ФИЛОСОФСКИЕ НАУКИ

УДК 32.1 (04): 1(04)

BRICHKOV A.S., Doctor of Philosophy, Associated Professor[1]

NIKONOROV G.A., PhD in Philos. Sc., Associated Professor[1]

PERTSEV A.A.
Cadet[1]
[1]The Russian Federation Armed Forces Army Air Defense Military Academy, Smolensk, Russian Federation

Received 21 March 2023

RUSSIAN INFORMATION SPACE IN THE ERA OF «HYBRID WAR»: DEFENSE OR ATTACK[1]

The article deals with analysis of information security of Russian society individual and public consciousness state. Tasks, forces and means of destructive information influence are defined; conclusion is made about realization of long-term strategy regarding Russian society which is inherent part of hybrid warfare of united Western world led by the USA against Russian Federation and its allies.

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

[1]Статья публикуется в авторской редакции.

А.С. БРЫЧКОВ, доктор филос. наук, профессор[1]

Г.А. НИКОНОРОВ, канд. филос. наук, доцент[1]

АА. ПЕРЦЕВ, курсант[1]

[1]Военная академия войсковой ПВО Вооруженных Сил Российской Федерации,
г. Смоленск, Российская Федерация

РОССИЙСКОЕ ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО В ЭПОХУ «ГИБРИДНОЙ ВОЙНЫ»: ЗАЩИТА ИЛИ НАПАДЕНИЕ

В статье предпринята попытка анализа состояния информационной безопасности сферы индивидуального и общественного сознания российского общества. Определены задачи, силы и средства деструктивного информационного воздействия, сделан вывод о реализации долгосрочной стратегии в отношении российского социума, которая является неотъемлемой частью «гибридной войны» объединнного Запада во главе с США против Российской Федерации и ее союзников.

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

Generally speaking, in the age of information society human being constantly connected to information space becomes the bearer of spiritual values. Information space serves as a confrontation arena for traditional societies and civilizations. National values in the sphere of public consciousness are to be protected against internal and external threats in information age.

Hence it is impossible to look into the state of public consciousness without analysis of processes in information space.

The state of Russian public consciousness reflects the degree of negative information influence and allows to define its methods and ultimate goals. Thus, the degree of information corruption of public consciousness is defined by its destroyed parts or by ones fulfilling other from its own social system goals.

Threats created by adversaries in political, economic and military spheres are materialized threats in the public consciousness sphere. More than 30 years of new Russian statehood allow to understand that the direction of pressure put on Russia does not change with time. The history of Russian statehood shows that confrontation has geopolitical character and attitude of geopolitical adversaries towards our country does not change with form of governance, state system or political regime.

Confrontation of Western world and Russia has a deep ideological (civilization) character. It results in armed hostilities during wars and in negative information influence during peacetime. Development of information technologies and formation of post-information society allows for such a wide-scale utilization of information influence on geopolitical civilizations-adversaries that it can be said that there is an information warfare going on.

Information warfare is a planned information influence on all info-communication system of adverse and neutral states to create favorable global information environment for conduct of political and geopolitical campaigns providing maximum control over space and resources of adversary.

The of information warfare is to disrupt technical systems of governance and military management and to put negative disruptive influence on individual and public consciousness in order to disorganize and destroy the society of adverse state.

The purpose of disruptive information influence is to weaken overall society potential which causes decrease in security level in all spheres (including military).

Subjects of disruptive influence are the USA and members of the European Union supporting the USA in the framework of NATO.

Until 1999 the United States Information Agency was the coordination center of information warfare cooperating with CIA and NSA which put great emphasis on intellectuals and youngsters working against Russia. Since 1999 broadcasting functions were delegated to Broadcasting Board of Governors - independent feder-

al agency which defines the policy of international broadcasting of the USA, information functions were delegated to United States Department of State, Office of International Information Programs. No doubts, there just cannot be any independence in the operation of former information-propagandistic agency – it is just a change of signboard with function being the same. From the experts' point of view, it is intellectuals and youngsters who make up those «sample groups» able to affect internal political processes.

The strategy of negative information influence was developed in the beginning of cold war, during A. Dulles presidency. Under R. Reagan administration special psychological warfare group was created. It was led by national security adviser and included US Secretary of State, director of CIA, Defense Secretary, director of USIA, members of FBI, Pentagon and other high-ranking officials. Since its creation USIA spread information only abroad because the Congress of USA prohibited to conduct information operations on the territory of the USA. In the beginning of 1980s realization of mega project «Truth» started which was later transformed into global propaganda program «Democracy». 44 particular projects regarding «specific problems» were conducted in the framework of this program. President of the USA R. Reagan claimed «crusade» against the USSR and information diversion operations which costs rose up to $10 billion became an important part of it. Reagan's successor G. Bush authorized the development of new national strategy regarding «foreign PR» «Rapid reaction center» was created in the framework of this strategy. Its specialists conduct operational analysis of foreign mass media and immediately react if, according to manipulators' perspective, the policy of USA government is presented «wrong». Training of such specialists is launched on state level.

First-hand retranslators of information influence include mass media controlled by BBG and OIIP They are administrated via multilateral links to information agencies, advertisers, press syndicates, network structures and PR-organizations. Major part of all information is monopolized by the two largest information agencies - media companies «United Press International» and «Associated Press».

Mass media from 180 countries around the world use their services. The amount of transmitted information is more than 70 million words per day (in English, French, Spanish and Arabic) On American soil there are more than 300 operating press syndicates (the largest are «New York News Syndicate», «United Feature», «Newspaper enterprise association», «Chicago Tribune», «G.U. Thompson») which services are used by major part of everyday and weekly newspapers.

All military conflicts and acts of aggression unleashed by the USA in last decade began with preliminary powerful information pressure on targeted country and destruction of its national information security system. Post-Soviet Russia had an opportunity to prove this point twice: Russia lost information war during first Chechen campaign in 1994-1996; there was also extremely weak information-propaganda support during first phase of conflict in Transcaucasia reacting to aggression of Georgia against South Ossetia. The next phase of information war was a regime-change operation in Ukraine and forming of explicit anti-Russian nationalistic state there to provoke two former Slavic republics of USSR (nowadays - sovereign states) to fall into fratricidal conflict. Any statement of Russian government trying to tell the truth about events in the Caucasus and Ukraine are subjects to censorship, editing and filtering. Modern Western censorship, propaganda system and information-psychological warfare services of NATO members significantly surpass all Soviet counterparts (publicly denying the fact that they possess the most severe censorship and claiming «press freedom», «publicity», «right to information» etc.) An attempt to control information flows on the territory of Russia is exercised via mass media incorporation system and numerous non-governmental organizations. In May of 2005 a special group for enemy (anyone dissent with policy and ideology of Anglo-Saxons) suppression in social networks was created in Pentagon. Military hacker group which started as a "pilot project" resulted in creation of cyber force as a separate branch of armed forces of USA, and then - members of NATO. Analytic center of USA - Defense Advanced Research Projects Agency (DARPA) developed an information warfare program against geopolitical rivals in 2015. «Program – 2015» includes the following subprograms:

«Social Media in Strategic Communication»

- aimed to develop identification and tracking algorithms for formation, development, dissemination of ideas and memes in social networks. In future it will allow to independently and deliberately initiate propaganda campaigns according to regional tasks and interests of the USA. Among claimed goals there are disinformation proliferation, propaganda campaign structure identification and influence campaigns on websites and social networks, identification of members and their intentions, change of effects of influence campaigns, counteraction to adverse campaigns via counter messaging;

«Abnormal processes occurring in society» - aimed to monitor separate individuals and social groups.

«Proof of aggression» - provides for creation of search technologies and comparison of different data arrays in order to get required proofs of information warfare led against the USA to start counteracting.

Events related to the USA administration change in 2017 and hysteria right before presidential election in 2020 and tried to be linked to Russia interference into internal affairs of that country, and also the same information agenda after the initiation of special military operation in Ukraine proves that the program is active.

Specialists' efforts to influence public consciousness of society are not limited to these programs. In the UK, there is a military unit consisting of 2000 people specialized in psychological warfare in social media, particularly in Facebook and Twitter. Its task is to support actual warfare in social networks by the use of offense psychological tactics. One of such units, «Brigade 77», was created in the British armed forces in 2015 and based in Berkshire. There are similar cyber forces in many armed forces of other states. Against the background of the civil war in Ukraine the Ministry of Information policy of Ukraine announced the recruitment into information forces which operate in close cooperation with psychological operation group. Volunteers are suggested to sign in special website and daily receive emails with tasks to attack Russian websites. Taking the role of the USA in events in Ukraine, it should be assumed that it is CIA that administer creation of such units.

New Digital innovation directorate was established in CIA. It is tasked with monitoring of cybertechnologies development and the use of them for agency operation. This directorate has the same status as other departments which existed for many years. Until today the task of information interception and monitoring was mainly given to National Security Agency (NSA).

BBG and OIIP, CIA, specialized military units exercise control over social processes in own society and also try to influence social sphere of supposed geopolitical adversary - as claimed by the USA, Russia, China and DPRK. In USA National Security Strategy of 2017 Russia is called major opponent 17 times [1].

According to «Proof of aggression», the USA uses a set of repeating information cliches (H-cases) against Russia. They are used as pretexts to excuse informational (and other) aggression and may be filled with new content (doping during Olympic games case, poisoned Skripal (Navalny) case, election interference case, Russian aggression against Ukraine case etc.).

«Hybrid warfare» regarding China is mainly conducted in economic sphere due to China's significant economic and military potential via economic sanctions. But information H-cases are always ready to use (Uyghur-separatist case, Hong Kong-democratic case, student case linked to events on Tiananmen square, LGBT case, Taiwan case etc.). Specific set of H-cases is used against DPRK (the last one was linked to Koreans' cunning unwilling to fulfill unilateral nuclear disarmament) and Iran («terror stronghold» in the region).

National Security Strategy of the USA claims that deterrence policy towards Russia will be led more publicly and harshly political regardless of political changes in the USA. In full accordance with that set and regardless of member of which political party controls the White House (Trump or Biden) range of activities aimed to gain unquestionable dominance of the USA is under go. There are concerns regarding preparedness of the USA to conduct a preventive war (in fact it is aggression against states the USA finds possible to be attacked by). If we take into consideration that in the introduction of previous Strategy-2015 it was written that «… The question is never whether America should lead, but how we lead ... What unites us is the national consensus that American global leadership remains indispensable». The motive of global leadership of America stays in a new Strategy: «… The whole world is lifted by America's renewal and the reemergence of American leadership» [2].

Hence it may be claimed that “Proof of aggression” program assuming the use of H-cases is direct preparation of public opinion of American citizens and citizens of allies to preventive war.

Former US president Barak Obama approved deployment of cyberweapon in Russian infrastructure. At the same moment American special services were tasked to find weak spots in Russian infrastructure. The task was written in an unpublished part of sanction package against Russia. Prepared program suggests infiltration of so called «implants» developed by NSA into important Russian infrastructure networks. It was USA former president Donald Trump who decided to start this program, but even without his approval special services could continue its development. And current USA President Baden, after failed attempt to solve the situation regarding the USA influence sphere in the world with Russian Federation President V. Putin «good way», openly switched to other strategy - prolonging of Ukrainian crisis in order to weaken Russia by weapon supply from the territory of NATO members and information warfare against Russian Federation. It resulted in total block of Russian information sources on the territory of EU and the USA.

American president claimed «escalation dominance» principle as a premise for Washington to use cyber weapons. It is about potential guaranty of the USA to stop conflict (including one in Ukraine) on their own demands. To prove their point, USA created a video project called «Footage vs Footage» in Russian social media. The goal of this project is to discredit «Russian information propaganda» At the same time YouTube and Rus2Web creates favorable conditions for Russian opposition journalists and bloggers (as a vivid example - A. Navalny).

According to BBG data collected in 2017-2022, “Voice of America” increased level of cooperation with Russian mass media, particularly with RBK-TV channel. Its monthly coverage is about 22.4 million people in Russia and 5.4 million people in Moscow. And opposition channel «Echo of Moscow» closed after the beginning of special military operation has the most reliable radio signal and sustainable funding. «Voice of America» and RBK-TV planned to extend time of co-produced content up to 60 minutes per week cooperating with studios (“Voice of America”) and journalist resources in Washington and New York. The main theme of that broadcast would be Russian aggression against Ukraine, as claimed in BBG materials.

Considering that, hybrid warfare against the Russian Federation in information domain is continuing. In full accordance with «Proof of aggression» program a state uses proxies as subjects-initiators and any third parties to conduct h-cases operation. These proxies are characterized by «outsourcing» meaning hiring of third-party specialists or creation of fake hacker groups. The last events related to various virus epidemics, attacks on websites and information systems of government and commercial establishments, ministries and services, full information blockade of Russian mass media after February of 2022 prove this point. The conclusion is that «cold war» (which resulted in USSR loss without any shot fired) and numerous changes of political regimes on territories previously controlled by Russia and also the last attempt to overthrow government in Belarus and Kazakhstan were the result of carefully designed information influence. Philosopher and political scientist A. Panarin said that: «Nowadays history doesn’t happen capriciously, spontaneously. It is made deliberately; I can even say - by the order of powerful ones of our world».

The reasons why it became possible today are as follows:

1) Development of collection, processing and transmitting of information;

2) Development of communication means;

3) Development of population surveillance and control, mass movement initiation and termination systems;

4) Standardization of people’s lifestyle caused by mass culture [3].

Practicing information influence technologies showed that the most effective way method of influencing via information is in cultural communication sphere. Cultural sphere is a sphere of spiritual values competition. These values form up a basis of individual and public consciousness of people, which, after being realized, create a specific type of material relationship in society (cultural values determine economic system, and it determines political regime in its turn). The development of information influence technologies resulted in “drastic reduction of unpredictability and unexpectedness degree of historical events together with rapidly raised degree of predictability and planning, and «cold war» of the West led by the USA against the

communistic East led by the Soviet Union was from the very beginning a grand planned operation by its cost, scale and results «… There was a lot of unplanned, unforeseen and uncontrolled - it is unavoidable even in small operations. But overall, as a whole, in key processes it was just like that» [4, p.12].

The emergence of information space leads to desire not only to divide it, but to control and run processes happening in it. To do it, so called information weapon which is means of destruction, distortion or stealing of information; means of security system bypass; means of legitimate users' access restrictions; means of technical equipment and computer systems disruption. It may be said that information weapon itself is the use of information and information technologies to influence military and civil cybernetic systems and also public consciousness.

Over the 30 last years covered a period from «perestroika» led to the largest geopolitical catastrophe before «hybrid warfare» happening between Ukraine with Russian Federation and the USA with its allied members of NATO showed effectiveness of information influence on geopolitical enemy and necessity to build systems of information offense and defense.

Considering unprecedented in scale, deployed forces and means information war waged against the Russian Federation (especially after special military operation started in Ukraine) it is absolutely necessary to:

1) Build a system of information protection on population and the territory of state. It provides active offensive information cations against geopolitical adversary in domains of government and military management technical systems as well as cultural domain.

2) Develop and conduct preventive measures for affected part of society government structure (closure of and claiming an array of opposition mass media as "foreign agent" in vividly not enough).

3) Conduct a set of political and economic measures aimed at stabilizing of extremely disturbed due discontent caused by internal and external policy led from 1991 to our days Russian society. There are a lot of discounted people in the state, which creates a pleasant condition for destructive information influence and «hybrid warfare»). Foreign economic sanctions against Russia are designed to worsen state of people masses to enlarge protest base. Without great social reforms in the interests of major part of society there is no sense to create an internal and external Russian society protection system from destructive information influence. Without complex solution for Russian societal crisis strengthening of defense and ensuring of military security of Russian Federation is impossible because armed forces are the part of society [5, p. 106].

To build a system of information protection on population and the territory of state during «information war» it is necessary to:

1) Monitor information from every foreign incoming source.

2) Terminate or distort beyond recognition harmful information (which is not meet national values in spiritual sphere and enabling for disintegration of government and military administration).

3) Create a powerful structure to broadcast undermining information on the territory and information space of geopolitical adversary.

4) Using all information channels and their potential, create a flow of neutral advertisement content regarding own lifestyle into neutral states and their information space from the territories not affected by information war (this flow should exceed overall information flow regarding Russia).

To do so, the following should be done:

1) all governmental and nongovernmental (in which government has a controlling stake) information companies must be united into information holding under government ministry of information status;

2) measures must be taken to control all information companies with no governmental participation;

3) opening of new companies must be ceased and operation of companies with foreign funding must be legally prohibited;

4) internal information policy must be changed from entertaining to educational, patriotic and scientific;

5) information monitoring service with censorship functions under direct command of the President must be created;

6) in mentioned service following department must be created: information security of state and society system; information warfare and special operation; information affection prevention;

7) information campaigns abroad must be initiated, including ones enabled by privatization by individuals followed by ministry of information taking control over them;

8) In the condition of full information blockade applications for mobile devices (connected via satellite network, free and easy to install) receiving around-the-clock broadcasting on user's language from Russian Federation must be created (also other technical measures to pierce information blockade regarding Russian Federation via the Internet and other channels of information may be taken);

9) system of information warfare personnel training must be created;

10) human resources of creative community, scientists, public activists, members of religious confessions who are willing to cooperate with mention service must be used;

11) mentioned information system must cover all ages and professions, especially state law enforcement personnel.

Central administration service (state ministry of information) must become the main Russian society information security system.

The most important functions of central information security service would include:

1) Intelligence conducted for timely countermeasures against information aggression acts.

2) Planning and organization of different activities regarding mentioned intelligence.

3) Direct management of forces and means and overall support of their actions.

4) Conduct of scientific studies on information offense and defense.

5) Coordination of interaction of all system departments and services.

6) Information influence effects control.

In addition to mentioned functions other activities will fall under central management service jurisdiction. In particular, they may include analysis of geopolitical and political situation, suggestions regarding information security and key guidance documents, structure, composition, location and tasks of system components, definition of requirements for technical means etc.

These are general actions which needs to be detailed during their implementation. The degree of completion of tasks given to individual element should be considered criterion of operation efficiency of individual units and structures of suggested system, *and the change of crisis social-political situation in the country and the degree of initiation of negative processes on the territory and in the information space of geopolitical counterpart (USA, EU and other influenced countries).*

Considering this, *it is necessary to create a system of information security of state territory (with an option to conduct defensive and offensive information operations). To create this system, the complex of different actions must be fulfilled (juridical, technical, management, human resource etc.).* It is vivid that in the age of hybrid warfare with information warfare being inherent part of it the necessity of Russian society public consciousness security maintenance theory and set of mentioned measures is urgent [6, p. 28]. Armed conflict in Ukraine showed that despite pro-Russian position of main Russian federal and regional mass media regarding it clearly there is incoherence and even ill-reasoned information agenda. This gives geopolitical counterparts a possibility to report the facts as they want more rapidly and even create a virtual universe (Russian mass media constantly find themselves in excuse position). Given no ability to broadcast to Western audience (the blockade of information channels, creation of environment in which it is impossible for foreign journalists to work, prosecution of ones who try to gain access to information coming from Russian Federation up to satellite antennas confiscation etc.), it is necessary to consider reflective measures aimed to completely prohibit adverse mass media on the territory of Russian Federation. In the condition of "hybrid warfare" fought against Russian Federation with information warfare being its inherent part all previous ideas of democracy and freedom of press must be forgotten. Information is weapon [7, p. 222]. *The main problem of Russia in information domain is the absence of central service for effective information confrontation.*

Thus, security of Russian society public consciousness requires large-scale measures. This is the most preferable variant as geopolitical processes (initiated «hybrid war» against Russia, the USA leaving key international treaties and public calls for the change of authorities of state, armed conflict in Ukraine started by the USA) show that there is almost no time left [8, p. 16].

References

1. National Security Strategy of the United States of America December 2017. Available

at: http://nssarchive.us/wp-http://nssarchive.us/wp-content/uploads/2017/12/2017. Pdf.
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
3. Panarin A.S. *Iskushenie globalizmom* [Temptation of globalism]. Moscow. Russian world, 2000, pp. 172. (In Russian)
4. Zinoviev A.A. *Interv`yu zhurnalu Rossijskaya Federacziya segodnya* [Interview to «Russian Federation today» magazine]. 2000, no. 18, pp. 12. (In Russian)
5. Sokolova A.A., Sokolova S.N. The media sphere and personal security in the information society. *Vestnik Polesskogo gosudarstvennogo universiteta. Seriya obshhestvenny`kh i gumanitarny`kh nauk* [Bulletin of Polessky State University. Series in Social Sciences and Humanities]. Pinsk, 2022, no. 1, pp. 106-112. (In Russian)
6. Sokolova A.A., Sokolova S.N. The age of hybrid wars and neo-terrorism in the information society *Vestnik Polesskogo gosudarstvennogo universiteta. Seriya obshhestvenny`kh i gumanitarny`kh nauk* [Bulletin of Polessky State University. Series in Social Sciences and Humanities]. Pinsk 2021, no. 1, pp. 26-34. (In Russian)
7. Sokolova A.A., Sokolova S.N. Infosphere and fundamental values in the age of hybrid wars December 2-3, 2021. *Aktual`ny`e e`kologicheskie problemy`* [Current environmental problems]. Minsk, BSU, pp. 222. (In Russian)
8. Sokolova A.A., Sokolova S.N. Neo-terrorism as a resource for hybrid wars. *Vestnik Polesskogo gosudarstvennogo universiteta. Seriya obshhestvenny`kh i gumanitarny`kh nauk* [Bulletin of Polessky State University. Series in Social Sciences and Humanities]. Pinsk, 2022, no.1, pp. 16-21. (In Russian)

Список литературы

1. National Security Strategy of the United States of America December 2017. – [Электронный ресурс]. – Режим доступа: http://nssarchive.us/wp-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 – Датадоступа: 16.03.2021.
3. Панарин, А. С. Искушение глобализмом / А. С. Панарин. – М.: Русский мир, 2000. – С. 172.
4. Зиновьев, А. А. Интервью журналу / А. А. Зиновьев // Российская Федерация сегодня – 2000. – № 18. – С.12.
5. Соколова, А. А.The media sphere and personal security in the information society / А. А. Соколова, С. Н. Соколова // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – Пинск, 2022. – №1. – С. 106-112.
6. Соколова, А. А. The age of hybrid wars and neo-terrorism in the information society / А.А. Соколова, С.Н. Соколова // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – Пинск, 2021. – №1. – С. 26-34.
7. Sokolova, A. A. Infosphere and fundamental values in the age of hybrid wars / A. A. Sokolova // Актуальные экологические проблемы : тезисы XI международной научной конференции молодых ученых, аспирантов, магистрантов, студентов. 2-3 декабря 2021. – Минск : БГУ. – С. 222.
8. Соколова, А. А. Neo-terrorism as a resource for hybrid wars / А. А. Соколова, С. Н. Соколова // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – Пинск, 2022. – №1. – С. 16-21.

Статья поступила 21 марта 2023 г.