

УДК 32.001

BRICHKOV A.S., Doctor of Philosophy, Associated Professor¹



NIKONOROV G.A., PhD in Philos. Sc., Associated Professor¹

¹The Russian Federation Armed Forces Army Air Defense
Military Academy



Received 22 March 2022

SOCIO-POLITICAL EMPHASES OF GEOPOLITICS AND SECURITY OF PUBLIC CONSCIOUSNESS IN THE CONTEXT OF INFORMATION CONFRONTATION¹

The article presents the author's analysis of the state of information security of the sphere of individual and public consciousness of Russian society. Tasks, methods and means of destructive information influence are defined, the conclusion on the implementation of a long-term strategy in relation to the Russian society, which is an integral part of the "hybrid war" of the united West led by the United States against the Russian Federation is made.

Keywords: *information, confrontation, individual and social consciousness, destructive influence, H-cases.*

А.С. БРЫЧКОВ, доктор филос. наук, профессор¹

Г.А. НИКОНОРОВ, канд. филос. наук, доцент¹

¹Военная академия войсковой ПВО Вооруженных Сил Российской Федерации,
г. Смоленск, Российская федерация

СОЦИАЛЬНО-ПОЛИТИЧЕСКИЕ АКЦЕНТЫ ГЕОПОЛИТИКИ И БЕЗОПАСНОСТЬ ОБЩЕСТВЕННОГО СОЗНАНИЯ В КОНТЕКСТЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

В статье представлен авторский анализ состояния информационной безопасности сферы индивидуального и общественного сознания российского общества. Определены задачи, методы и средства деструктивного информационного воздействия, сделан вывод о реализации долгосрочной стратегии в отношении российского социума, которая является неотъемлемой частью «ги-

¹Статья публикуется в авторской редакции.

бридной войны» объединенного Запада во главе с США против Российской Федерации.

Ключевые слова: информация, противоборство, индивидуальное и общественное сознание, деструктивное воздействие, Эйч-кейсы.

Introduction. In a generalized form, in the age of the formation of the information society, the bearer of spiritual values becomes a person, inextricably linked to the information environment. Information environment serves as an arena of clash of values of traditional societies and civilizations. National values in the sphere of public consciousness in the information age are the object of protection against internal and external threats. Therefore, it is impossible to consider the state of the sphere of public consciousness outside the analysis of the processes taking place in the information sphere.

The state of the sphere of public consciousness of the Russian people reflects the degree of negative information impact and allows us to determine its methods and ultimate goals. At the same time, the degree of information defeat of the components of the sphere of public consciousness is determined through the part of them that is either dead or works for goals alien to its own social system.

Threats of geopolitical adversaries in the political, economic and military sphere are materialized ways of threats in the sphere of public consciousness. Almost thirty years of the new Russian statehood made it possible to make sure that the direction of pressure on Russia does not change over time. The history of Russian statehood shows that the confrontation is geopolitical in nature, and the attitude of ideological opponents to our country does not change depending on the form of government, state structure or political regime.

The confrontation between the Western world and Russia has a deep - worldview (civilizational) character, which in periods of war is resolved through armed struggle, and in periods of peaceful coexistence through negative information influence. The progress of information technologies and the formation of a post-information society allow us to talk about such a massive application of information influence on geopolitical civilizational opponents, which allows us to talk about information war.

Information warfare is a systematic information impact on the entire infocommunication system of the enemy and neutral states in order

to form a favorable global information environment for political and geopolitical actions, providing maximum control over the enemy's space and resources.

The task of information warfare is to disable the technical systems of state and military control and to provide destructive information impact on individual and public consciousness in order to disorganize and destroy the society of the enemy state.

The purpose of destructive information influence is to weaken the overall potential of society, which entails a decrease in all types of security (including military), and the subjects of destructive influence are the United States and European Union countries, which are allies of the United States in NATO.

Main part. The focal point of the information war until 1999 was the United States Information Agency (USIA), which cooperated with the CIA and NSA, and which, when working in Russia, paid particular attention to the intelligentsia and young people. Since 1999, broadcasting functions were transferred to the Broadcasting Board of Governors (BBG), an independent federal agency that sets U.S. international broadcasting policy; and information functions were transferred to the U.S. Department of State, Office of International Information Programs (OIIP). Obviously, the former news agency is not independent in its activities, it is nothing more than a change of signboard while retaining the same functionality. According to experts from the newly formed structures, it is the intelligentsia and young people who make up the "selective groups" capable of influencing the development of domestic political processes in the future.

The strategy of negative information influence has been developed since the beginning of the Cold War, back in the days of A. Dulles. Dulles. Under R. Reagan created a special psychological warfare planning group headed by the Assistant to the President for National Security and consisting of the U.S. Secretary of State, CIA Director, Secretary of Defense, Director of the U.S. Information Agency (USIA), representatives of the FBI, the Pentagon and other high-

ranking officials. In the early 1980s, the Truth megaproject was launched, which later transformed into the global advocacy program "Democracy", which included 44 private projects on "specific issues". U.S. President Reagan declared a "crusade" against the Soviet Union and an important component of this "crusade" was information-sabotage operations, the cost of which rose to ten billion U.S. dollars. President George W. Bush, successor of Reagan, ordered the development of a new national strategy in the field of foreign policy "PR". As part of this strategy, a "Rapid Response Center" was created, whose specialists are engaged in rapid analysis of foreign media statements and immediate response to those of them in which the "wrong", from the point of view of manipulators, the policy of the U.S. administration is presented. Specialists are trained at the state level in this area. The direct conductors of information influence are the BBG and OIIP-controlled media. They are controlled through their multi-channel relationships with news agencies, advertisers, press syndicates, networks, and "public relations". Most of all information is monopolized by the two largest news agencies, News World Communications (the successor of United Press International (UPI)) and Associated Press (AP).

Their services are used by media representatives from 180 countries around the world. The volume of information transmitted is more than 70 million words a day (in English, French, Spanish and Arabic). More than three hundred press syndicates (the largest: New York News Syndicate, United Features, King Features, Newspaper Enterprise Association, Chicago Tribune, J. W. Thompson) operate in the American territory, whose services are used by the overwhelming majority of daily and weekly newspapers.

All military conflicts and aggressions unleashed by the U.S. in recent decades began with a preliminary powerful information pressure on the victim countries and the destruction of their national information security systems. Post-Soviet Russia was twice convinced of the validity of this conclusion: Russia lost the information war during the first Chechen campaign in 1994-1996; information-propaganda support was also extremely weak during the first phase of the conflict in Trans-Caucasus when Georgia's aggression against South Ossetia was repulsed. The next phase of the information war was the

operation to change the political regime in Ukraine and to form an openly anti-Russian nationalistic state there with an attempt to provoke the involvement of the two former Slavic republics of the USSR (now sovereign states) in a fratricidal conflict. Censorship, editing and filtering were applied to absolutely all statements of the Russian leadership that sought to convey the truth about the events in the Caucasus and Ukraine. Modern Western censorship, the counter-propaganda apparatus and information and psychological warfare services of NATO countries are far superior to their Soviet counterparts (while publicly denying the existence of the strictest censorship and making statements about "freedom of the press", "glasnost", "the right to information", etc., etc.) Through a system of media corporatization, through numerous NGOs and social networks, an attempt is being made to control information directly on the territory of Russia.

The U.S. think tank, the Defense Advanced Research Projects Agency (DARPA), developed an information warfare program against geopolitical rivals back in 2015. "The 2015 program includes the following subprograms:

"Social media in strategic communication," aimed at developing algorithms for identifying and tracking the formation, development, dissemination of ideas and concepts (memes) in social networks, which will further allow the independent and intentional initiation of propaganda campaigns, depending on the objectives of the region and U.S. interests. Among the stated objectives are dissemination of disinformation, recognizing the structures of propaganda campaigns and influence operations on websites and social networks, identifying participants, their intentions, measuring the effect of influence companies, countering hostile companies with counter-messages;

The "Abnormal Processes in Society" subprogram is designed to monitor individuals and social groups;

The subprogram "Proof of Aggression" provides for the creation of technologies for searching and comparing various bodies of information to obtain the necessary evidence of information warfare against the United States in order to initiate operational activities against the counterpart.

Events related to the change of the U.S. administration in 2017 and the hysteria on the eve

of the U.S. presidential election in 2020, which are associated with Russian interference in the internal affairs of this country, are evidence of the work of this program.

The efforts of specialists to influence the social consciousness of society are not limited to the above programs.

In the United Kingdom, a 2,000-strong military unit has been created that specializes in psychological warfare on social media, particularly on Facebook and Twitter. Its task is to accompany the waging of wars in social networks through the use of psychological attack tactics. A similar unit "Brigade 77" in the British armed forces appeared in 2015 and is based in Berkshire. There are similar cyber units in many armies around the world.

Against the backdrop of the civil war in Ukraine, the Ukrainian Ministry of Information Policy has announced a recruitment drive for information troops, which operate in close coordination with Psychological Operations groups. Anyone interested is invited to register on a special website and receive daily e-mail assignments to attack Russian-language sites. Given the U.S. role in the events in Ukraine, we must assume that the creation of such units is under the control of the CIA.

The CIA has established a new Directorate of Digital Innovation to work on the "cyber front," which is responsible for tracking advances in cyber technology and using them in the agency's operations. This division has equal status with other directorates that have existed for many years. Until now, at the CIA, interception and monitoring of information was predominantly handled by the National Security Agency (NSA). BBG and OIIP, CIA, specialized military units control social processes, both in their own society, and try to influence the social sphere of the alleged geopolitical enemy, which the U.S. has declared Russia, China and North Korea to be. In the U.S. National Security Strategy adopted in 2017, "The U.S. National Security Strategy adopted in 2017, Russia is mentioned 14 times as the main adversary [1].

In accordance with the "Proof of Aggression" program, with regard to Russia, the United States applies a set of recurrent information stamps (HRCs), which play the role of pretexts to justify informational (and not only) aggression and which, depending on the situation, can be filled with new content or create new ones

(Olympic doping - case, poisoning Skripal (Navalny) - case, interference in elections - case, etc.). With regard to the PRC, which has significant economic and military potential, at the moment "hybrid warfare" is carried out mainly in the economic sphere (economic sanctions), although information HR-cases (Uighur separatist, Hong Kong democratic, student, Tiananmen Square events, LGBT-case, etc.) are always ready for use. Their own set of H-cases is used against the DPRK (the latter related to the perfidy of the Koreans who do not want nuclear disarmament unilaterally).

The U.S. National Security Strategy states that the policy of containment of Russia will now be conducted openly and even more fiercely, regardless of political changes within the United States. In full accordance with this policy and regardless of which political party controls the White House (Trump or Biden), a set of measures for the unconditional dominance of the United States in the world is being implemented. The provision that the U.S. must be prepared to wage preventive wars (in fact, aggression against countries, an attack by which the U.S. considers possible) is also alarming. And if you consider that in the introduction to the previous Strategy-2015 it was written: "The question is not whether or not America should lead. The question is how we should lead... We are united by a shared national conviction that America's global leadership remains immutable. The motif of America's global leadership remains in the new Strategy: "The whole world is elevated by the renewal of America and the resurgence of American leadership" [2].

Conclusion. Thus, it can be argued that the "Proof of Aggression" program, involving the use of H.Q. technology, is a direct preparation of public opinion of the U.S. population and its allies for a preventive war. Former U.S. President Barack Obama approved the placement of cyberweapons in the Russian infrastructure, at the same time U.S. intelligence agencies were instructed to find weaknesses in the Russian infrastructure, the instruction was contained in the unpublished part of the sanctions package against Russia. The prepared program involves the introduction of certain "implants" developed by the U.S. National Security Agency into important Russian infrastructure networks. The decision to deploy the program was made by former U.S. President Donald Trump, but even

without his approval, the intelligence services could continue to develop it.

The U.S. president has conditioned Washington's use of cyber weapons on compliance with the principle of "escalatory dominance. This refers to the potential guarantee of the U.S. ability to end the conflict on its own terms. And in confirmation of its intentions, the U.S. is implementing the Footage vs Footage video project in Russian social networks.

The goal of the video project is to discredit "Russian television propaganda. At the same time, the YouTube channel and the Rus2Web website are creating conditions for the work of Russian opposition journalists and bloggers (a prominent representative of which is A. Navalny). According to the publication, BBG has significantly expanded Voice of America's cooperation with Russian media from 2017-2020, in particular with the RBC-TV channel, which has a monthly reach of about 22.4 million people in Russia and 5.4 million people in Moscow. "The Voice of America and RBC-TV plan to expand their co-produced content to 60 minutes a week, using studios (Voice of America) and journalistic resources in Washington and New York," according to BBG.

As a result, the hybrid war against the Russian Federation in the information sphere continues. In full accordance with the provisions of the "Proof of Aggression" program, h-Cases activities of the state as the initiator subject are indirect, i.e. carried out with the help of executing subjects and any outside participants, so its attribute has become a kind of "outsourcing", i.e. attraction of outside specialists or creation of fictitious hacker associations. Recent events with various virus epidemics, attacks on websites and information systems of government and commercial institutions, ministries and agencies that took place around the world from 2017 to 2020 confirm this conclusion.

On this basis, we can conclude that both the "cold war" (which resulted in the defeat of the USSR without a single shot fired) and numerous changes of political regimes in the territories formerly under Russian control, as well as the latest attempted coup d'etat in the Republic of Belarus, were the result of skillfully organized information influence.

Contemporary political scientist A. Panarin notes that: "Now history does not happen on a whim, spontaneously. It is now done conscious-

ly, one might say - by order of the powers that be," and the reasons why such a thing has become possible today are as follows:

- 1) progress in the means of collecting, processing and transmitting information;
- 2) the progress of the means of communication;
- 3) progress of means of manipulating people, supervising them, suppressing and initiating mass movements;
- 4) the influence of mass culture on the standardization of people's way of life [3, p.172].

Development of technologies of information influence has shown that the most effective impact through the presentation of certain information is carried out in the sphere of intercultural communication [4, p. 174].

The sphere of culture is the sphere of competition of spiritual values - the values that constitute the basis of individual and public consciousness of people, which, materializing, create a certain type of material and practical relations in society (spiritual values determine the economic system, and that in turn - the political regime).

The development of information influence technologies has led to the fact that "The degree of unpredictability and surprise of historical events has been sharply reduced in comparison with the sharply increased degree of predictability and planning. And the Cold War of the West, led by the United States, against the Communist East, led by the Soviet Union, was from the beginning a grand planned operation, in cost, scope and results the grandest human operation on a global scale. It had many of the unplanned, unforeseen, uncontrollable things that are inevitable even in small operations. But in general, in the main, in the decisions determining the course of the process it was just like that" [5, p. 12].

The fact of the emergence of information space leads to the emergence of those wishing not only to divide this space, but also to control and manage the processes occurring in it. For this purpose, the so-called information weapons are used, which are means of destroying, distorting or stealing information; means of overcoming protection systems; means of restricting access of legitimate users; means of disorganizing the work of technical means and computer systems. We can say that information weapons are the very use of information and information-networking technologies to influence military

and civilian cybernetic systems, as well as the public consciousness [6, p. 130].

Thus, in the era of hybrid wars, an integral part of which are neo-terrorism, information violence, disinformation and systemic cyberattacks [7, p. 25], objectively there is a need to develop a comprehensive theory of security of the sphere of social consciousness of the Russian society and the implementation of relevant measures to create a more effective system of information protection of the Russian state [8, p. 222].

References

1. National Security Strategy of the United States of America December 2017. Available at: <http://nssarchive.us/wp-content/uploads/2017/12/2017.pdf> (accessed: 02.03.2021).
2. Report to Congress on 2017 U.S. National Security Strategy. Available at: <https://news.usni.org/2018/01/05/report-congress-2017-u-s-national-security-strategy> (accessed: 16.03.2021).
3. Panarin A.S. *Iskusheniye globalismom* [The Temptation of Globalism]. Moskva: Russkij mir, 2000, pp.172. (In Russian)
4. Sokolova, S.N. Kalenchuk, T.V. Neoterrorism i informatsionnaya bezopastnost' [Neoterrorism and information security]. *Bezopastnost' tseloveka i obshchestva: sovershenstvovanie systemy reagirovaniya I upravleniya zashchitoy ot tsezvychajnykh situastij: Sbornik materialov II Mezhdunarodnoj ochnoj nauchno-prakticheskoy konferenchi* [Security of man and society: improving the system of response and management of emergency protection: coll. materials of the II International full-time scientific and practical conference]. Minsk: UGZ, 2018, pp. 170-174. (In Russian)
5. Zinoviev A.A. *Intervjy zhurnaly "Rossijskaja Federatsiya segodny"* [Interview to the Russian Federation Today magazine]. M., 2000, no. 18, pp.12. (In Russian)
6. Brychkov A.S., Nikonorov G.A., Sokolova A.A., Sokolova S.N. [et al]. *Duhovnye izmenenie gibridnoj vojny v informatsionnoj sfere: tsennistnyj aspekt. Gibridnye vojny XXI stoletija: proishogdenie, sushchnost' i mesto v tsivilizatsionnom protsesse* [Spiritual Dimension of Hybrid Warfare in the Information Sphere: Value Aspect. Hybrid War-

fare of the 21st Century: Origin, Essence and Place in the Civilization Process]. Smolensk: VA VPVO Armed Forces of the Russian Federation, 2019, pp. 306. (In Russian)

7. Sokolova A.A., Kalenchuk T.V., Sokolova S.N. Neo-terrorism in the information society as a basic element of hybrid warfare strategy. *Vestnik Polesskogo gosudarstvennogo universiteta. Seriya obshhestvennykh i gumanitarnykh nauk* [Bulletin of Polesky State University. Series in Social Sciences and Humanities]. 2021, no. 2, pp. 21-27.
8. Sokolova A.A., Sokolova S.N. Infosphere and fundamental values in the age of hybrid wars *Aktual'nye ekologicheskie problem* [Actual ecological problems]. 2021. Minsk. BGU, pp. 222.

Список литературы

1. National Security Strategy of the United States of America December 2017. – [Электронный ресурс]. – Режим доступа: <http://nssarchive.us/wp-content/uploads/2017/12/2017.pdf> – Дата доступа: 02.03.2021.
2. Report to Congress on 2017 U.S. National Security Strategy. [Электронный ресурс]. – Режим доступа: <https://news.usni.org/2018/01/05/report-congress-2017-u-s-national-security-strategy>. – Дата доступа: 16.03.2021.
3. Панарин, А. С. Искушение глобализмом / А. С. Панарин. – М.: Русский мир, 2000. – С.172.
4. Соколова, С. Н. Нео-терроризм и информационная безопасность / С. Н. Соколова, Т. В. Каленчук // Безопасность человека и общества: совершенствование системы реагирования и управления защитой от чрезвычайных ситуаций: сб. материалов II Международной очной научно-практической конференции. – Минск: УГЗ, 2018. – С. 170-174.
5. Зиновьев, А. А. Интервью журналу «Российская Федерация сегодня» / А. А. Зиновьев. – М., 2000, № 18. – С.12.
6. Брычков, А. С. Духовное измерение гибридной войны в информационной сфере: ценностный аспект / Угрозы гибридных войн в современном обществе / Гибридные войны XXI столетия: происхождение, сущность и место в цивилизационном

- процессе: монографія / А. С. Брычков [и др.]. – Смоленск: ВА ВПВО ВС РФ, 2019. – 306 с.
7. Соколова, А. А. Neo-terrorism in the information society as a basic element of hybrid warfare strategy / А. А.Соколова, Т. В. Каленчук, С. Н. Соколова // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – Пинск, 2021. – № 2. – С. 21-27.
8. Sokolova, A. A. Infosphere and fundamental values in the age of hybrid wars / А. А. Sokolova, S. N. Sokolova // Актуальные экологические проблемы: тезисы XI международной научной конференции молодых ученых, аспирантов, магистрантов, студентов. 2-3 декабря 2021. Минск: БГУ. – С. 222.

Статья поступила 22 March 2022 г.