War*. Office of the Secretary of Defense, Washington, DC. July 1, 1976. URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf (accessed: 10.01.2025).

⁸ Silver M. *Memo to People of Earth: ‘Third World’ Is an Offensive Term!* // NPR. January 8, 2021. URL: <https://www.npr.org/sections/goatsandsoda/2021/01/08/>

Moreover, “the principal ‘weapon’ of information-ideological wars is the set of evaluative worldviews, or ideological, constructs deliberately created to justify the expansion of a given geopolitical actor and to condemn the expansion of the opposing actor(s)” (Kefeli & Komleva, 2019, p. 57). This policy is characteristic of the United States, which has consistently justified its presence in various regions of the world, its support for “color revolutions,” and its interference in the internal affairs of sovereign states.⁹ However, when Russia launched a special military operation (SMO) in Ukraine in 2022, the United States and its allies were among the first to condemn these actions, highlighting the existence of double standards in international politics.¹⁰

Military analyst A.A. Bartosh (2024) argues that information confrontation, as a key element of hybrid warfare, was initiated by the United States with the aim of preserving a unipolar world order and maintaining its hegemony on the international stage. Within the framework of the first stage of achieving global dominance, the destruction of Russia is envisioned through the elimination of its statehood, fragmentation, and the establishment of external governance. The next step is identified as establishing control over China, followed by influence exerted on India and other Eurasian states. A similar logic is reflected in the official strategic documents of the United States, where Russia and China are designated as primary threats and competitors to be contained within the framework of global rivalry. Such documents directly or indirectly articulate objectives aimed at limiting the influence of non-systemic actors and maintaining

U.S. global leadership through hybrid and informational means.¹¹

New technologies, including information and communication technologies, have become the basis for protecting the national interests of the United States, as explicitly stated in the country’s national military strategy.¹² Information confrontation with Russia is conducted in accordance with the concept of *strategic communication*, which was actively developed within NATO structures and was formalized in the final communiqué of the Warsaw Summit in 2016 as an element of political and informational pressure.¹³ The term is directly mentioned among the priority areas for strengthening the Alliance’s ability to counter external challenges and shape favorable perceptions of its agenda. The economic and political weakening of Russia, the loss of its subjectivity, the erosion of traditional values, the destabilization of the internal situation, and other objectives have been identified as priorities. The conduct of information operations by the U.S. military command is considered the principal means of maintaining dominance in the information domain. Key methods include the dissemination of false information, the manipulation of facts, the creation of fake news, the suppression of important information, and the

954820328/memo-to-people-of-earth-third-world-is-an-offensive-term (accessed: 19.01.2025).

⁹ GT Investigates: US Wages Global Color Revolutions to Topple Govts // Global Times. December 30, 2021. URL: <https://www.globaltimes.cn/page/202112/1240540.shtml> (accessed: 19.01.2025).

¹⁰ War in Ukraine // Council on Foreign Relations. April 14, 2025. URL: <https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine> (accessed: 19.04.2025).

¹¹ See: 2022 National Defense Strategy of the United States of America. U.S. Department of Defense, 2022. URL: <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf> (accessed: 19.01.2025); Renewed Great Power Competition: Implications for Defense — Issues for Congress. Congressional Research Service. August 28, 2024. URL: <https://sgp.fas.org/crs/natsec/R43838.pdf> (accessed: 19.01.2025).

¹² Description of the National Military Strategy 2018 // Office of Primary Responsibility: Strategy Development Division, Deputy Directorate for Joint Strategic Planning, Directorate for Strategy, Plans, and Policy (J-5). The Joint Chiefs of Staff. 2018. URL: https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf (accessed: 06.01.2025).

¹³ Warsaw Summit Communiqué // NATO. July 9, 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed: 07.01.2025).

emphasis on secondary aspects in order to disorient and mislead the target audience. To implement this strategy, the *NATO Strategic Communications Centre of Excellence* operates in Latvia, along with various anti-Russian non-governmental organizations (NGOs) such as the “*Soros Foundation*,”¹⁴ *Freedom House*,¹⁵ and others. Among NATO’s most immediate priorities are the formation of a negative image of Russia as the primary threat to NATO and European Union’s countries, the isolation of Russia on the global stage, the reduction of Russia’s influence in the post-Soviet space, including the Commonwealth of Independence States (CIS), and the maintenance of a policy of strategic deterrence with minimal dialogue with Moscow.¹⁶

In the Anglo-American world, the concept of “malign Russian influence” is widely used. Doctor of Political Sciences D. Proroković observes that this concept was deliberately introduced and disseminated by the United States in order to ensure comprehensive informational pressure on Russia. The researcher emphasizes that “Any action involving a Russian state institution, state corporation, or organization (whether non-governmental, scientific, or religious) can be classified as malign Russian influence” (Proroković, 2021, pp. 82–83). References to “malign Russian influence” allow the United States to use this notion as a pretext for justifying its actions, including those of questionable legitimacy.

¹⁴ The activities of foreign non-governmental organizations funded by the “Soros Foundation” — the Open Society Foundations and the OSI Assistance Foundation — have been recognized as undesirable on the territory of the Russian Federation (*Editor’s note*).

¹⁵ The activities of the international non-governmental organization *Freedom House* have been recognized as undesirable on the territory of the Russian Federation (*Editor’s note*).

¹⁶ Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Adopted on June 29, 2022 // NATO. 2022. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (accessed: 09.01.2025).

According to E.A. Danilova and E.D. Zabolotnaya, information warfare poses not only threats and risks, but also opportunities, particularly those associated with Russia’s transition from a defensive posture to an offensive one (Danilova & Zabolotnaya, 2023). Professor A.V. Manoylo argues that Russia should seek equal competition with the United States in the sphere of information confrontation and provides detailed descriptions of manipulative strategies used against adversaries, advocating for the adoption of similar approaches to strengthen Russia’s own positions (Manoylo, 2021, p. 94).

Doctor of Political Sciences I.A. Vasilenko posits that contemporary Russia should allocate greater attention to the policy of building a positive image on the international arena (Vasilenko, 2014). The researcher emphasizes that the hostility of the West contributed to the strengthening of Russia’s eastern orientation, as the necessary foreign policy support was found in the BRICS countries, the Shanghai Cooperation Organization (SCO), and the Eurasian Economic Union (EAEU). At present, the Russian Federation is independently shaping the international agenda, including in the field of information security. Within the BRICS framework, Russia is proactively advocating for the establishment of norms of state behavior in cyberspace, intended to protect national interests and strengthen digital sovereignty. Russia’s participation in shaping regulatory approaches in the information domain is examined in the academic literature addressing legal regimes of cybersecurity (Ramich & Piskunov, 2022).

Artificial Intelligence as a Tool of Information Warfare

Artificial Intelligence can be defined as a set of technologies based on data processing algorithms that simulate human analytical and cognitive abilities. The significance of AI in information warfare lies in its ability to generate, adapt, and manipulate information on a scale previously unattainable by any other tool or

method. AI technologies serve simultaneously as a resource and a weapon. They facilitate the processing of large volumes of data and the identification of complex interconnections between elements of information, which would be impossible using traditional methods. AI is being used in forecasting, managing mass consciousness, and influencing public perception.

AI technologies possess significant constructive potential; however, they also generate additional risks that intensify the information confrontation. For instance, they are actively used to produce propaganda content. Notably, the effectiveness of such methods of confrontation results from the activation of the principle that “demand creates supply.” In other words, the demand for fast and diverse information generates its production. Such information is generally easy to perceive, requires minimal effort for collection and analysis (as it reaches the audience in a ready-made form), and appears engaging and attractive (Goldstein, Sastry & Musser, 2023, p. 65). Thus, one way to counter propaganda facilitated by AI technologies is to meet society’s demand for genuine awareness.

It can thus be concluded that the primary threat does not stem from AI technologies themselves, but rather from their malicious use, which poses a danger to international information-psychological security (Pashentsev, 2019). The main methods of employing AI technologies in information confrontation include the creation of deepfakes (“deep learning” + “fake”), agenda-setting and reinforcement, targeted image transformation, the “poisoned data” technique, sentiment analysis in texts, the “fake people” technique, and others.

AI technologies are highly effective in targeting audiences, directing information attacks toward specific population groups, taking into account their cultural, political, and social characteristics. The precision of such influence is enhanced through the use of deep learning technologies, which enable the modeling of probable reaction scenarios to informational

stimuli. AI systems have the capacity to analyze the behavior of social media users, correlating their interests, behavioral patterns, and emotional responses to create personalized content that maximally impacts their perception and actions. AI is not merely a tool of influence; it is also a factor that governs the dynamics of the information field in real time.

Researchers D.Yu. Bazarkina and E.N. Pashentsev note that the negative effects of AI use and its impact on information-psychological security have not yet been sufficiently studied (Bazarkina & Pashentsev, 2019, p. 149). In their joint study, the scholars identified several factors that complicate efforts to minimize the damage caused by the malicious use of AI technologies. These factors include the ongoing geopolitical confrontation (the lack of consensus among global actors on achieving an acceptable level of security), social instability resulting from economic crises, distrust toward state institutions and political parties, competition between humans and AI in the employment sector (leading to increased unemployment), and several others. It is thus clear that the use of AI to disrupt security, including in the area of information-psychological security, is complex in nature, overlapping with traditional challenges and creating qualitatively new threats.

The automation of data processing and content creation processes enables AI to operate in real time, creating the effect of mass support or resistance, which significantly enhances its influence on public consciousness. The decentralized nature of such systems virtually eliminates the possibility of neutralizing them through traditional methods of countering disinformation. Moreover, AI technologies ensure the coordination of actions on a global scale, which in turn opens up opportunities for organizing information campaigns aimed at destabilizing various regions. AI-based technological solutions are characterized not only by their considerable complexity but also by their close interconnection with social and psychological processes, making them a powerful tool for influencing mass

consciousness. The technology of *deepfake* is particularly effective in this regard, as it effectively replaces physical reality with fabricated images.

The use of AI in the context of information confrontation represents not only a technological innovation but also a significant cultural challenge, altering perceptions of truth, credibility, and objectivity. The development of such technologies highlights the need to rethink methods of ensuring information security and to develop new approaches to managing information flows.

AI tools are not limited to performing predefined functions; they possess the capacity to adapt to changes in the information environment. The ability to adapt is critically important amid the rapid changes occurring in global information structures, where events unfold dynamically, and timely responses require the use of all available resources.

The evolution of AI technologies has led to the emergence of new forms of “informational autonomy,” wherein systems independently make decisions regarding the nature and content of the information they disseminate. Autonomous processes encompass not only the generation of content but also the selection of the most effective methods for its delivery. AI functions as a strategic agent, setting priorities and adjusting the direction of informational influence based on changing circumstances. These new capabilities thus expand the potential for information confrontation, while simultaneously raising serious ethical and legal questions.

The nature of AI technologies in the information confrontation is characterized by dynamism, adaptability, and the capacity to transform fundamental approaches to working with information. These technologies not only accelerate and simplify the creation and distribution of content, but also alter the way in which information influences public consciousness and political processes. Consequently, new rules of interaction are being established on a global scale.

Information Warfare amid the Formation of a Multipolar World

At present, threats to the information-psychological security of leading non-Western countries have emerged, associated with the use of advanced technologies (including AI). The consequences of their application can be catastrophic for psychological security (Pantserev, 2020). According to D.Yu. Bazarkina and E.N. Pashentsev, psychological damage caused by the use of AI technologies constitutes the third and most dangerous level of threat (the first level involves the spread of a false negative image of AI, and the second level involves the direct malicious use of AI without the goal of influencing public consciousness, for instance, the use of unmanned aerial vehicles (UAVs) in enemy territory or the theft of money through AI technologies) (Bazarkina & Pashentsev, 2020, p. 162). The discrediting of reliable systems (such as multi-level protection systems for banking applications and accounts), the emergence of uncertainty, and the absence of action algorithms in situations where AI technologies are used to undermine information-psychological security inflict serious harm on societies subjected to such attacks.

One of the most striking manifestations of the information-technical warfare amid the formation of a multipolar world has been the technological and informational rivalry between the United States and China, developing according to the logic of *decoupling*. While *coupling* — the idea of “connection” — symbolized globalization at the end of the twentieth century, in the twenty-first century, the reverse process, *decoupling* — “disconnection” — has come to the forefront, most clearly manifested in U.S. — China relations during the first presidential term of Donald Trump (2017–2021). As emphasized by Ya.V. Leksyutina, China’s actions — cyberespionage, the activity of telecommunications companies, and investments in the U.S. economy — were perceived in the USA as a threat to national security, which served as the basis for the formation of a course

in Washington aimed at technological and informational distancing from Beijing (Leksyutina, 2020, p. 86).

The sanctions pressure, which escalated after the start of Russia's special military operation in Ukraine (since 2022), accelerated the rupture of global production and logistics chains, as well as informational ties. The previously proclaimed mutually beneficial cooperation has now been perceived as a strategic vulnerability. In the evolving architecture of international relations, interdependence is increasingly regarded as a risk factor not only in the economic sphere but also in the ideological and technological domains. The phenomenon of "decoupling" is taking on the features of a kind of "parade of sovereignties" of the twenty-first century, reflecting the desire of states to construct autonomous development trajectories. Donald Trump's return to power in 2025 predetermines the further expansion of the protectionist agenda: even before taking office, he announced plans to impose tariffs on goods from China, the BRICS countries, and the European Union (Vinogradov, Salitsky & Semenova, 2019, p. 42).

The U.S. — China confrontation in the field of high technologies has acquired the character of a protracted conflict. Under the administration of Barack Obama, the first steps were implemented to contain China through sanctions mechanisms, and under Donald Trump, the confrontation escalated into a full-fledged "technological war" (Danilin, 2020, p. 161). The United States imposed strict restrictions on major technology giants such as *Huawei* and *ZTE*, curtailed academic cooperation, and tightened control over the export of critical components. In response, China accelerated its domestic digital modernization and established partnerships with other countries, including those in European Union, Japan, Russia, Israel, and a number of developing states.

As a result, two distinct autonomous spaces are emerging on the global technological map: the first under the leadership of the United States, and the second characterized by the

growing influence of China (Vykhodets, 2022, pp. 262–263). Russia is orienting itself toward the eastern vector, seeking to compensate for the losses caused by the rupture with Western technology suppliers such as *Intel*, *AMD*, and semiconductor manufacturers from Taiwan (China). Developing countries, deprived of access to advanced digital components, are becoming particularly vulnerable under the evolving conditions. The struggle for leadership in the sphere of Technologies 4.0 is becoming not only an economic but also a political priority. States that possess technological sovereignty gain advantages in both industry and in the defense sector, including through the use of artificial intelligence in military developments.

It should be noted that in China, issues of information and technological confrontation are being actively developed within the academic community. The primary focus of this article is placed on the strategic initiatives of the United States and their impact on the global balance. A detailed examination of Chinese theoretical approaches requires a separate study.

Although the United States is the principal ideologist and actor in the contemporary information warfare, it views Russia, China, Iran, and several other non-Western states as revisionist powers conducting warfare in the so-called "grey zone," where the states of peace and war are indistinguishable and covert actions carried out through advanced information technologies enable the achievement of political objectives (Azad, Haider & Sadiq, 2023, p. 95). Information technologies, despite being "immaterial" instruments, produce tangible, material consequences. A notable illustration of this phenomenon was the series of events that came to be known as the "*Twitter*"¹⁷ revolutions," which had a significant impact on a number of countries in the Middle East and North Africa (Tatunts, 2024, p. 4).

Russia recognizes the threat of informational influence; therefore, the "Foreign

¹⁷ The social network *Twitter* (now *X*) was blocked by Roskomnadzor of the Russian Federation in 2022 (*Editor's note*).

Policy Concept of the Russian Federation” of 2023 emphasizes the importance of creating and developing a secure information space to protect the population from destructive foreign information-psychological influence. A significant step forward has been the open official identification of adversaries by name, which has been reflected in conceptual documents.¹⁸

As the methods of information confrontation continue to evolve, Russia must also respond promptly to emerging threats. A joint study by A. Ventsel, S. Hansson, M.-L. Madisson, and V. Sazonov examines the use of the culture of fear is examined through the example of Russia’s “Zapad 2017” military exercises near the borders of Belarus. According to the researchers, Russia actively uses the amplification of fear to achieve strategic objectives, which they see as a manifestation of information confrontation. “Uncertainty is an important source of fear,” the article states (Ventsel et al., 2019, p. 28). This, according to the authors, constitutes Russia’s principal advantage and objective. The article was written before the start of the special military operation, thus the fear (since 2014, Russia had insisted on the cessation of unlawful actions in Donbass by the Kiev authorities) ultimately materialized at a critical moment, with a warning that had long remained at the level of fear becoming a reality.

From our perspective, such a perception of Russia’s policy by its adversaries may yield positive results for Russia, especially since a precedent has already been established. It is important, however, that the opposing side perceives the warning not merely as an element of information confrontation or “military games,” but precisely as an expression of intent. In this regard, the assertion of A.V. Fenenko,

professor at the Faculty of World Politics of the Lomonosov Moscow State University, is justified: information warfare between states is possible only if both sides recognize each other’s authority. Otherwise, the act of communication becomes impossible.¹⁹ In the case of Ukraine, the warnings did not have the desired effect, which unfortunately led to the cultivation of fears about nuclear strikes in the informational space and, at the highest state level, to a shift in the nuclear doctrine.²⁰ Indeed, Russia’s adversaries must take it seriously and regard its intentions with due gravity. It is possible that for Russia, a winning strategy in the information confrontation could involve cultivating a culture of fear, whereby merely an informational signal from Russia would be sufficient to instill apprehension regarding its potential actions.

Cognitive warfare enables an individual to serve simultaneously as both the object and the subject of informational influence within the framework of information confrontation. The individual is both a recipient of information and a disseminator thereof. This blurs the boundary between the addressee and the sender, meaning that virtually any user can become an opinion leader. Since the beginning of the special military operation, a number of new social bot accounts have appeared on the social network *X* (formerly *Twitter*). For example, the account *@UAWeapons*, which posted biased messages aimed at discrediting Russia, gained several hundred thousand followers within just one month (Li et al., 2023, p. 69). This also highlights the problem of the lack of accountability for the spread of information, as the depersonalized nature of news publications

¹⁸ Decree of the Government of the Russian Federation No. 430-r of March 5, 2022 (ed. October 29, 2022) “On Approval of the List of Foreign States and Territories Committing Unfriendly Acts Against the Russian Federation, Russian Legal Entities and Individuals” // ConsultantPlus. (In Russian). URL: https://www.consultant.ru/document/cons_doc_LAW_411064/e8730c96430f0f246299a0cb7e5b27193f98fdaa/ (accessed: 02.11.2024).

¹⁹ Fenenko A. The Paradox of Information Wars // Russian International Affairs Council. August 17, 2022. (In Russian). URL: <https://russiancouncil.ru/analytics-and-comments/analytics/paradoks-informatsionnykh-voyn/> (accessed: 07.01.2025).

²⁰ Decree of the President of the Russian Federation No. 991 of November 19, 2024 “On Approval of the Fundamentals of the State Policy of the Russian Federation in the Field of Nuclear Deterrence” // President of Russia. (In Russian). URL: <http://www.kremlin.ru/acts/bank/51312> (accessed: 06.01.2025).

amplifies the manipulative effect of such messages.

Since 2022, there has been a growing tendency to divide the world's leading countries into "friends" and "foes"; however, states such as India and China have declared their neutrality.²¹ Such a position causes dissatisfaction in the West for several reasons: first, it reflects the independence of other actors; second, countries adhering to these principles do not share liberal values; and third, the ambiguity of their stance makes them potential partners of Russia. It is highly likely that states outside the Western bloc will continue to build a more equitable model of the world order and strengthen cooperation in the field of information technologies to counter pressure from the collective West. For Russia, these developments present a range of opportunities, including the formation of stable digital alliances, the promotion of alternative norms of international information interaction, and the strengthening of its role as a coordinator in the field of global information security.

Conclusion

Today's world and the relationships between global actors are characterized by flexibility, fragmentation, and pronounced manipulateness. Leading international players continue to seek to expand their geopolitical influence, but the means by which they do so have changed radically. The centers of power are undergoing a rapid transformation, and information confrontation is becoming, on the one hand, a tool for small and previously marginalized states to assert their interests on the international stage, and on the other hand, a source of destabilization that threatens the formation of a multipolar world.

²¹ China's Position on Russia's Invasion of Ukraine // U.S. — China Economic and Security Review Commission. February 28, 2025. URL: <https://www.uscc.gov/research/chinas-position-russias-invasion-ukraine> (accessed: 18.03.2025).

While information confrontation is only one element in the broader spectrum of global threats — alongside currency and financial pressure, military-political dominance, and sanctions policy — it is distinguished by its covert nature, limited predictability, and weak accountability. In the absence of clear international regulations and control mechanisms, manipulative influences within the information sphere take on a destructive character. For example, the United States employs this form of confrontation not to impose a universal liberal-democratic model, but as a tool to weaken non-Western centers of power capable of challenging American hegemony. The protectionist policies pursued by the administration of Donald Trump, the technological superiority of the United States, and the existence of competing actors, including China, are likely to intensify the information confrontation in the near future.

The relevance of the topic indicates the necessity for additional research in the field of strategic analysis of information confrontation. Future scientific research may focus on the following areas: mechanisms of interaction between states resisting the restoration of the unipolar world order and external informational pressure; information confrontation as an element of the United States' hybrid strategy toward non-Western countries; analysis of informational influence on Russia, China, India, Brazil, Arab states, and others; the evolution of Russia's model of information confrontation, transitioning from defensive to offensive strategies; new forms and methods of conducting information confrontation; and changes in the international security system under the influence of information-psychological and information-technological impacts. The expansion of research in these areas will facilitate a more precise delineation of the role and function of information confrontation as a key dimension of global competition in the context of a multipolar world.

Received / Поступила в редакцию: 03.11.2024

Revised / Доработана после рецензирования: 28.01.2025

Accepted / Принята к публикации: 20.03.2025

References

- Azad, T. M., Haider, M. W., & Sadiq, M. (2023). Understanding gray zone warfare from multiple perspectives. *World Affairs*, 186(1), 81–104. <https://doi.org/10.1177/00438200221141101>; EDN: YPIWZD
- Bartosh, A. A. (2024). *Global hybrid warfare*. Moscow: Goryachaya liniya-Telekom publ. (In Russian).
- Bazarkina, D. Yu., & Pashentsev, E. N. (2019). Artificial intelligence and new threats to international psychological security. *Russia in Global Affairs*, 17(1), 147–170. <https://doi.org/10.31278/1810-6374-2019-17-1-147-170>; EDN: FYAQFW
- Bazarkina, D. Yu., & Pashentsev, E. N. (2020). Malicious use of artificial intelligence. *Russia in Global Affairs*, 18(4), 154–177. <https://doi.org/10.31278/1810-6374-2020-18-4-154-177>; EDN: ZZANTF
- Castells, M. (2000). *The information age: Economy, society, and culture*. Moscow: GU VShE publ. (In Russian).
- Clarke, R., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: Ecco.
- Danilin, I. V. (2020). The U.S. — China technology war: Risks and opportunities for P.R.C. and global tech sector. *Comparative Politics Russia*, 11(4), 160–176. EDN: GYRYVR
- Danilova, E. A., & Zabolotnaya, E. D. (2023). Political PR technologies in the information warfare between Russia and the West amid the military-political conflict in Ukraine: New challenges and opportunities for Russia. *Vlast'*, 31(2), 56–63. <https://doi.org/10.31171/vlast.v31i2.9528>; EDN: XYKPLA
- Goldstein, J., Sastry, G., Musser, M., DiResta, R., Gentzel, M., & Sedova, K. (2023). *Generative language models and automated influence operations: Emerging threats and potential mitigations*. Ithaca, NY: Cornell University. <https://doi.org/10.48550/arXiv.2301.04246>
- Goncharova, I. V., Nicevich, V. F., & Sudorgin, O. A. (2024). Information warfare as a tool of political confrontation in the modern multipolar world. *RUDN Journal of Public Administration*, 11(1), 19–31. <https://doi.org/10.22363/2312-8313-2024-11-1-19-31>; EDN: ZIXNDI
- Hoyle, A., van den Berg, H., Doosje, B., & Kitzen, M. (2021). Grey matters: Advancing a psychological effects-based approach to countering malign information influence. *New Perspectives*, 29(2), 144–164. <https://doi.org/10.1177/2336825X21995702>; EDN: VKURAA
- Ilitsky, A. M. (2021). Mental warfare in Russia. *Voennaya Mysl'*, (8), 19–33. (In Russian). EDN: TDSKIX
- Kefeli, I. F., & Komleva, N. A. (2019). On the role of information and ideological security in the counter-strategy hybrid war in Eurasia. *Eurasian Integration: Economics, Law, Politics*, (1), 54–60. (In Russian). EDN: NAHPIC
- Leksyutina, Ya. V. (2020). U.S. — China relations in 2018–2019: Trade war and the process of decoupling. *World Economy and International Relations*, 64(6), 85–93. <https://doi.org/10.20542/0131-2227-2020-64-6-85-93>; EDN: QRYEBK
- Li, Q., Liu, Q., Liu, S., Di, X., Chen, S., & Zhang, H. (2023). Influence of social bots in information warfare: A case study on @UAWeapons Twitter account in the context of the Russia — Ukraine conflict. *Communication and the Public*, 8(2), 54–80. <https://doi.org/10.1177/20570473231166157>; EDN: BWKLRB
- Linebarger, P. (1962). *Psychological warfare*. Moscow: Voenizdat publ. (In Russian).
- Manoylo, A. V. (2019). Fake news as a threat to national security and as a tool of information management. *Vestnik Moskovskogo Universiteta. Seriya 12: Politicheskie Nauki*, (2), 37–45. (In Russian). EDN: HGEVPF
- Manoylo, A. V. (2021). Evolution of information operations. *Bulletin of Moscow Region State University*, (4), 80–103. <https://doi.org/10.18384/2224-0209-2021-4-1100>; EDN: MVAJGI
- Minor, D. (1970). *Information war*. Boston: Hawthorne Books Publishing House.
- Ördén, H. (2024). The neuropolitical imaginaries of cognitive warfare. *Security Dialogue*, 55(6), 607–624. <https://doi.org/10.1177/09670106241253527>; EDN: HIWMNY
- Pantserev, K. A. (2020). The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability. In H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, J. Ibarra (Eds.), *Cyber defence in the age of AI, smart societies and augmented humanity* (pp. 37–55). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-35746-7_3; EDN: IQCSJW
- Pashentsev, E. N. (2019). Malicious use of artificial intelligence: New threats to international psychological security and ways to neutralize them. *E-Journal Public Administration*, (76), 279–300. (In Russian). <https://doi.org/10.24411/2070-1381-2019-10013>; EDN: CVLXTW
- Pozdnyakov, A. I., & Shevtsov, V. S. (2017). Methodological basis of creation of the theory of information antagonism. *Sotsial'no-Gumanitarnye Znaniya*, (2), 244–257. (In Russian). EDN: YJYGXD
- Proroković, D. (2021). A Western attempt to portray Russia as an enemy (about the concept of Russian malign influence). *Vestnik Moskovskogo Universiteta. Seriya 12: Politicheskie Nauki*, (2), 72–85. (In Russian). EDN: LPTWIL

- Ramich, M. S., & Piskunov, D. A. (2022). The securitization of cyberspace: From rulemaking to establishing legal regimes. *Vestnik RUDN. International Relations*, 22(2), 238–255. <https://doi.org/10.22363/2313-0660-2022-22-2-238-255>; EDN: KSSXFK
- Tatunts, S. A. (2024). Formation of a multipolar world order under the conditions of a global information confrontation. *Information Society*, (3), 2–9. (In Russian). EDN: TRSYZC
- Vasilenko, I. A. (2014). Formation of the new image of Russia “after Crimea”: Paradoxes of information war. *Vlast*, (10), 204–208. (In Russian). EDN: SXSXCZ
- Ventsel, A., Hansson, S., Madisson, M.-L., & Sazonov, V. (2019). Discourse of fear in strategic narratives: The case of Russia’s Zapad war games. *Media, War & Conflict*, 14(1), 21–39. <https://doi.org/10.1177/1750635219856552>
- Vinogradov, A. O., Salitsky, A. I., & Semenova, N. K. (2019). U.S. — China economic confrontation: Ideology, chronology, meaning. *Vestnik RUDN. International Relations*, 19(1), 35–46. (In Russian). <https://doi.org/10.22363/2313-0660-2019-19-1-35-46>; EDN: ZBFCZN
- Vykhodets, R. S. (2022). Large AI spaces and Russia’s strategy in the context of the “sanctions war”. *Vestnik RUDN. International Relations*, 22(2), 256–270. <https://doi.org/10.22363/2313-0660-2022-22-2-256-270>; EDN: FYNYWU
- Vykhodets, R. S., & Pantserev, K. A. (2022). Comparative analysis of modern concepts of information warfare. *Eurasian Integration: Economics, Law, Politics*, 16(4), 139–148. <https://doi.org/10.22394/2073-2929-2022-04-139-148>; EDN: SVTUJU

About the authors:

Bazavluk Sergei Viktorovich — PhD (Political Science), Head, International Scientific Exchange Programs, National Research Institute for the Development of Communications (NIIRK); eLibrary SPIN-code: 3560-9701; ORCID: 0000-0002-9739-2594; e-mail: bazavluk@nicrus.ru

Kovalev Andrei Andreevich — PhD (Political Science), Associate Professor, Department of Public and Municipal Administration, North-West Institute of Management — Branch of the Russian Presidential Academy of National Economy and Public Administration (RANEPA); eLibrary SPIN-code: 1380-8790; ORCID: 0000-0002-7760-5732; e-mail: kovalev-aa@ranepa.ru