RUDN Journal of Public Administration
ISSN 2312-8313 (print), ISSN 2411-1228 (online)
Вестник РУДН. Серия:
ГОСУДАРСТВЕННОЕ И МУНИЦИПАЛЬНОЕ УПРАВЛЕНИЕ

2024 Том 11 No 1 19–31
http://journals.rudn.ru/
publicadministratory

DOI: 10.22363/2312-8313-2024-11-1-19-31
EDN: ZIXNDI

Research article / Научная статья

# Information Warfare as a Tool of Political Confrontation in the Modern Multipolar World

**Irina V. Goncharova**[1], **Victor F. Nicevich**[2], **Oleg A. Sudorgin**[2] ✉

[1]N.V. Parakhin Orel State Agrarian University,
*69 Generala Rodina St, Orel, 302019, Russian Federation*

[2]State University of Management,
*99 Ryazansky prospect, Moscow, Russian Federation*

✉ svis@mail.ru

**Abstract.** The study is devoted to the analysis of the phenomenon of information warfare in the modern world. Authors concretized the concept of information warfare and its connection with hybrid warfare, which has replaced the mechanisms of direct "forceful" influence in a rapidly changing political architecture. The significance of the wars of the XXI century, which are conducted from the position of "soft power" and are characterized by a protracted nature, is revealed. Information warfare is considered as their most important component. The authors highlight the following features of information wars: they are conducted in the cultural field; their purpose is to transform the consciousness of a political opponent. These wars are aimed at value orientations, traditions, historical and cultural identity. The emergence of the concept of "information warfare" in the article is associated with the end of the Cold War at the end of the XX century and the definition of a new U.S. strategy. The main conditions and reasons for the transition to a new type of war are the collapse of the bipolar world, the growing threat of international terrorism, and the erosion of ethnic and cultural identity within the United States and allied countries themselves. Cybernetic troops are analyzed as a new specialized type of troops. The authors revealed two main spaces of the information war impact: the communicative environment and the field of probable social macro-conflict. Information warfare in research is considered as part of a military, economic, and geopolitical confrontation. The authors substantiate that an extremely intensive information war has been waged against the Russian Federation for more than 20 years. It involves depriving Russia not only of allies, but also replacing the "cultural and historical codes" in friendly countries, primarily by reformatting the consciousness of young people. The authors analyzed the documents aimed at solving the problem of information wars in Russia — the "Information Security Doctrine of the Russian Federation" and the "National Security Strategy of the Russian Federation".

**Keywords:** hybrid warfare, information warfare, cyber warfare, cyberspace, information strategy, information security

**Conflicts of interest:** The authors declared no conflicts of interest.

**Article history:**
The article was submitted on 01.12.2023. The article was accepted on 10.01.2024.

**For citation:**
Goncharova I.V., Nicevich V.F., Sudorgin O.A. Information Warfare as a Tool of Political Confrontation in the Modern Multipolar World. *RUDN Journal of Public Administration.* 2024;11(1):19–31. https://doi.org/10.22363/2312-8313-2024-11-1-19-31

## Introduction

Today, information wars occupy the main, and in some cases the decisive place in the confrontation, both between individual states and at the level of individual political entities and alliances of states. Due to the rapidly increasing political uncertainty, in the context of the rapidly changing political architecture of the world, the mechanisms of direct "forceful" influence have been replaced by "hybrid warfare", involving a combination of traditional ("classical") methods of warfare and the use of so-called "soft power". It should be noted that most of the wars of the twentieth century, waged by the above-mentioned "traditional methods", were characterized by large-scale destruction in the warring countries, accompanied by a deep economic crisis, political deformation up to the collapse of the former political system, and psychological breakdown of society. The wars of the XXI century, waged from the position of "soft power", are characterized by a protracted nature. They are conducted in the cultural field, and their goal is to transform the consciousness of a political opponent who may not suspect that he is in the epicenter of "fighting". The objects of such wars are the values, traditions, historical and cultural identity of a country.

## Discussion

### *On the concept of "information warfare"*

From our point of view, Major General A.I. Vladimirov gave the most comprehensive assessment of the hybrid war. He pointed out that the main task of hybrid warfare is "… the gradual immersion of the victim state into a state of 'organized chaos', achieving its 'crushing by starvation' outside the use of armed forms of war". At the same time, the theater of warfare, the conditional "gray zone" in which the conflict unfolds, can be not only individual states, but also their conglomerate. The danger of a hybrid war lies in the fact that "non-violent methods" that paralyze the possibility of applying the norms of international law affect almost all spheres of state activity: economic and political space, science and education, healthcare, ideological space, morality and morality, cultural identity of society [1].

Like any war, a hybrid conflict involves an interconnected set of non-traditional combat operations (that is, conducted without the intervention of the armed forces and law enforcement agencies), which are understood as "hybrid operations" (hybrid operations). In separate studies, six main types of hybrid operations are distinguished: psychological, aimed at suppressing the spirit and depriving motivation to resist; economic, provoking stagnant and crisis processes in the economy, up to economic collapse; mass protest actions of the opposition; sabotage actions of illegal paramilitary structures that have no connection with other States; impact with the use of cybernetic weapons. But the most significant, and, in fact, the type of hybrid operations that continuously operates throughout the confrontation is the complex of information impact, which should be understood as a self-sufficient information war. Let us draw attention to the fact that in a number of works hybrid conflict is defined as a military strategy using, along with traditional "force methods", a set of information and psychological tools.

According to the official version, the term "information war" was first specified in the 1980s, although its use dates back to 1976. Its use is associated with Thomas Ron's report "Weapon Systems and Information Warfare" [2], it was developed for Boeing Aerospace Co. Ron wrote: "… information infrastructure is becoming a key component of the American economy, but it is simultaneously becoming a vulnerable target in both wartime and peacetime" [3. P. 11–15].

The "concretized term" defined the new U.S. strategy with the end of the Cold War. The active use of the term refers to the period after the completion of Operation Desert Storm. It is at this point that the material base and the general philosophy of using a new type of weapon are being formed. At the official level, the scope of its application of the new term was generally defined in the following documents: 1) Directive of the US Secretary of Defense No. TS-3600.1 "Information Warfare", issued in December 1992, 2) Directive of the Chairman of the Joint Chiefs of Staff Committee No. 30–93 in 1993, 3) Unified Charter of the Joint Chiefs of Staff Committee No. 3–13.1 "Joint Actions of Heterogeneous Forces to Combat Enemy control systems", 1995, 4) Instructions of the Joint Chiefs of Staff Committee 3210.01 A "Unified Perspective-2010", 5) "The concept of information operations of the united groups of the armed forces" 1996 and a number of others [4. P. 2–9] The active military-theoretical and military-political activities of the US law enforcement agencies to study the possibilities of information influence on their political opponents shows the serious importance of this type of "indirect" ("soft") methods of military operations at the turn of the XX — XXI centuries.

### *The transition to the US information war*

The reasons for the transition to a new type of war were the collapse of the bipolar world, the growing threat of international terrorism, the erosion of ethnic and cultural identity within the United States itself and a number of countries following in the wake of its policies. Since information wars are being waged in a "gray zone", in conditions of imaginary military and political stability, many experts note that at the present stage, significant changes have taken place in the information warfare strategy waged by the United States. In particular, the understanding of the cyberspace category has changed, in which a significant part of the information warfare processes take place. Cyberspace is understood as an essential component of the unified information space. Now the "global cyberspace" includes the "blue" (American), "red" (enemy) and "gray" (neutral) areas. At the same time, it is considered that "… it is allowed on a 'legitimate basis' to conduct cyber operations in any foreign cyberspace ('red' and 'gray' zones) without notifying the authorities of these countries on the grounds that cyberspace has no state borders" [5. P. 22–29]. The information confrontation may have a "preventive character". For a more in-depth understanding of what constitutes a cyberattack, as an "attack in cyberspace" see [5. P. 22–29].

It should also be noted that the warring parties are developing special terminology designed to distort the true content of hidden military and political activity (In fact, we are dealing with outright semantic simulacra). So, initially, the phrase "information operations" was used as a term denoting methods of conducting information warfare, later the terms "strategic communications" and "public diplomacy" appeared in scientific, theoretical and political rhetoric.

Domestic experts, in particular, colonel P. Kolesov notes: "Strategic communications… this is a new concept of the IW themselves … The purpose of the IC is to convince or compel the target audience to make decisions or take actions aimed at forming, preserving or developing favorable conditions for the promotion of American national interests" [6. P. 9–14]. The main instruments of influence on the enemy are considered to be: "coordinated information actions, indoctrination, various information and propaganda plans and programs". They are implemented by the "US Department of Defense, combat commands of the Armed Forces, engineering troops, the Agency for International Development, the State Department" and a number of other structures [6. P. 9–14].

It is noteworthy that by the zero years of the XXI century, a new type of troops — cybernetic troops — begins to take shape. To date, the architecture of this type of troops in relation to the United States and NATO includes:

1) structures of the US Department of Defense — Ardingham County, Virginia;
2) structures of the US Strategic Command — US Base Offutt, Nebraska;
3) U.S. Cyber Command — Fort George J. The Ministry of Foreign Affairs;
4) the US NSA (20 thousand people, the budget of about 3 billion dollars);
5) the CIA information operations center (the total number of full-time CIA employees is about 15 thousand people, the budget is 3 billion dollars);

6) as separate structures, we can distinguish: the intelligence directorate of the Joint Staff J, the intelligence directorate of the US Department of Defense with a staff of 6 thousand people, the intelligence directorate of the US Air Force;
7) The FBI has also established special departments to counter cybercrimes;
8) NATO Communication and Information Agency — Brussels;
9) Joint Center of Excellence for Electronic Counteraction of NATO — Tallinn, Estonia;
10) NATO Joint Center of Excellence for Strategic Communications — Riga, Latvia.

In this case, the list of structures carrying out information impact ("offensive operations") and counteraction ("defensive operations") is not exhaustive. The total number of cyber forces of individual NATO countries by the early 2020s is shown in Table.

**The total number of cyber forces of individual NATO countries**

| Country | Total number of cyber troops |
|---|---|
| USA | 64.000 people |
| Germany | 14.500 people (the country has an "information technology security center" with a staff of 500 people) |
| France | 4.000 people (the country is also developing an information security system "Echelon") |
| Great Britain | 2000 people (the problem is handled by the Department of Government Communications with a staff of up to 6000 people) |

Despite the fact that the North American defense Department spends $ 10 billion annually on information security, American military experts continue to note the country's continuing information vulnerability and the lack of the ability to ensure complete information security. As a result: "… the option of reorganizing cyber commands into information operations commands is being considered, which will allow combining cybernetic, psychological and electronic operations with a single plan" [5. P. 22–29]. The operational deployment of this institutional formation is planned to be completed in 2028.

Initially, the general concept of information warfare affected two main impact spaces: the communicative environment and the field of probable social macro-conflict. Diverse information and mechanisms for working with it became the main means of waging war. At the same time, the information war was considered not as a self-sufficient phenomenon, but as part of a military, economic, and geopolitical confrontation. As a result, at the **macro level**, information (information and psychological) wars were defined as a form of confrontation in the global and local information environments, implemented by manipulative methods, technologies and methods of influencing the information and psychological fields of the opposing party (counterparty) in order to inflict maximum damage to it.

In the directive of the US Department of Defense T8 3600.1, the following were noted as the main types of information warfare:

1) "political, diplomatic and economic actions;
2) information and psychological operations;
3) subversive and demoralizing propaganda actions;
4) assistance to opposition and dissident movements;
5) exerting a comprehensive influence on political and cultural life with the task breaking up the national and state foundations of society;
6) penetration into the public administration system;
7) protection of national information systems" [7].

Special attention is paid to the "military level" of information warfare, the main purpose of which is to "achieve information dominance over the enemy in an armed conflict and protect their own control systems from the enemy's information weapons" [7]. According to the Joint Chiefs of Staff Committee directive in March 1993 "Combating control systems", the military level solves tasks, in addition to the electronic and physical destruction of the enemy's communication systems, misleading him and psychological struggle [7].

Identical types of information warfare are recorded in the curricula of the US National Defense University. Along with electronic warfare, they consider psychological, intelligence, and cybernetic warfare.

In turn, a micro-level definition of information warfare is also possible. In this case, it can be interpreted as a set of discrete operations (influences) carried out in the information space (field) aimed at achieving superiority over the counterparty, controlling (manipulating) his actions. The main goals of information warfare at the micro level include:

1) maximum control of the private information space;
2) its protection;
3) the possibility of obtaining private information of contractors;
4) the possibility of influencing their information system, up to its destruction.

Summarizing the above arguments, it can be argued that information wars are designed to solve the tasks of strengthening the positive motivation and stress resistance of the population of a given country and its armed forces, on the one hand, provoking depressive moods and psychological chaos among the population of the counterparty countries, creating a negative political and cultural image of the counterparty countries at the level of the world community, on the other hand.

Today we can state that an extremely intensive information war has been waged against the Russian Federation for more than 20 years. Back in the early 1990s, the United States declared a potentially hostile attitude towards a renewed Russia as priorities of its foreign policy in Paul Wolfowitz's "conditional doctrine" (In the version dated 04.15.1992). In particular, it was emphasized: "… we must remember that democratic changes in Russia are not irreversible and that, despite the current difficulties, Russia will remain the strongest military power in Eurasia and the only power in the world capable of destroying the United States" [8].

This doctrinal approach assumed the preservation of the political hegemony of the United States in the world by implementing the "end of history" — the creation of a unipolar world system. One of the possible forms of preserving the current situation for as long as possible was the creation of a "cordon" against a "potentially strong" Russia — the expansion of NATO to the East by including the Baltic states in NATO and the beginning of an intergovernmental and international dialogue on the inclusion of Ukraine and Georgia in the bloc. In this case, one of the tools for rocking the political situation was the "color revolutions" along the borders of Russia, as an instrument of permanent "hybrid war". Information warfare became an element of this complex of "indirect actions".

***Ensuring the information security of Russia.*** According to Russian Foreign Minister Sergey Lavrov, the goals of the hybrid and, as a result, information war against Russia are to create around the country: "… a belt of instability, forcing our closest neighbors and fraternal peoples to make a choice — either you are with the West or you are with the Russian Federation" [9]. This policy is aimed at preventing the very possibility of geo-economic consolidation of Eurasia. It involves depriving Russia not only of allies, but also replacing the "cultural and historical codes" in friendly countries, primarily by reformatting the consciousness of young people.

An important role in understanding and solving the problem of hybrid and information wars was played by the adoption in Russia of the "Information Security Doctrine of the Russian Federation" (Decree of the President of the Russian Federation dated 5.12.2016 No. 646) and the "National Security Strategy of the Russian Federation" (Decree of the President of the Russian Federation dated 02.07.2021 No. 400).

In the "Information Security Doctrine of the Russian Federation", the list of threats in the information sphere highlights:

1) the expansion by a number of foreign countries of the possibilities of information technology impact on the information infrastructure for military purposes;

2) the desire of individual states to use technological superiority to dominate the information space;
3) strengthening the activities of organizations engaged in technical intelligence in relation to Russian government agencies, scientific organizations and enterprises of the military-industrial complex;
4) an increase in the volume of materials in foreign mass media containing a biased assessment of the state policy of the Russian Federation;
5) an increase in the scale and coordination of computer attacks on critical information infrastructure facilities;
6) 6) the increasing threats of the use of information technology to damage the sovereignty, territorial integrity, political and social stability of the Russian Federation.

Thus, the main directions of ensuring information security in the field of defense of the Russian Federation are:

1) strategic deterrence and prevention of military conflicts that may arise as a result of the use of information technology;
2) improvement of the information security system of the Armed Forces of the Russian Federation, other troops, military formations and bodies, including forces and means of information warfare;
3) forecasting, detection and assessment of information threats, including threats to the Armed Forces of the Russian Federation in the information sphere;
4) assistance in ensuring the protection of the interests of the allies of the Russian Federation in the information sphere;
5) neutralization of information and psychological effects, including those aimed at undermining the historical foundations and patriotic traditions associated with the protection of the Fatherland [10].

The content of the analysis of the main information threats to the Russian Federation from the conditional “collective West” allows us to identify as objects of information warfare: the armed forces of the Russian Federation involved in the SVO; military personnel and authorities of the DPR and LPR; the civilian population of Russia and the allied state of Belarus (children and spouses of the military); politicians and residents Western countries sympathetic to Russia; politicians and laymen of non-Western and anti-Western countries.

It is customary to refer to the subjects of information warfare as the most significant political figures of the state, the cyber army, which we mentioned above, the media, civilians who have left the combat zone (refugees).

Among politicians with real political weight, representatives of the federal level of the country’s political elite are most often singled out: the head of state; the Prime Minister (Prime Minister) and heads of individual, most significant ministries; individual representatives of the Ministry of Foreign Affairs; the most significant representatives of the Ministry of Defense and individual law enforcement agencies; representatives of the legislature; heads of the most significant subjects of the state. Representatives of the political elite, as well as the military and political leadership of countries, as a rule, form the space, content and direction of information confrontation.

Speaking about the mass media as an instrument of information warfare, Western experts identify two such "conditional" groups of media in modern Russia. At the same time, it is believed that "… unlike American experts, Germans consider media management as an element of information warfare" [3. P. 11–15]. In this regard, the Russian experience of conducting information warfare, according to researchers, is closer to the German experience than to the American one.

The first group of Russian media in the context of the problem of information warfare includes TV channels and radio channels, as well as a variety of printed materials that voice the official agenda of government authorities. As a rule, they have full or partial government funding and work not only for domestic, but also for foreign consumers.

In fairness, it should be said that the media also plays an important role in the theory of "strategic communication" in the United States. Experts note that the American set of communication tools is extensive. This includes "mass media, as well as communications and telecommunications, wireless communication infrastructure, sociological research, cultural and linguistic means, electoral technologies and methods of counting votes, mass trainings and educational programs" [6. P. 9–14]. Nevertheless, the media continues to play a major role in this process.

In Russia, Rossiya Segodnya (Russia Today; RT) played an important role in shaping the country's official image abroad. The company started operations in June 2005. Its goal was to promote Russia as a positive political and cultural brand abroad. RT is run by the autonomous non-profit organization TV-News. The company's weekly audience is approaching 100 million people in 47 countries [11].

The second group of considered domestic media formed by opposition and anti-Russian radio and TV channels, printed materials and information sites. The operation of these funds is under the control of Roskomnadzor and the Ministry of Justice of the Russian Federation in accordance with Federal Law No. 236-FZ dated July 1, 2021 "On the activities of Foreign Persons in the Internet Information and Telecommunications Network in the territory of the Russian Federation". In 2022, the sites Beats-1, Steam, Spotify, Pandora, and FOX were blocked. In turn, Meta's social networks have been identified in our country as extremist. Their resources ceased to operate on March 21, 2022.

The refugee problem is also extremely relevant for understanding the military-information confrontation. People affected by local and regional conflicts often become an instrument of “dirty” insinuations and information propaganda. Often their personal tragedy is used to “dehumanize” the image of one of the warring parties. At the same time, an extremely intensive exploitation of the emotional field of the world community is carried out (the formation of indignation, indignation, bitterness, aggression). It is extremely difficult for people who find themselves hostages of the information war to form an objective assessment of the events taking place.

An important place in the implementation of various information warfare strategies is occupied by information weapons. In the Russian theory of information warfare, it is customary to divide it: according to the scope of application — into information-technical and information-psychological; according to the intended purpose — into defensive and offensive (“offensive and defensive information operations can be carried out according to a single plan and plan and complement each other” [4]).

A special place in the information confrontation is occupied by “psychological warfare”, in the arsenal of which there are various types of exposure to information media, from propaganda to the creation of virtual reality. Audio and video simulacra are used to manipulate mass consciousness, including images and voices of politicians and prominent personalities. Disinformation is carried out by changing enemy information databases, geolocation, navigation systems, etc. [12]

One of the common techniques of modern information warfare is the “bombardment” of the counterparty with fake information or fakes. With the help of fakes, the real space of events is actively simulated and distorted. Fakes are usually divided into “simple” and “complex” ones. The main techniques used to create fakes are: dissemination of deliberately false information about an actual socially significant event; demonstration of unreliable photo and video documents that do not belong to the event zone; falsification of signatures under reliable photo and video documents; staged video filming; demonstration of fragments of video games, extracts from feature films, virtual content.

## Conclusion

Summing up, it should be emphasized that information wars have become an irreversible reality, constantly invading not only the space of the functional fields of individual states, but also the daily life of each individual person. At the same time, information wars have highlighted the vulnerable sides of even democratic societies, making them more fragile and vulnerable. Authoritarian mechanisms of influence have been replaced by multi-channel mechanisms of manipulation of public consciousness, transformed into a system of total control over human consciousness. Ordinary people who find themselves in a permanent "information siege", in conditions of "information overload", generating increasing stress and various phobias, become hostages of complex political games and confrontation in the information field. At the same time, there is an effect of fragmentation of society, filled with diverse simulations. It can be argued that humanity was faced with the threat of a grandiose catastrophe of an ecumenical scale, since a significant part of humanity either lost or did not have time to acquire adequate means of understanding the rapidly changing, "opaque" and unpredictable world.

## REFERENCES

1. Vladimirov A.I. *Osnovy obshchei teorii voiny: monografiya: v 3 ch.* [Fundamentals of the General Theory of War: monograph in 3 parts]. Moscow: Synergy publ.; 2013. 2856 p. (In Russ.).
2. Rona T.P. *Weapon Systems and Information War.* Boeing Aerospace Co., Seattle, WA; 1976. 50 p.
3. Grinyaev S. Kontseptsiya vedeniya informatsionnoi voiny v nekotorykh stranakh mira [The Concept of Information Warfare in Several Countries of the World]. *Foreign Military Review.* 2002;2:11–15 (In Russ.).
4. Zhukov V. Vzglyady voennogo rukovodstva SShA na vedenie informatsionnoi voiny [The Views of the US Military Leadership on the Conduct of Information Warfare]. *Foreign Military Review.* 2001;1:2–9 (In Russ.).
5. Dylevsky I., Bazylev S., Zapivakhin O., Komov S.A. Peschenko K., Yunichenko S. O vzglyadakh administratsii SShA na kiberprostranstvo kak novuyu sferu vedeniya voennykh deistvii [About the Views of the US Administration on Cyberspace as a New Sphere of Warfare]. *Military Thought.* 2020;10:22–29 (In Russ.).
6. Kolesov P. Vedenie Soedinennymi Shtatami informatsionnykh voin. Kontseptsiya «Strategicheskikh kommunikatsii» [The Conduct of Information Wars by the United States. The Concept of "Strategic Communications"]. *Foreign Military Review.* 2010;6:9–14 (In Russ.).
7. Averchenkov V.I., Rytov M.Yu., Kondrashin G.V., Rudanovsky M.V. *Sistemy zashchity informatsii v vedushchikh zarubezhnykh stranakh* [Information Security Systems in Leading Foreign Countries]. Bryansk: BSTU; 2007. 203 p. (In Russ.).
8. Vertlib E. Voina resursnaya v kontekste gibridno-mental'noi [Resource Warfare in the Context of Hybrid-mental Warfare]. *Russkaya narodnaya liniya.* 11.10.2022. URL: https://ruskline.ru/news_rl/2022/10/11/voina_resursnaya_v_kontekste_gibridnomentalnoi?ysclid=lrkuz7ixof126111033 (accessed: 10.11.2023) (In Russ.).
9. Kolesnikova M. Zapad pytaetsya sozdat' «poyas nestabil'nosti» vokrug RF [The West Is Trying to Create a "Belt of Instability" around the Russian Federation]. *The Moscow Post.* 23.07.2021. URL: http://www.moscow-post.su/politics/zapad_pytaetsya_sozdat_poyas_nestabilnosti_vokrug_rf36446/?ysclid=lrkv4nd58c871899594&utm_source=ya.ru&utm_medium=referral&utm_campaign=ya.ru&utm_referrer=ya.ru (accessed: 10.11.2023) (In Russ.).
10. *Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii (Ukaz Prezidenta Rossiiskoi Federatsii ot 05.12.2016 № 646)* [On the Approval of the Information Security Doctrine of the Russian Federation (Decree of the President of the Russian Federation dated 5.12.2016 No. 646)]. URL: http://www.kremlin.ru/acts/bank/41460 (accessed: 10.11.2023) (In Russ.).

11. *Russia Today TV (RTTV).* URL: https://rkn.gov.ru/mass-communications/reestr/media/?id=315435 (accessed: 10.11.2023) (In Russ.).
12. Informatsionnaya voina (Opredelenie informatsionnogo oruzhiya) [Information Warfare (Definition of Information Weapons)] *Liniya Stalina*. 25.02.2022. URL: https://stalinline.ru/2022/02/25/informaczionnaya-vojna/?ysclid=lpbnapyns8740653990 (accessed: 10.11.2023) (In Russ.).

**Information about the authors:**

*Irina V. Goncharova* — Doctor of Historical Sciences, Professor of the Department of History, Philosophy and Russian Language, N.V. Parakhin Orel State Agrarian University (Russian Federation) (ORCID ID: 0000-0002-7532-8751) (e-mail: int@orelsau.ru).

*Viktor F. Nitsevich* — Doctor of Political Sciences, Deputy Director of the Research Institute for Public Policy and Sectoral Economy Management, State University of Management (Russian Federation) (ORCID ID: 0000-0002-1668-3067) (e-mail: dr.nitsevich@mail.ru).

*Oleg A. Sudorgin* — Doctor of Political Sciences, Director of the Economy Digital Transformation Management Research Institute, State University of Management (Russian Federation) (ORCID ID: 0000-0001-7670-7238) (e-mail: svis@mail.ru).

# Информационная война как инструмент политического противостояния в современном многополярном мире

**И.В. Гончарова[1], В.Ф. Ницевич[2], О.А. Судоргин[2] ✉**

[1]Орловский государственный аграрный университет имени Н.В. Парахина,
*302019, Российская Федерация, Орёл, ул. Генерала Родина, д. 69*

[2]Государственный университет управления,
*109542, Российская Федерация, Москва, Рязанский просп., д. 99*

✉ svis@mail.ru

**Аннотация.** Анализируется феномен информационной войны в современном мире. Конкретизируется понятие информационной войны и ее взаимосвязь с гибридной войной, которая пришла на смену механизмам прямого «силового» воздействия в условиях стремительно меняющейся политической архитектуры. Раскрывается значение войн XXI в., которые ведутся с позиции «мягкой силы» и отличаются затяжным характером. Информационная война рассматривается как их важнейшая составляющая. Выделяются особенности информационных войн: они ведутся в культурном поле, их целью является трансформация сознания политического оппонента. Эти войны направлены на ценностные ориентиры, традиции, историческую и культурную идентичность. Появление понятия «информационная война» связывает с завершением Холодной войны в конце XX в. и определением новой стратегии США. Раскрываются условия и причины перехода к войнам нового типа: крушение биполярного мира, нарастание угрозы международного терроризма, размывание этнокультурной идентичности внутри самих США и союзных стран. Анализируется кибернетические войска как новый специализированный вид войск. Раскрываются два основных пространства воздействия информационной войны: коммуникативная среда и поле вероятного социального макроконфликта. Информационная война в исследовании рассматривается как часть военного, экономического, геополитического противостояния. Авторы обосновывают, что против Российской Федерации уже более 20 лет ведется крайне интенсивная по насыщенности средств информационная война. Она предполагает лишение России не только союзников, но и замены «культурно-исторических кодов» в дружественных нам странах, в первую очередь, путем переформатирования сознания молодежи. Анализируется документы, направленные на решение проблемы информационных войн в России: «Доктрина информационной безопасности Российской Федерации» и «Стратегия национальной безопасности РФ».

**Ключевые слова:** гибридная война, информационная война, кибервойска, киберпространство, информационная стратегия, информационная безопасность

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

**История статьи:**
Поступила в редакцию: 01.12.2023. Принята к публикации: 10.01.2024.

**Для цитирования:**
*Гончарова И.В., Ницевич В.Ф., Судоргин О.А.* Информационная война как инструмент политического противостояния в современном многополярном мире // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2024. Т. 11. № 1. С. 19–31. https://doi.org/10.22363/2312-8313-2024-11-1-19-31

**Информация об авторах:**
*Гончарова Ирина Валентиновна* — доктор исторических наук, профессор кафедры истории, философии и русского языка Орловского государственного аграрного университета имени Н.В. Парахина (ORCID ID: 0000-0002-7532-8751) (e-mail: int@orelsau.ru).
*Ницевич Виктор Францевич* — доктор политических наук, ведущий научный сотрудник НИИ Государственной политики и управления отраслевой экономикой Государственного университета управления (ORCID ID: 0000-0002-1668-3067) (e-mail: dr.nitsevich@mail.ru).
*Судоргин Олег Анатольевич* — доктор политических наук, директор НИИ Управления цифровой трансформацией экономики Государственного университета управления (ORCID ID: 0000-0001-7670-7238) (e-mail: svis@mail.ru).