УДК 327.8-042.4:004
DOI 10.20339/AM.02-26.108

Javlon A. Abdurasulov,
Research fellow
University of World Economy and Diplomacy, Uzbekistan
https://orcid.org/0009-0006-1553-1471
e-mail: abdurasulovj1402@gmail.com
Dinora Ruzimboyeva,
Student
University of World Economy and Diplomacy, Uzbekistan
https://orcid.org/0009-0002-4282-3673
e-mail: rozimboyevadinora268@gmail.com

INFORMATION WARFARE AND ITS PROSPECTS IN THE CONTEXT OF GLOBALIZATION:
THE CASE OF THE UNITED STATES AND CHINA

This article examines the emergence of the concept of information warfare within the context of globalization processes and analyzes its role in international relations. As one of the key instruments of geopolitical competition in the 21st century, information warfare is gaining increasing significance in the political, economic, and military strategies of states. The article explores the fundamental features of modern information warfare through the example of the informational rivalry between the United States and the People's Republic of China (PRC). In particular, it analyzes the cyber strategies of these states and their interactions in the international arena. Furthermore, the study focuses on the forms and methods of information operations conducted through cybersecurity measures, disinformation campaigns, artificial intelligence, and media platforms. The research employs comparative, analytical, analogical, and retrospective methods to evaluate the strategic approaches of both countries toward achieving 'information superiority' from various perspectives.

Keywords: *information warfare, cybersecurity, artificial intelligence, information environment , globalization, information security, cyberattack, information manipulation, strategic communication, geopolitics, cyberspace, military technologies, sovereignty, media control*

ИНФОРМАЦИОННАЯ ВОЙНА И ЕЕ ПЕРСПЕКТИВЫ В КОНТЕКСТЕ ГЛОБАЛИЗАЦИИ:
ПРИМЕР СОЕДИНЕННЫХ ШТАТОВ И КИТАЯ

Джавлон А. Абдурасулов, научный сотрудник Университета мировой экономики и дипломатии, Узбекистан, https://orcid.org/0009-0006-1553-1471, e-mail: *abdurasulovj1402@gmail.com*
Динора Рузимбоева, студентка Университета мировой экономики и дипломатии, Узбекистан, https://orcid.org/0009-0002-4282-3673, e-mail: *rozimboyevadinora268@gmail.com*

В данной статье рассматривается возникновение концепции информационной войны в контексте процессов глобализации и анализируется ее роль в международных отношениях. Как один из ключевых инструментов геополитической конкуренции XXI века, информационная война приобретает всё более важное значение в политических, экономических и военных стратегиях государств. В статье исследуются основные особенности современной информационной войны на примере информационного соперничества между Соединенными Штатами Америки и Китайской Народной Республикой (КНР). В частности, анализируются киберстратегии этих государств и их взаимодействие на международной арене. Кроме того, внимание уделено формам и методам информационных операций, осуществляемых посредством мер кибербезопасности, дезинформационных кампаний, искусственного интеллекта и медиаплатформ. В исследовании используются сравнительный, аналитический, аналоговый и ретроспективный методы для оценки стратегических подходов обеих стран к достижению «информационного превосходства» с различных точек зрения.

Ключевые слова: *информационная война, кибербезопасность, искусственный интеллект, информационная среда, глобализация, информационная безопасность, кибератака, информационная манипуляция, стратегическая коммуникация, геополитика, киберпространство, военные технологии, суверенитет, контроль над медиа.*

Introduction

In the current era, where globalization processes are encompassing all spheres of human life, the information environment has become a central arena of geopolitical competition among states. In particular, the information confrontation between the United States and the People's Republic of China is shaping a new balance of power within the international political system of the 21st century. This article explores the formation of the concept of information warfare under the conditions of globalization, its geopolitical significance, and the informational strategies of both states, while also highlighting the implications of these processes for international security and the future of the cyber domain. Moreover, according to our research, information warfare as an integral compo-

nent of globalization exerts profound influence not only on military affairs but also on political, economic, and cultural spheres. The informational rivalry between the United States and the PRC manifests itself as a complex, multifaceted geopolitical process that contributes to the emergence of a new power configuration within the international security system.

Globalization

Globalization (from the Latin 'globus' — sphere, planet) is a concept that describes the emergence of new global structures in world development during the second half of the 20th century and the early 21st century. It reflects the expansion and intensification of interactions among states and individuals; the integration of the global information space, capital, goods, and labor markets; the increasing technogenic impact on the environment; the widespread diffusion of mass culture; and the growing risks associated with informational-ideological and religious-extremist threats.

The term 'globalization' was first mentioned by the American scholar T. Levitt in his 1983 article published in Harvard Business Review, where he used it to describe the process of unifying diverse product markets created by major transnational corporations[1]. Later, in 1985, the prominent American sociologist R. Robertson introduced the term 'globalization' into academic discourse, defining it as a process that reflects "the compression of the world and the intensification of global interconnectedness among people"[2].

Although debates regarding the essence and scope of this term are still ongoing, a unified interpretation or a comprehensive conceptual framework has yet to be fully established. Nevertheless, various branches of the social sciences continue to thoroughly examine the distinctive features and manifestations of globalization.

In economics, attention is primarily focused on issues such as financial globalization, the growing influence of transnational corporations, regional economic integration, and the acceleration of global trade. Historical research, on the other hand, views globalization as one of the stages of human development that extends back through many centuries.

In political science, scholars study the intensification of transnational processes, the strengthening of interdependence among states, and the emergence of a new global order shaped by the activities of the United Nations and other international organizations. Meanwhile, in sociology, researchers explore evidence confirming the convergence and homogenization of lifestyles across different regions as a result of cultural universalization.

We found it necessary to expand on T. Levitt's views. In our opinion, globalization can be understood as the development of cooperation in any field without regard to borders, territories, or nationalities. According to our analysis, globalization can be considered to have reached its peak only when a set of universal values is established worldwide.

Information warfare

The term "information warfare" was first used in 1976 by T. Ron in a document prepared for the Boeing Company. Since 1992, the term has been officially used by the United States Department of Defense[3]. The diversity of scientific approaches studying informational-psychological confrontation and cyber warfare indicates the absence of a single, unified perspective on the phenomenon. Currently, the scholarly literature identifies the following main approaches: geopolitical, psychological, communicative, and conflictological[4].

According to the geopolitical approach, information warfare is a form of strategic confrontation between states. Within this framework, states utilize information resources to influence adversary countries and strive to achieve superiority in critical areas. Today, the competition between the United States and the People's Republic of China (PRC) serves as a clear example of geopolitical information warfare. Studies indicate that the United States primarily employs information warfare to protect democratic values, ensure national security, and counter cyber threats. In contrast, China uses its information strategy as a means to expand its global influence, promote its political model, and create a balance against the information dominance of the West.

According to proponents of the psychological approach, the core essence of information warfare lies in covertly influencing the public consciousness through information. As V.A. Lisichkin emphasized, the manipulation of thought is the hidden implementation of informational influence aimed at controlling intellectual-psychological and socio-cultural processes, in a manner that the targets do not perceive[5]. We support this perspective. The formation of opinions plays a crucial role in portraying states as allies or adversaries on the international stage.

From a constructivist perspective, understanding this phenomenon contributes to the effectiveness of our research. According to Alexander Wendt, a representative of

[1] Oyina.uz Globallashuv https://oyina.uz/uz/teahause/1482
[2] Ibid.
[3] Factcheck.uz Axborot xavfsizligi https://factcheck.uz/?p=5507
[4] Ibid.
[5] Ibid.

the Constructivist school in political science, a state's foreign policy is shaped by its "identity" and "beliefs."[6] For example, the perception of the United States and Canada regarding each other as partners rather than adversaries is not determined by geopolitical distance, but by their social relations. In this context, it is not weapons, armies, or economic power per se that matter, but the meanings attached to them. For instance, the nuclear arsenal of the United States may be perceived as a threat by China, but not by the United Kingdom, due to differences in perception and discourse. This constructivist perspective can also be applied to the relationship between the United States and China, where mutual constructions of enmity have emerged between the two states.

In his article "Constructivist Aspects of Contemporary US-India Relations," I. Gafarov, a researcher at UWED, provides a scholarly foundation for understanding how the construction of ideas shapes states' perceptions of each other as friends or adversaries[7]. Similarly, in his study "Internal and external geopolitical factors affecting the formation of international relations in Central Asia," J. Abdurasulov pays particular attention to the geopolitical aspects of China's constructivist policies toward other regions, especially Central Asia[8]. The perspectives of both researchers can be summarized as follows: in international relations, it is not friendship or enmity between states that predominates, but rather the primacy of national interests, which constitutes a crucial factor in the construction of ideas.

In the contemporary world, both states employ information as a strategic tool. The United States pursues a 'soft power' policy through international media, technological platforms, and diplomatic communications. China, on the other hand, seeks to strengthen its ideological and political image through initiatives such as the Digital Silk Road and control mechanisms on social networks. Thus, the information warfare between the United States and the PRC manifests as a complex process at the intersection of geopolitical and psychological factors. In the words of Joseph Nye, this demonstrates that a state's power can be exercised not only through military or economic means but also through cultural, political, and ideological influence[9].

In our view, information warfare is primarily conducted covertly, in accordance with its objectives and essence. The main reason for this is the gradual inculcation of specific ideas into public consciousness over years. Information wars are not openly declared; rather, they are implemented step by step based on a strategic approach. The precise moment of initiation, conclusion, or the potential strength and consequences of an information war cannot be predetermined. This process typically involves gathering tactical information, disseminating interest-driven content, propaganda, disinformation campaigns, demoralization (leading to moral and ethical degradation), and various manipulation techniques. Thus, the concept of information warfare is no longer limited to propagandistic materials or cyberattacks. It has evolved into a complex strategic process capable of influencing human thought, societal consciousness, and even the formulation of international political decisions. The information rivalry between the United States and the PRC represents a practical manifestation of this process, initiating a new era of 'informational geopolitics' on a global scale. Notably, this competition intensified significantly with Donald Trump's second term as President.

Transformation of the information environment in the Era of Globalization

In the new century, often described as the Information Age, the rapid development of information and communication technologies, particularly the Internet, is creating both new opportunities and risks for human development. It is noteworthy that major economic centers of the West primarily the United States driving the process of globalization, strive to transform the entire world into a "single market for raw materials, consumption, production, and information" that aligns with and serves their geo-economic and geopolitical interests. These processes contribute to the transformation of the information environment, which increasingly serves as a crucial tool in state decision-making and international relations. The transformation of the information space plays a direct role in global diplomatic processes and the formulation of political decisions. For instance, according to research by the Oxford Internet Institute, there are 189 active diplomatic Twitter accounts in China, which play a significant role in disseminating state-affiliated media content to a wide audience[10].

The transformation of the information environment plays a crucial role in political decision-making at any point in the world. The information space is not merely a technological

[6] *Wendt, Alexander.* Social theory of International Politics. (1999). URL: https://www.guillaumenicaise.com/wp-content/uploads/2013/10/Wendt-Social-Theory-of-International-Politics.pdf
[7] *Gafarov, I.* Zamonaviy AQSH-Hindiston munosabatlarining konstruktivsit jihatlari. 2024 b. 8.
[8] *Abdurasulov, J.* Internal and external geopolitical factors affecting the formation of international relations in central Asia (case study of transport corridors and water resources usage). URL: https://almavest.ru/ru/archive/4230/5823
[9] *Nye, J.S.* (2002) Why military power is no longer enough. The Guardian, 2002, March 31.
[10] DemTech / Oxford Internet Institute. "China's Public Diplomacy Operations: Understanding Engagement and Inauthentic Amplification of PRC Diplomats on Facebook and Twitter." Ishchi qog'oz, 2021. P. 15.

tool; it is also regarded as a strategic resource for supporting peace in interstate communication and international relations. Notably, the COVID-19 pandemic has triggered revolutionary changes in the transformation of the information environment. According to our research findings, while ownership of natural resources was traditionally considered the primary determinant of state power, we argue that influence within the information environment should now be regarded as a new strategic resource for ensuring global stability and security.

Approaches to the information environment by the United States and the PRC

The PRC and the United States have developed different approaches and strategies regarding the information environment, each shaped in accordance with the state's political and economic model, strategic objectives, and technological capabilities.

The PRC's "Three Warfares" model treats information, psychological, and legal warfare as an integrated strategic instrument. Through this framework, China seeks to employ multiple approaches. Information warfare aims to slow down an adversary's decision-making process and strengthen its own position by controlling information and communications. Psychological warfare focuses on influencing public consciousness and intensifying social divisions to achieve political objectives. Legal warfare involves attempting to legitimize political ideas and constrain the actions of adversaries through international and national legal mechanisms[11]. The practical application of these concepts can be clearly observed in China's domestic and foreign policies concerning the South China Sea, Taiwan, and several other regions.

Chinese state institutions utilize online platforms in an integrated manner to consolidate their positions, manage public opinion internationally, and maintain internal order and discipline. China's "Three Warfares" concept is not merely a conventional approach to conflict; it also treats the information environment as a battlefield. In other words, China perceives victory not only through military means but also through information, psychological, and legal instruments. The essence of this approach lies in the idea that modern warfare is no longer limited to armed confrontation. It is increasingly conducted through mass information flows, social-media–driven cognitive manipulation, and efforts to shape international legitimacy. The "Three Warfares" concept is based on the strategy of defeating an adversary without engaging in direct military conflict. Within this framework, China views the information domain as a primary strategic instrument for safeguarding and advancing its cultural, economic, and political interests.

In the United States, a different set of approaches and mechanisms is observed within the information environment. American strategies are built upon several key elements, including:

- Cyber defense and offensive cyber capabilities — These involve not only protecting national critical infrastructure, but also maintaining the capacity to disrupt or disable an adversary's systems when necessary. In the United States, particular emphasis is placed on the effectiveness of specialized cyber commands, the Department of Defense (DoD), and various federal agencies responsible for cybersecurity operations[12].
- Information Law and Legislation — In the digital era, stability is ensured and measures are taken against undesirable information campaigns through legal and regulatory mechanisms.
- Soft Power and International Media — These strategies involve promoting democratic values on a global scale through mass information communications, technological platforms, and diplomatic instruments. In this context, J. Nye notes: "In the information age, the mark of a great power is not just whose army wins, but also whose story wins."[13] However, Nye did not initially take into account the development of artificial intelligence, which in subsequent years increases the likelihood of revising or adapting these views to reflect new technological realities.

According to the views of various scholars and our own research findings, the competition between the United States and China is deepening not only in the field of technology, but also across strategic and ideological dimensions. In the era of modern globalization, both states are actively striving for information dominance on a global scale.

The main characteristics of this rivalry can be classified as follows.

Technological Dimension. The United States and China are competing for leadership in areas such as cybersecurity, artificial intelligence, 5G networks, and space-based communication systems. China seeks to expand its technological influence through corporations such as Huawei and Zhongxing Telecommunication Equipment Corporation (ZTE), while

[11] NATO ACT (2021) Decision Making in the Age of Big Data and Artificial Intelligence (AC 2020 Final Report), sah. 47. URL: https://www.act.nato.int/wp-content/uploads/2024/07/20210301

[12] U.S. Department of Defense. (2023) Department of Defense Cyber Strategy. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf

[13] *Nye, J.S.* (2011) The Future of Power. Carnegie Council. 10 February 2011. URL: https://www.carnegiecouncil.org/media/series/39/20110210-the-future-of-power

the United States views the activities of these companies as potential threats to national security[14].

Strategic Dimension. Strategically, the United States treats information security as a central component of its national defense strategy, whereas China seeks to employ information, psychological, and legal pressure in an integrated manner through its Three Warfares doctrine.

Ideological Dimension. Ideologically, the United States promotes principles such as free information flows and freedom of expression among its citizens. China, by contrast, views maintaining strict control over the internet within its territory as an essential element of national security. These sharply divergent approaches further intensify the rivalry surrounding the governance of the global internet.

The current information rivalry between the United States and China increasingly resembles a new type of Cold War, echoing the confrontation between the United States and the Soviet Union after the Second World War. The starting point of this intensified competition is closely associated with political developments surrounding Donald Trump in 2024. It is not impossible that, in the future, information-based instruments of power may acquire a strategic significance comparable to nuclear weapons, fundamentally reshaping global security dynamics. The confrontation between the two states further accelerates the transformation of the information domain under conditions of globalization. As researchers, we view this process as a natural outcome of the clash between different political systems. In this sense, the competition between capitalist and communist ideologies is manifested in the form of modern information warfare. Future conflicts are likely to be driven not by struggles over territory or natural resources, but by efforts to control information spaces and shape global public opinion. For example, if negative stereotypes emerge around the Coca-Cola brand, its sales may decline regardless of its taste or widespread popularity. This demonstrates that the construction of perceptions within the information sphere can have a direct impact on real economic processes.

The United States' open information policy and its reliance on the concept of soft power emerge as a natural continuation of its democratic system. In this framework, free information flow is seen as a factor that strengthens political credibility and enhances international prestige. In contrast, China's socialist and centrally controlled governance model interprets information regulation as a tool for maintaining order and preserving social stability. Consequently, China views 'information security' not only as a technical necessity but also as an ideological safeguard. In our view, the differences between the two states' information policies are directly linked to their respective political systems and value structures, and these distinctions are clearly reflected in their approaches to information warfare. However, both of these opposing strategies carry certain risks for global information security: the dominance of U.S. media may lead to one-sided information dissemination, while China's strict control mechanisms can constrain information freedom. Therefore, strengthening international cooperation and ensuring normative balance appears to be the most optimal solution.

The competition between the United States and the People's Republic of China

PRC in the information domain is reflected not only in theoretical approaches but also in concrete operational campaigns. Considering China's active use of information tools to advance its strategic objectives, the PRC increasingly employs information warfare tactics in its regional and global activities. In the context of tensions surrounding Taiwan and the South China Sea, China utilizes propaganda, disinformation, and media influence to shape both internal and international public opinion. The primary goal of this approach is to isolate Taiwan, weaken international support for it, and reshape the regional narrative in favor of Beijing.

The achievement of these objectives is primarily carried out through informational and psychological mechanisms. In practice, this approach can be observed through several actions: amplifying supportive content via troll accounts on social media, presenting Beijing's position through local publications or blogs, and promoting alternative legal and historical narratives through diplomatic channels. Recent observations indicate that China has also attempted to extend its influence to the Philippines.

In contrast, the United States employs a more comprehensive approach in this area. Its main strategies include:

- Ensuring security through national cyber defense and legal-regulatory measures;
- Expanding international cooperation and strengthening relations with allied countries;
- Collaborating with information and technology companies to identify and limit the spread of misinformation.

The U.S. Congress and specialized agencies actively study China's capabilities in the information domain and develop strategic responses. In practice, the United States coordinates intelligence operations through USCYBERCOM and other cyber units, while the Cybersecurity and Infrastructure Security

[14] CNBC. (2020, August 13). FCC declares Huawei, ZTE national security threats. URL: https://www.cnbc.com/2020/07/01/fcc-huawei-zte-officially-designated-national-security-threats.html

Agency (CISA) manage the protection of civilian infrastructure[15].

At the same time, the United States actively engages with numerous countries by offering support to strengthen information stability and by using information platforms to detect and limit the spread of inaccurate information. Both the United States and China extend their competition beyond their own territories, vying for informational influence in third-party states. The primary aim of these campaigns is to shape political sentiment in strategically important countries — such as the Philippines and Mexico — and to secure cooperation and support from allies.

According to analytical publications such as War on the Rocks and the Jamestown Foundation, China is actively seeking to reshape regional narratives through its informational influence. Meanwhile, the U.S. Congress and researchers assess China's information pressure and cyber capabilities as threats, emphasizing the need for robust cyber defense and the strengthening of alliances. Experts at the Foundation for Defense of Democracies (FDD) argue that the United States should not limit itself to defensive measures but adopt an offensive posture in information warfare in response to active operations conducted by rival states, particularly China, Russia, and Iran[16].

In our view, responding to information operations in kind-especially if conducted without proper oversight-could escalate international tensions and exacerbate ethnic and social divisions.

Prospects

The intensification and expansion of information warfare indicate that human civilization has entered a new stage. In modern conflicts, reliance on military force alone is no longer sufficient; managing information flows and shaping the perceptions and beliefs of adversaries have become critically important. As noted in International Affairs: "Technological developments have long been used to create tailored versions of reality for rivals in pursuit of strategic interests."[17] In other words, in the 21st century, military, economic, and political advantages depend not only on the strength of conventional weapons but also on superiority in the digital information domain. Emerging information technologies-particularly artificial intelligence (AI), automated systems, and Big Data-have introduced a new phase in warfare strategies. According to the War of 2050 report, by 2050, conflicts may be conducted with minimal human involvement, managed instead by automated systems and AI[18]. These systems would allow not only political analysis but also real-time, rapid decision-making capabilities. Consequently, every advanced state today seeks to strengthen its AI capabilities alongside its conventional military potential. China's Three Warfares strategy exemplifies this trend, integrating classical informational, psychological, and legal components with modern technological advancements.

Research indicates that the People's Liberation Army of China (PLA) considers technologies such as artificial intelligence (AI), cloud computing, and Big Data analytics as key to future warfare success. Through these capabilities, China aims to consolidate global political and ideological influence via information[19]. Central to this policy is the concept of 'information sovereignty,' which refers to a state's right to exercise full control over its informational domain. Accordingly, China maintains national information security through the Great Firewall, internal social media platforms, and digital monitoring systems. At the same time, the United States also regards information security as a critical component of its national defense strategy.

Modern cybersecurity is no longer viewed solely as a technical issue; it also carries significant political and strategic implications. As Singer and Friedman note, "For these reasons, cybersecurity is something both technical and political." This highlights that preventing cyberattacks and protecting information systems requires oversight not only by IT specialists but also by government bodies and state institutions from political and strategic perspectives. The United States has also actively engaged in developing legal norms for information warfare at the international level. Within NATO, the "Tallinn Manual" has been created to establish the legal framework for cyber warfare[20]. Initiatives like this may serve as an important step toward ensuring international information security in the future.

In the future, information warfare is likely to have a dual impact on humanity:

- On one hand, it drives technological advancements and the development of new security systems;

[15] U.S. – China Economic and Security Review Commission (USCC). 2022 Annual Report to Congress — Chapter 3, Section 2: China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States. USCC. URL: https://www.uscc.gov/annual-report/2022-annual-report-congress

[16] Foundation for Defense of Democracies (FDD). American Confidence in Elections: Prohibiting Foreign Interference. 18 December 2024. URL: https://www.fdd.org/analysis/2024/12/18/american-confidence-in-elections-prohibiting-foreign-interference/

[17] *Rid, T.* (2020) Active Measures: The Secret History of Disinformation and Political Warfare. Review in International Affairs, 97 (1): 244–258. Oxford University Press. URL: https://academic.oup.com/ia/article-abstract/97/1/244/6041478

[18] *Kott, A., Alberts, D.S., Wang, C.* (2015) War of 2050: a Battle for Information, Communications, and Computer Security. *arXiv preprint*. URL: https://www.emergentmind.com/papers/1512.00360?utm_source

[19] *Drinhausen, S., Legarda, H.* (2025) Reconfiguring International Security — The Strategic Evolution of Modern Warfare. Zeitschrift für Außen- und Sicherheitspolitik.URL: https://link.springer.com/article/10.1007/s12399-025-01018-9?utm_source

[20] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, editors Michael N. Schmitt, Liis Vihul.

- On the other hand, it exacerbates international conflicts, legal gaps, and ethnic tensions.

We argue that mitigating these risks requires international legal agreements, such as a United Nations convention on the limitation of information weapons or a treaty on cyber arms control. Losing control over information not only threatens individual states but also poses a serious risk to global security as a whole.

Conclusion

In the context of globalization, information warfare has become one of the most significant dimensions of international relations. The research findings indicate that, in the twenty-first century, control over information resources has emerged as a key measure of geopolitical influence among states. The competition between the United States and China represents the most prominent manifestation of this process and plays a critical role in shaping the global security architecture.

The United States directs its information policy toward promoting democratic values and enhancing soft power through global media platforms. In contrast, China employs the "Three Warfares" strategy, utilizing informational, psychological, and legal instruments to advance its national interests and expand its geopolitical influence.

Advancements in technologies, artificial intelligence, and cybersecurity have increasingly complicated the nature of information warfare. This process encompasses not only cyberattacks but also strategies aimed at influencing public opinion, disrupting decision-making mechanisms, and reshaping international norms.

To minimize the consequences of information warfare and maintain geopolitical stability, the following recommendations are proposed:

- Strengthen international cooperation diplomatically, implementing agreements on cybersecurity through international organizations;
- Develop specialized academic programs such as Information Policy, Cybersecurity Diplomacy, and Geopolitical Communication at universities to train experts according to international standards;
- Enhance public resilience to information influence, given that information warfare primarily targets the population's perception, including literacy in managing information and understanding AI technologies.

The information domain has become the primary arena of competition among states. Control over information shapes a state's global image and geopolitical strategy. The information rivalry between the United States and China directly affects the future configuration of the international system. At the same time, the intensification of information warfare compels states to develop new mechanisms for global information security and cyber defense. Strategic information competition will remain a central factor in global politics for the foreseeable future.

Статья поступила: 21.11.2025
Принята к печати: 19.12.2025