www.volsu.ru

DOI: https://doi.org/10.15688/jvolsu4.2020.3.14

UDC 94(41/99)
LBC 66.4

Submitted: 12.08.2019
Accepted: 20.11.2019

CURRENT ISSUES OF INFORMATION SUPPORT OF RUSSIAN FOREIGN POLICY IN THE NEW POLITICAL ENVIRONMENT

Petr V. Menshikov
MGIMO University, Moscow, Russian Federation

Aida Ya. Neymatova
MGIMO University, Moscow, Russian Federation

Abstract. *Introduction*. In the context of growing anti-Russian information wars, intensive and sharp ideological confrontation active information support of Russia's foreign policy becomes more and more crucial. *Methods*. Authors use mainly the methods of expert evaluation and trends, opinion polls to prove that the US has long been waging information wars against Russia first using the term ("information war") back in 1992. Moreover, with time the United States makes the methods of struggle more and more sophisticated and has already attracted the EU and NATO as associates. In addition, the methods of comparative analysis of research results of leading domestic and foreign experts in the field of information and ideological component of modern international relations and issues of information support of foreign policy of the Russian Federation, as well as general scientific and special methods of knowledge of legal phenomena and processes made as the object of the research: the method of systematic and structural analysis, comparative legal and formal-logical methods have been used. *Analysis*. Along with the tools of public diplomacy our state takes all the needed measures to defend its information sovereignty at all levels. Despite the fact that the Russian state strategy has consistently created a system of detecting, preventing and eliminating threats to its information security, still it is necessary to deal with ever growing amount of anti-Russian false information in the global media space. *Results*. Being one of the instruments of public diplomacy and foreign policy of any sovereign state, soft power takes into account the objective conditions of international relations and world politics and proceeds from the requirements of the national interests of the state as the main actor of the entire system of modern international relations. In the world practice of implementing the policy of soft power, starting with the creation of the Westphalian system of international relations, there was no precedent, when the state regardless of the socio-political nature of building a political system or the purposes of the foreign activity would be guided by different objectives and methods of analysis of world politics, the entire system of international relations and other goal-setting action in the international arena, including defined in the last decade by the concept of soft power. In the history of international relations, there has not been any world policy free from its ideological component. The thesis of de-ideologization of international relations, which received its definite distribution in the period immediately after the collapse of the Soviet Union, in the practice of foreign policy actions of all the main actors of modern world politics has clearly proved its complete failure. Today, in the context of "hybrid wars" within the entire system of international relations, the world politics is no less ideologized than during the "cold war". The political leadership of Russia allows the hypothetical possibility of cyberwarfare, provoked by the actions of the Republican administration of the United States. In December 2019, the White House authorized the preparation of a plan for conducting an information war with the Russian Federation by special forces of the U.S. Army, assigning the solution of this task to the above-mentioned cyber command. The policy of soft power of Russia, as well as its public diplomacy, as the whole complex of foreign policy activities of the Russian Federation in the international arena, is derived from the fundamental function of defending the national interests of Russia in the new political reality. The Russian Federation has consistently opposed the transformation of international relations into an arena of ideological confrontation with the use of tools of the so-called "information wars". State sovereignty is unified. Information security, as a factor of ensuring information sovereignty, is a basic component of the unified state sovereignty. This is an accepted truth underlying the understanding of the nature of modern international relations, the principle underlying the foreign policy activity of any modern sovereign state, due to the objective regularity of the growth of the ideological factor of modern international relations. Moreover, in the face of targeted misinformation Russia needs to ensure its information security at both levels:

political (ideological) and technical (technological) ones combining cyber as well as soft power tools. Only such a combination of these two crucial elements and continuous improvement can lead to victory in hybrid wars.

Key words: information policy, information security, information infrastructure, foreign policy PR, soft power, public diplomacy, "hybrid wars", cyber war.

Citation. Menshikov P.V., Neymatova A.Ya. Current Issues of Information Support of Russian Foreign Policy in the New Political Environment. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 4. Istoriya. Regionovedenie. Mezhdunarodnye otnosheniya* [Science Journal of Volgograd State University. History. Area Studies. International Relations], 2020, vol. 25, no. 3, pp. 161-171. DOI: https://doi.org/10.15688/jvolsu4.2020.3.14

УДК 94(41/99)
ББК 66.4

Дата поступления статьи: 12.08.2019
Дата принятия статьи: 20.11.2019

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ ВНЕШНЕЙ ПОЛИТИКИ РОССИИ В НОВЫХ ПОЛИТИЧЕСКИХ УСЛОВИЯХ

Петр Витальевич Меньшиков

Московский государственный институт международных отношений (университет) МИД РФ,
г. Москва, Российская Федерация

Аида Ягутовна Нейматова

Московский государственный институт международных отношений (университет) МИД РФ,
г. Москва, Российская Федерация

Аннотация. *Введение*. В условиях интенсивного идеологического противостояния и нарастающей антироссийской информационной войны все более релевантным становится вопрос грамотного информационного сопровождения внешней политики России. *Методы*. В первую очередь авторами были использованы метод экспертной оценки и трендовый метод, которые доказывают, что Соединенные Штаты уже на протяжении долгих лет целенаправленно ведут информационные войны против России. Стоит отметить, что впервые термин «информационная война» был официально введен в директиве министра обороны США в 1992 году. С каждым годом методы, находящиеся в арсенале США, становятся все более изощренными и масштабными (ЕС и НАТО уже выступают в качестве союзников). Кроме того, авторами использовались методы компаративного анализа результатов исследований ведущих отечественных и зарубежных специалистов в области информационной и идеологической составляющей современных международных отношений и проблематики информационного сопровождения внешней политики РФ, а также общенаучные и специальные методы познания правовых явлений и процессов, вынесенных в качестве объекта исследования: метод системно-структурного анализа, сравнительно-правовой и формально-логический методы. *Анализ*. Наряду с инструментами публичной дипломатии наше государство принимает все необходимые меры для защиты своего информационного суверенитета на всех уровнях. Несмотря на то что в России последовательно создается система выявления, предотвращения и устранения угроз информационной безопасности, по-прежнему актуальным остается вопрос борьбы со всевозрастающим объемом недостоверной антироссийской информации в мировом медиапространстве. *Результаты*. Будучи одним из инструментов публичной дипломатии и внешней политики в целом любого суверенного государства, «мягкая сила» учитывает объективные условия международных отношений и мировой политики и исходит из требований национальных интересов государства как основного актора всей системы современных международных отношений. В мировой практике имплементации политики «мягкой силы», начиная с создания Вестфальской системы международных отношений, не было ни одного прецедента, когда государство вне зависимости от общественно-политического характера построения политической системы или целей внешнеполитической активности руководствовалось бы иными целями и методами анализа мировой политики, всей системы международных отношений и иным целеполаганием действий на международной арене, в том числе определяемых в последние десятилетия понятием «мягкая сила». В истории международных отношений нет мировой политики, свободной от ее идеологической составляющей. Тезис о деидеологизации международных отношений, получивший свое определенное распространение непосредственно после распада СССР, на практике внешнеполитических действий всех основных акторов современной мировой политики однозначно доказал свою полную несостоятельность. Сегодня, в условиях «гибридных войн» во всей системе международные отношений, мировая политика не менее идеологизирована, чем во времена

холодной войны. Политическое руководство России допускает гипотетическую возможность кибервойны, спровоцированной действиями республиканской администрации Соединенных Штатов. В декабре 2019 г. Белый дом санкционировал подготовку плана ведения информационной войны с РФ силами спецподразделений американской армии, возложив решение такой задачи на упоминавшееся выше киберкомандование. Политика «мягкой силы» России, как и ее публичная, народная дипломатия, есть комплекс внешнеполитической деятельности страны на международной арене является производным от принципиальной по своему значению функции отстаивания национальных интересов России в условиях новой политической реальности. Россия последовательно выступает против превращения международных отношений в арену идеологического противоборства с задействованием инструментария так называемых информационных войн. Государственный суверенитет един. Информационная безопасность как фактор обеспечения информационного суверенитета является базовой составляющей единого государственного суверенитета. Это общепризнанная истина, являющаяся фундаментальной для понимания характера современных международных отношений, принцип, лежащий в основе внешнеполитической деятельности любого современного суверенного государства, обусловленный именно объективной закономерностью возрастания идеологического фактора современных международных отношений. Более того, в условиях ведения «гибридных войн» России необходимо обеспечить свою информационную безопасность на обоих уровня: как на политическом (идеологическом), так и на техническом (технологическом), комплексно используя и «мягкую силу», и передовые цифровые технологии.

Ключевые слова: информационная политика, информационная безопасность, информационная инфраструктура, внешнеполитический PR, мягкая сила, публичная дипломатия, «гибридные войны», кибервойна.

Цитирование. Меньшиков П. В., Нейматова А. Я. Актуальные вопросы информационного сопровождения внешней политики России в новых политических условиях // Вестник Волгоградского государственного университета. Серия 4, История. Регионоведение. Международные отношения. – 2020. – Т. 25, № 3. – С. 161–171. – (На англ. яз.) – DOI: https://doi.org/10.15688/jvolsu4.2020.3.14

Introduction. The information space of the modern multi-polar world is characterized by an already open and ever growing ideological confrontation, numerous sanctions regimes against Russia, a desire to root the negative image of our country in the international public consciousness and attempts to discredit its domestic and foreign policy. Both the long-standing notorious stereotypes of the Cold War era and the new-fangled "accusations" of various machinations of official Moscow – from "Russian hackers" to the so-called "Pro-Kremlin" media are being used. According to them, Russia interferes, supposedly, in the internal affairs of the United States, England, France, Germany in order to provide the impact on the electorate of these countries "in the best interests of the Kremlin", trying, allegedly, to achieve some kind of destabilization of the internal political situation during the election campaigns or on their eve. In Western countries (UK, USA, France, Latvia, Lithuania and others) and countries to which the West is trying hard to extend its influence (Moldova, Ukraine and others), the Russian press faces various kinds of discrimination and restrictions: from censorship on the Internet and forcing around her an atmosphere of hostility, to physical pressure and threats of violence against our journalists, refusals of accreditation to official events, expulsions and bans on crossing state borders. The "collective West" is actively developing initiatives to legalize discriminatory measures against the media and to clean up its information space from undesirable points of view at the international level, which are supposedly designed to counteract disinformation and improve the quality of journalism. France continues to be the main inspirer on this track today. For example, the French authorities in close conjunction with the Paris-based NGO "Reporters Without Borders" promote international projects that discriminate against our media, in particular the "Media Confidence Initiative" (the so-called "white lists" of the media), which offers the division of the media into trustworthy information resources and sources of disinformation. Ironically, the Russian media from the point of view of official Paris are associated exclusively with the latter.

Methods. In 2018, Russia was in the penultimate place among countries that Americans considered to be allies or friendly states. According to this joint survey conducted by the Economist and YouGov, a research organization, a third of Americans consider Russia an enemy rather than a friend of the United States [7]. Does Russia make any attempts to improve its image abroad?

Russia's foreign information policy is defined in the concept of Russia's foreign policy, approved by President Vladimir Putin on November 30, 2016. It contains two separate sections – Information support of Russian foreign policy and International humanitarian cooperation and human rights. The task of bringing to the world community objective information about Russia's position on the main international issues, its foreign policy initiatives and actions, processes and plans of the social and economic development of the country, achievements of the Russian culture and science is formulated in them as two independent complementary directions of foreign policy activity. In this context, the participation of civil society institutions in solving international problems, the use of public diplomacy, international cultural and humanitarian cooperation as a means of establishing an inter-civilizational dialogue, reaching agreement and ensuring mutual understanding between nations are identified as one of the top-priority tools for achieving this goal.

In fact, all the above is entirely the subject of such a discipline as foreign policy PR, as one of the key components of soft power – a foreign policy strategy, involving the ability to achieve the desired results based on voluntary participation, and public diplomacy – a set of measures aimed at studying and informing foreign audiences in order to establish long-term relationships and promote national foreign policy in order to achieve a better understanding of national values and institutions abroad. The key element of soft power is the ability to set meanings [2]. Soft power is a more complex phenomenon and public diplomacy is its most important component. Public diplomacy is a key tool of soft power, a means of transmitting components of soft power to foreign countries, a tool of cross-border export of national values and interests. Public diplomacy and soft power in their unity of action pursue the goal of converting the influence of one state into the motivation of another through the implementation of national interests in the sphere of international relations. In this case non-violent methods of foreign policy are used exclusively peacefully to influence foreign public opinion in general and its individual specific target audiences in particular. Among other things, the most important result of such foreign policy activity is to create a favorable international image of the country.

At first glance it may seem that the conceptual foundations of such types of foreign policy activity as soft power and public diplomacy [8] developed by Joseph S. Nye Jr. are not relevant in the present time, characterized by a well-known aggravation of international relations, "hybrid wars" and multiple sanctions regimes against Russia. But, in fact, they are. Russia has the potential of soft power and public diplomacy for the large-scale promotion of its national interests in international relations precisely through these components of foreign policy activity. Besides, it is crucial to note that soft power can be based on conservative values [3].

In the analysis of the modern world and Russia's foreign policy (Section II of the foreign policy Concept of Russia) it is emphasized that the use of soft power tools, primarily civil society, information and communication, humanitarian and other methods and technologies, in addition to traditional diplomatic methods, is becoming an integral part of modern international policy (Paragraph 9) [10].

The institutional framework of the Russian soft power system policy is formed by state institutions (included in the structure of Rossotrudnichestvo of the Russian Ministry of Foreign Affairs), non-governmental organizations and civil society institutions ("Russkiy mir" foundation and the Alexander Gorchakov Public Diplomacy fund), the global media (MIA "Russia Today", project of Rossiyskaya Gazeta "Russia Beyond the Headlines"), the country's leading universities (MGIMO University, RUDN University), the Russian Orthodox Church and other religious institutions. Every year the work with foreign media representatives is being brought to a higher level. In confirmation of this, it should be mentioned that in 2018 Russian Foreign Ministry ensured the participation of foreign press and – for the first time – bloggers in covering the election of the President of the Russian Federation and the the FIFA World Cup 2018 [9].

In fact, all the above is as a special form of the ideological activity of foreign policy subjects aimed at effectively managing their public communication in international relations and increasing political competitiveness by attracting public support of the broad layers of world public

opinion and shaping a correct image of the state abroad. It is important to stress the ideological component of the information support of foreign policy, which undoubtedly implies a purposeful ideological impact on foreign public consciousness, but it is not identical to the function of propaganda with its inherent method of manipulating mass consciousness [4]. Russia has never acted as an initiator of information wars anywhere - neither in the sphere of international relations, nor in the context of bilateral or multilateral diplomacy and foreign policy activity in general.

Any attempts to adhere to the classical traditional formulations of the principles of foreign policy PR as a communicative process, devoid of an ideological component and not implying active advocacy and, in a certain sense, the promotion of a set of ideas that constitute the ideological basis of national interests and a specific system of values, are doomed to failure. The practice of foreign policy PR activity of all the leading actors of modern international relations, without exception, characterized by a very high intensity and sharpness of ideological rivalry, competition, sometimes open confrontation, clearly supports the above considerations, which in the context of "hybrid wars" has taken the form of a statement of fact.

It has been a long time since the development of the basic theoretical foundations of PR and the whole world around us, the whole system of international relations has changed dramatically, where the role of the force factor (the Concept of Russia's foreign policy of 2016) [10], the content and technological level of cross-border information flows has increased. Russia's understanding of its place in the modern world, the importance of its own national interests, the need for their consistent active defense and the offensive nature of progress in international relations has also changed.

Besides the conditionally defensive measures and among the relevant challenges of information support of Russian foreign policy is, of course, the problem of providing the intellectual leadership by means of foreign policy PR and participation in the formation of the international agenda. A good example of this type of activity are, in particular, Vladimir Putin's annual speeches during the "Valdai" International Discussion Club, designed primarily for the elite of world public opinion, which, as an effective channel of subsequent communication, is a very authoritative source of wide dissemination of the principled positions of our state on the most pressing international issues. Vladimir Putin also periodically publishes articles in the world's leading media and gives numerous interviews, which is one of the important communication channels of direct appeal to mass foreign audiences. Another form of communication with the foreign public, equally significant in its informational effect, is the press conference of the President of Russia with the participation of representatives of foreign media. Together, these types of communication with the participation of the head of the Russian state form the highest level of information support of the country's foreign policy, setting the tone and largely forming the representation of the world public opinion on the most pressing and fundamental issues of international relations. All the above mentioned initiatives are being implemented in order to gain trust which is "the high prize in the Public Diplomacy game" [6].

Nowadays in the context of new political conditions, in particular the already mentioned "hybrid wars", one of the relevant challenges for Russia is to effectively secure its information infrastructure. For this purpose, over the past decades Russian state strategy has consistently created a system for detecting, preventing and eliminating threats to its information security, including the consequences of computer attacks on the country's information resources, cybercrime, various information and ideological attacks, which sabotage to undermine the information sovereignty and national security of the Russian Federation as a whole. The information security, as a priority component of the information sovereignty of the state, includes two main components – technical and technological, political and ideological (informational), in other words, they have a technical and a political dimensions. The information sphere was transformed into a zone of military activity along with the traditional theaters of military operations on land, at sea and in aerospace – in fact, what British The Economist wrote about – cyber war actually became the fifth area of the war. Today critical infrastructure is the object of increasingly sophisticated cyber attacks, virtual space – information and psychological sabotage.

Russian President Vladimir Putin has repeatedly drawn attention to the already mentioned trend – the changing nature of military conflicts, the ways of their unleashing and conducting, the ongoing militarization of cyberspace, the widespread use of special operations mechanisms and soft power tools. Moreover, Vladimir Putin stressed that Russia should effectively respond to cyber threats and increase the level of protection of information systems of strategic objects, be ready to effectively fend off threats in the information space by increasing the level of protection of the relevant infrastructure, first of all, information systems of strategic and critically important facilities. The so-called "information attacks" are already being used to solve military-political problems and their "striking force" may be higher than that of conventional weapons.

Russia's new Military doctrine sets out the main tasks to curb and prevent military conflicts, including the creation of conditions that reduce the risk of using information and communication technologies for military and political purposes to carry out actions that are contrary to international law, directed against the sovereignty, political independence, territorial integrity of countries and pose a threat to international peace, security, global and regional stability. The doctrine also notes the importance of developing the forces and means of information warfare; the qualitative improvement of information exchange tools based on the use of modern technologies and international standards, as well as the creation of a single information space of the Armed Forces, other troops and agencies as part of the Russian information space.

Along this path, the Ministry of Defense has taken a number of important steps to implement the provisions of the Military Doctrine of 2010 concerning the tasks of ensuring information security of the Russian Armed Forces. On January 14, 2014, the Minister of Defense of the Russian Federation, Army General S.K. Shoigu signed an order to establish a cyber command within the General Staff of the Russian Armed Forces, whose main task is to protect against unauthorized interference in Russia's electronic control systems.

Speaking on February 22, 2017 at the "government hour" in the State Duma, Minister of Defense, Army General S.K. Shoigu reported on the creation of the troops of information operations in the Russian Armed Forces – a special formation of the Russian Army, whose main tasks are the management and protection of military computer networks, Russian military control systems and communications from cyber attacks and reliable protection of information passing through them. The troops of information operations are called upon to coordinate and integrate operations conducted by cyber subdivisions, to examine the cyber potential of the Russian Ministry of Defense and to expand the possibilities of its actions in cyberspace. Their main purpose is to protect the Russian military control and communication systems from cyber-terrorism and ensure that information passing through them is blocked from a possible enemy.

Analysis. According to available estimates, in terms of the level of the cyber warfare development, Russia can be in the top 5 countries of the world along with the United States, China, the United Kingdom and South Korea. Several dozens of states, unofficially over a hundred have special units for cyber security. Officially several dozen countries, unofficially more than a hundred have specialized cyber security divisions. The USA has the strongest army in cyberspace, where, according to published data, government funding in this area may be about $7 billion a year, and the number of hackers working for the Pentagon is up to 9 thousand people, in China – 1.5 billion dollars and about 20 thousand people, Great Britain – 450 million dollars a year for the maintenance of 2 thousand specialists, South Korea – 400 million dollars, 700 people. The assessment of the potential of such special troops is based on the military budgets of these coutries, cybersecurity strategies, statutory documents, reference information of international organizations, official comments and insider information. The main activities of the U.S. and NATO cyber forces are espionage, cyber attacks and information wars, including various means of influencing the mood and behavior of people in different countries of the world.

For the first time cyber troops appeared in the American Army. The term "information war" has been used for more than a quarter of a century after it was introduced into circulation in the Directive of the United States Secretary of Defense DODD 3600 dated December 21, 1992. The directive of the Chiefs of Staff Committee

no. 30 of 1993 laid down the basic principles waging information warfare. At the end of 1998, the Chiefs of Staff Committee of the United States Armed Forces issued the document "Doctrine for conducting information operations" (Joint Doctrine of Information Operations), which for the first time officially confirmed the fact of preparation of armed forces of the United States to conduct offensive information operations not only in war but also in peace, although previously there has always been a defensive focus of action in the information sphere. Information and psychological weapons are a type of non-lethal weapons of mass destruction capable of providing a decisive strategic advantage over a potential enemy with a distinctive ability not to fall under the concept of "aggression" adopted in international norms.

"Dominance across the spectrum" acquired the status of a key concept of the U.S. military construction in the early twenty-first century [1]. On the basis of the 688th wing of the U.S. electronic intelligence formed in 2006 an experimental operational command to repel cyber threats. Since October 2008, the Pentagon, in the framework of the Joint Doctrine of Information Operations considers information and psychological support of hostilities as one of the most important components that ensure the success of military operations in modern conditions. On May 5, 2009 the head of the U.S. National Security Agency (NSA), Lieutenant General Keith Alexander announced the beginning of the formation of the cyber army as a special unit of the U.S. Strategic Command, which was created on June 23, 2009. According to the order of the then U.S. Secretary of Defense R. Gates, such a special unit of the U.S. Army was entrusted with the responsibility for the security of military information networks, protecting the country from attacks through computer networks, as well as, as shown later by the well-known revelations of E. Snowden, the creation of a global electronic intelligence mechanism.

The U.S. Cyber Command (USCYBERCOM) was established on May 21, 2010 and achieved full operational capability on October 31, 2010. It is a formation of the U.S. armed forces, which is subordinate to the United States strategic command to coordinate the cyber commands of the army, navy, air force, coast guard and marine corps. The U.S. Cyber Command is organizationally combined with the National Security Agency. The commander of the Cyber Command is at the same time the head of the NSA. The Cyber Command united under its command several previously existing organizations, such as Global Network Operations (JTF-GNO), Network Warfare Joint Command (JFCC-NW), Military Information Systems Agency, a division of JTF-GNO, and is stationed at the military base of Fort Mead, Maryland. The main tasks of the command are centralized operations of cyber war, the management and protection of U.S. military computer networks.

Eight large brigades were introduced into the U.S. cyber armies. The United States was the first in 2010 to carry out a real military operation with the help of these troops, when Iranian nuclear facilities, in particular the Bushehr nuclear power plant, were attacked by a hacker using the Staxnet computer virus developed by the Pentagon in cooperation with Israel.

In 2011, the U.S. Department of Defense adopted the Strategy for Operating in Cyberspace, which assesses the challenges and opportunities arising from the growing importance of information technology for military, intelligence operations and business. In the documents of the Chiefs of Staff Committee of the U.S. Department of Defense "Unified Outlook 2010" and "Unified Outlook 2020" the goal of conquering the informational superiority over the enemy by conducting information operations is stated. Moreover, a special Cyber Warfare Intelligence Center was created. It declared the formation of the 41st special brigade as a part of the cyberarmies of the United States. Staff and field exercises were conducted to test cyberattacks on power grids, oil pipelines, information networks of banks and government agencies.

It is important to note that the White House declares its readiness to announce its intention to use offensive and defensive cyber capabilities in the interests of NATO when the need arises. The US openly announces its readiness to offer the Pentagon's cyber capabilities to the North Atlantic Alliance, stressing that such a statement is addressed primarily to Russia. The Pentagon's new cyber security strategy says that Russia, China, Iran and North Korea pose a threat to Washington, as they use cyber weapons to harm the Americans and their

interests. The military Department proposes to "stop malicious activity in its source." The Pentagon believes that for this aim, it is necessary to create "more deadly forces" to conduct combat operations and counter cyber threats.

NATO, the US, leading EU countries are actively expanding their efforts to create a large-scale system of information warfare in the international arena, which makes the task of removing ideology from international relations all the more distant and illusory perspective. Technologies of cross-border dissemination of information dramatically increase the danger of cyber attacks, including those aimed at critical public infrastructure, including strategic military control systems. Declared by the West some pseudo-threats from the information impact of the Russian global media on the Western audience significantly prevail over the real danger of real ideological influence from international terrorist groups.

Within NATO, information and psychological operations, as part of the Alliance's overall information and political-ideological activities, are coordinated by the Atlantic Council. The fundamental document in this context is the single Directive "On the principles of planning and conducting psychological operations", which states that psychological operations are a vital part of NATO's diplomatic, military, economic and information activities and represent planned psychological activities in peacetime, crisis or wartime towards an enemy, friendly or neutral audience in order to influence its attitude and behavior in order to achieve its own political and military goals.

A special Public Diplomacy Division has been operating in the structure of the NATO Secretary General since 2002. NATO's official policy in cyberspace was defined in the NATO Cyber Defence Policy doctrine at the summit in Bucharest in April 2008. In 2010, at the Lisbon summit, this doctrine has been significantly upgraded and fleshed out, and entered into force in June 2011. In the new edition of the document the so-called information threat is located immediately after the one of the spread of weapons of mass destruction and global terrorism.

There is the Cyber Defence Centre of Excellence and the Computer Incident Response Capability, as well as the Cyber Security Authority, the Cyber Defense Management Board, composed of the heads of NATO's political, military, operational and technical bodies, which, in turn, is part of the Emerging Security Challenges Division of the North Atlantic Alliance Headquarters.

The work of the NATO Strategic Communications Centre of Excellence or STRATCOM, established in Riga in summer 2015, has been significantly activated. There are twenty centres like this. Three of them are located in the Baltic States. The centre in Estonia deals with cybersecurity, in Lithuania – with energy security, in Latvia – with strategic communication of the Alliance. The mission of the centre is to conduct research and develop recommendations for conducting information and psychological operations, public relations, propaganda.

The Cyber Defense Centre of Excellence, accredited since 2008 under NATO, operates in Tallinn. It trains specialists and conducts research in the field of information and psychological operations in the virtual space in cooperation with the Committee for Planning the Use of Civilian Communication Systems, deployed in Ankara. Moreover, there are agreements between NATO and the EU on seventy-four areas of cooperation, including cyber security and military cooperation.

The European Centre of Excellence for Countering Hybrid Threats has been opened in Helsinki. Twelve Western European countries participate in its work. The centre is a platform for ideological cooperation between the EU and NATO. The declared goal of the center is to collect and disseminate information about hybrid threats, including those related to information influence at the international level of Russia.

NATO as a whole has established a unified organizational system at both the organizational, tactical and strategic levels on the basis of NATO's long-term doctrines, which include, in particular, the use of the potential of cyberattacks as a means of digital propaganda, DDoS-attack campaigns, website defaces, information leakage due to hacker cyberattacks, the use of malicious software for intelligence and subversive purposes. As adopted by the Pentagon in 2015, the new law of war manual actually states the fact that the U.S. government has come to believe that in order to control and manipulate information as a weapon of soft power it is necessary to combine psychological operations, propaganda and work with the public under the phrase "strategic communications". In other words, it is a common

practice of information policy of the United States and NATO to use psychological operations and manipulative methods of influence in the processes of forming public opinion and public consciousness to form the views of the target groups.

In September 2017, the U.S. Secretary of State approved the spending of $60 million allocated in 2016 by the Congress to combat propaganda of ISIS (a terrorist group banned in Russia) and to counter the influence of information of such states as Russia. At the same time, it is planned to spend three times less money on the information counteraction to terrorism than on the fight against the so-called Russian propaganda – $20 and $40 million, respectively [5].

The United States allocated $160 million from its budget for the activities of the Global Engagement Center (GEC), including the information war with Russia. Its main goal is to conduct and coordinate the efforts of the U.S. government both to reduce the influence of foreign terrorist organizations and to counter state propaganda and misinformation that undermine the interests of the national security of the United States. The fight against "foreign propaganda" is expected through, in particular, the allocation of grants to journalists, non-profit organizations and private campaigns in the host countries of information expansion in the United States.

In 2015, a working group on strategic communications East StratCom Task Force was established in the EU to "counter Russian disinformation campaigns". The group oversees the implementation of the EU project against disinformation, which has launched a special website in Russian, English and German with a similar name. Its purpose – "fight against false information" and "denial of the Russian promotion". The site was launched in the context of the EU activities on the implementation adopted in November 2016. The EU Parliament adopted the resolution "Strategic communications of the EU as a counteraction to propaganda of third countries", within the framework of which it was also supposed to introduce censorship against a number of Russian media.

Results. The accusations of Russia's informational interference in the internal political affairs of Western countries – from D. Trump's election campaign to the protests of "yellow vests" in France are being purposefully escalated. It deliberately creates a false idea in its essence that there is no mechanism in the United States to oppose Russian propaganda and that the West does not take systematic actions to response to the misinformation spread by Russia, China and the ISIS (banned in Russia), allegedly directed against the development of democracy, strengthening alliances and protecting U.S. international reputation.

Facebook officially acknowledged the leakage of personal data of 84 million users from all over the world during the American investigation of trumped-up accusations against some Russian hackers who allegedly tried to influence the course of the presidential campaign in the United States. In fact, the British company Cambridge Analytica, founded in 2013 as a branch of the English Strategic Communication Laboratories (SCL Group) for participation in political campaigns in the United States, stole Facebook's data. The company's relationship with the government of England and its involvement in more than 200 election campaigns around the world, including the United States, Argentina, India, Kenya, Nigeria and the Czech Republic, became public.

Since 2013, Cambridge Analytica has participated in forty-four political campaigns in the United States. Personal information stolen from Facebook was used to create algorithms for targeted political advertising, in particular to support D. Trump's election campaign in 2016. The company had access to secret data of the British Ministry of Defense and co-developed several projects with it, in particular, codenamed Duco (2014), to study people's reaction to information disseminated by the government on various socially significant problems. The company received 548 thousand pounds for the development related to the analysis of methods of influence on the change of political attitudes and social and socio-behavioral patterns of various target audiences, including a two-month training course for NATO personnel.

The fact that Cambridge Analytica stole data from Facebook became an unprecedented episode for the global information space which demanded an explanation. First of all – to achieve what political and ideological goal this cybercrime was committed using big data technologies, and from what positions the ruling circles of Western countries interpreted it. Cambridge Analytica made only one statement that the company really used social platforms for carrying out some

external marketing, providing the created content again to a certain target audience. An investigation conducted by a journalist of the British Channel 4, who, posing in 2017–2018 as a person interested in influencing the elections in Sri Lanka, showed that the system of Cambridge Analytica included the collection of compromising evidence, provocative bribery and other methods of discrediting political opponents, by posting compromising data on various sites and social networking platforms.

The U.S., UK and EU authorities have urged Facebook to give explanations about the theft of personal data of nearly one hundred million users, adding speculation about the so-called "possible Russian trace". Paradoxically, no one in the West specifically asked for the cybercriminals themselves, nor did they really require any clear answer about the obvious cybercrime in the global information space for the purpose of openly interfering in the electoral processes of the countries of "advanced democracy".

Building the foreign policy information and propaganda potential of the USA, NATO, the EU goes in several directions at once. The existing structures are being reformed and new ones are being created, and significant allocations are being made for their technical equipment. Advanced technologies of modern strategic communications are used. The priority of shifting the activity mainly towards strengthening the communication presence in the global Internet is obvious.

Russia has never acted as an initiator of information wars and nowadays combats attempts to undermine information security (including its both dimensions – political (ideological) and technical (technological)) and foremost counteract disinformation at all levels. Soft power, as one of the instruments of public diplomacy and foreign policy of any sovereign state, takes into account the objective conditions of international relations and world politics and proceeds from the requirements of the national interests of the state, as the main actor of the entire system of modern international relations. In the world practice of implementing the policy of soft power, starting with the creation of the Westphalian system of international relations, there was no precedent, when the state regardless of the socio-political nature of building a political system or the purposes of the foreign activity would be guided by different objectives and methods of analysis of world politics, the entire system of international relations and other goal-setting action in the international arena, including defined in the last decade by the concept of soft power. In the history of international relations, there has not been any world policy free from its ideological component. The thesis of de-ideologization of international relations, which received its definite distribution in the period immediately after the collapse of the Soviet Union, in the practice of foreign policy actions of all the main actors of modern world politics has clearly proved its complete failure. Today, in the context of "hybrid wars" within the entire system of international relations, the world politics is no less ideologized than during the "cold war". The political leadership of Russia allows the hypothetical possibility of cyberwarfare, provoked by the actions of the Republican administration of the United States. In December 2019, the White House authorized the preparation of a plan for conducting an information war with the Russian Federation by special forces of the U.S. Army, assigning the solution of this task to the above-mentioned cyber command. The policy of soft power of Russia, as well as its public diplomacy, as the whole complex of foreign policy activities of the Russian Federation in the international arena, is derived from the fundamental function of defending the national interests of Russia in the new political reality. The Russian Federation has consistently opposed the transformation of international relations into an arena of ideological confrontation with the use of tools of the so-called "information wars". State sovereignty is unified. Information security, as a factor of ensuring information sovereignty, is a basic component of the unified state sovereignty. This is an accepted truth underlying the understanding of the nature of modern international relations, the principle underlying the foreign policy activity of any modern sovereign state, due to the objective regularity of the growth of the ideological factor of modern international relations.

At the forefront of this "information war" are the President of the Russian Federation, the Russian Ministry of Foreign Affairs including all its structures in Russia and abroad first of all adhering to the soft power system policy as well as the Ministry of Defense fighting in cyber warfare effectively responding to cyber threats and increasing the level of protecting information

systems of strategic objects. Strengthening the anti-Russian discourse abroad is a reaction from the ruling civil and military elites of Western countries to the objectively advanced historical stage of the Russian national revival. It is possible that Russia's consistent defense of its national interests, including the use of the potential of the Armed Forces to actively counter cybercrime and ideological sabotage, will lead to an even tougher confrontation and even greater strengthening of the anti-Russian content of global information flows.

REFERENCES

1. Alekseev A.P., Alekseeva I.Yu. Informatsionnaya voyna v informatsionnom obshchestve [Information War in the Information Society]. *Voprosy filosofii* [Russian Studies in Philosophy], 2016, no. 11, pp. 5-14.

2. Andreev A. "Myagkaya sila": aranzhirovka smyslov v rossiyskom ispolnenii ["Soft Power": Arrangement of Meanings in the Russian Version]. *Polis. Politicheskie issledovaniya* [Polis. Political Studies], 2016, no. 5, pp. 122-133.

3. Keating V.C., Kaczmarska K.J. Conservative Soft Power: Liberal Soft Power Bias and the 'Hidden' Attraction of Russia. *Journal of Intrenational Relations and Development*, 2019, vol. 22, pp. 1-27.

4. Menshikov P.V. Aktualnye aspekty informatsionnogo obespecheniya rossiyskoy vneshney politiki [Current Aspects of Information Support of Russian Foreign Policy]. Martynenko E.V., ed. *Mediaprostranstvo mnogopolyarnogo mira: sb. nauch. st. (Moskva, RUDN, 13 apr. 2017 g.)* [Media Space of the Multipolar World. Collection of Scientific Articles (Moscow, RUDN, April 13, 2017)]. Moscow, PFUR, 2017, pp. 346-358.

5. Menshikov P.V. PR v kontekste rossiyskoy vneshney politiki [PR in the Context of the Russian Foreign Policy]. *Mezhdunarodnye kommunikatsii* [The Moscow Journal of International Communications], 2016, December, no. 1. URL: http://www.intcom-mgimo.ru/2016-01/polit-pr.

6. Mogonsen K. "International Trust and Public Diplomacy." *The International Communication Gazette*, 2015, vol. 77, no. 4, pp. 315-336.

7. *Nazvano otnoshenie amerikantsev k Rossii* [The Attitude of Americans to Russia Was Named]. URL: https://lenta.ru/news/2018/10/17/usa_russia.

8. Nye J.S. Soft Power. *Foreign Policy*. 1990, Autumn, no. 80, Twentieth Anniversary, pp. 153-171.

9. Obzor vneshnepoliticheskoy deyatelnosti v 2018 godu [Review of Foreign Policy Activities of the Russian Federation in 2018]. *Sayt Ministerstva inostrannykh del Rossiyskoy Federatsii* [Website of the Russian Foreign Ministry]. URL: http://www.mid.ru/ru/activity/review.

10. *Ukaz Prezidenta Rossiyskoy Federatsii ot 30.11.2016 № 640 "Ob utverzhdenii Kontseptsii vneshney politiki Rossiyskoy Federatsii"* [Decree of the President of the Russian Federation of November 30, 2016 no. 640 "On Approving the Foreign Policy Concept of the Russian Federation]. URL: http://www.kremlin.ru/acts/bank/4145.

Information About the Authors

Petr V. Menshikov, Candidate of Sciences (History), Head of the Department of Advertising and Public Relations, MGIMO University, Prosp. Vernadskogo, 76, 119454 Moscow, Russian Federation, menshikov-petr@rambler.ru, https://orcid.org/0000-0001-6547-6032

Aida Ya. Neymatova, Candidate of Sciences (History), Lecturer, Department of Advertising and Public Relations, MGIMO University, Prosp. Vernadskogo, 76, 119454 Moscow, Russian Federation, aida.neimatova@gmail.com, https://orcid.org/0000-0003-4765-3554

Информация об авторах

Петр Витальевич Меньшиков, кандидат исторических наук, заведующий кафедрой рекламы и связей с общественностью, Московский государственный институт международных отношений (университет) МИД РФ, просп. Вернадского, 76, 119454 г. Москва, Российская Федерация, menshikov-petr@rambler.ru, https://orcid.org/0000-0001-6547-6032

Аида Ягутовна Нейматова, кандидат исторических наук, преподаватель кафедры рекламы и связей с общественностью, Московский государственный институт международных отношений (университет) МИД РФ, просп. Вернадского, 76, 119454 г. Москва, Российская Федерация, aida.neimatova@gmail.com, https://orcid.org/0000-0003-4765-3554