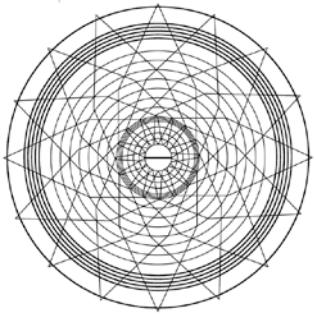


STRATEGIC COMMUNICATIONS AND WORLD POLITICS

Panarin I.
Doctor of Sciences in Politics, Head of the"Information Special Force" Association
(Moscow, Russia)
infowar@mail.ru

Abstract:

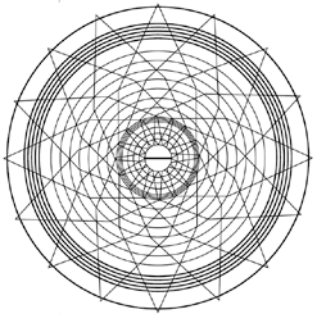
Today all indications point to the drastic escalation of the geopolitical and geo-economic situation in the world. It resulted in an increased risk of the instability spreading to Russia, primarily through hybrid warfare techniques such as misinformation, terrorism, etc. The following article describes and analyzes various tools of information and hybrid wars. The Author gives several recommendations on the further communication strategy of Russia in the hybrid war.

Keywords: social media, hybrid war, information war, Russia, Ukraine, United Kingdom, Vladimir Putin, propaganda tools

1. The specific nature of the current world situation

Today all indications point to the drastic escalation of the geopolitical and geo-economic situation in the world. It resulted in an increased risk of the instability spreading to Russia, primarily through hybrid warfare techniques such as misinformation, terrorism, etc. There is a danger that Russia will be embroiled in a new Great War with regard to the situation in Syria, Afghanistan and Ukraine. At the same time President of Russia Vladimir Putin's address to The Federal Assembly, in the course of which he spoke about Russia's latest military technology (hypersonic air-launched missile and etc.), is a powerful constraint to the Evil Powers of the World, aiming at starting The Third World War. We will give a few key quotations from V. Putin's address:

1. We are greatly concerned by certain provisions of the revised nuclear posture review, which expand the opportunities for reducing and reduce the threshold for the use of nuclear arms. Behind closed doors, one may say anything to calm down anyone, but we read what is written. And what is written is that this strategy can be put into action in response to conventional arms attacks and even to a cyber-threat. I should note that our military doctrine says Russia reserves the right to use nuclear weapons solely in response to a nuclear attack, or an attack with other weapons



of mass destruction against the country or its allies, or an act of aggression against us with the use of conventional weapons that threaten the very existence of the state. This all is very clear and specific. As such, I see it is my duty to announce the following. **Any use of nuclear weapons against Russia or its allies, weapons of short, medium or any range at all, will be considered as a nuclear attack on this country. Retaliation will be immediate, with all the attendant consequences. There should be no doubt about this whatsoever.**

2. «There is no need to create more threats to the world. Instead, let us sit down at the negotiating table and devise together a new and relevant system of international security and sustainable development for human civilisation. We have been saying this all along. All these proposals are still valid. Russia is ready for this».

3. «Our policies will never be based on claims to exceptionalism. We protect our interests and respect the interests of other countries. We observe international law and believe in the inviolable central role of the UN».

The current climate in the world can be comparable to the worst international relations crises after 1945. The large-scale expulsion of Russian diplomats in March 2018 is an indicator of the formation of the global anti-Russian coalition organized by the Great Britain, the main historical enemy of Russia. **At the same time, the deterioration of the crisis can not only quickly but suddenly exceed the critical threshold.**

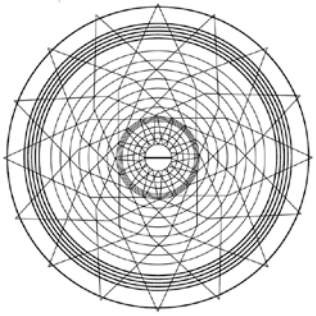
The change in the general nature of the geopolitical confrontation in the 21st century is so evident that it does not require proof. The key component of a strategy of containment endorsed at the NATO summit in Warsaw (at 2016) is a hybrid warfare that is being systematically waged against Russia with the purpose of weakening and breaking it up.

Hybrid warfare is a range of techniques with the objective of exerting military and security, political and diplomatic, financial and economic, informational, psychological and technological pressure as well as such methods as color revolutions, terrorism and extremism, activities of intelligence services, the formation of special task forces, special operations forces and structures of public diplomacy, carried out according to a single plan by the governmental bodies, a military-political bloc and scientific and technological sphere (technological-scientific complex).

It is important to understand that information war is at the core of the hybrid warfare.

The objectives of the hybrid warfare are an entire or partial disintegration of the state, a qualitative shift in its internal or external political course, a replacement of its leadership with loyal regimes, creating chaos, establishing an external ideological, financial and economical control over the country and its subjugation to the dictates of other states or technological-scientific complexes.

Therefore, **it is important to take into account the trend of the lines being blurred between the state of war and peace.** Non-military information and ideological methods of influence tapping into the protest potential of the population



are increasingly employed. This was vividly demonstrated by public protests in the aftermath of Kuzbass shopping centre fire. These means are complemented by the covert military steps, including informational confrontation and action taken by the special operations forces.

Apart from the response to the growing acts of hybrid warfare being waged against Russia, it is important for Russian authorities and largest corporations to intensify their efforts in the area of information. It is not very promising to be confined to the defensive position. It is necessary not only to take pre-emptive measures and countermeasures, but actively undertake well thought-out systematic steps that are offensive in nature.

As the development of the strategic offensive information operation carried out by the secret intelligence service MI6 has shown (the alleged poisoning of the traitor Skripal), the existing mechanism to counter the information operations of Great Britain and the West as a whole on the part of Russian government structures is piecemeal and not very effective. There is no coordination and comprehensive informational-analytical support. Not enough efforts have been devoted to social networks, as was demonstrated by the tragedy in Kemerovo, whereas the countries of NATO are increasing their presence in them. Tragic events in Kemerovo drew attention to our shortcomings in the system of operational response to the comprehensive anti-Russian information operations in social networks. In the immediate aftermath of the emergency in Kuzbass Western intelligence services carried out active hybrid warfare operations (speculation, misinformation, etc.). The 77th Brigade of a British Army (two thousand servicemen), established specifically to work in Russian social networks, was most active in that regard.

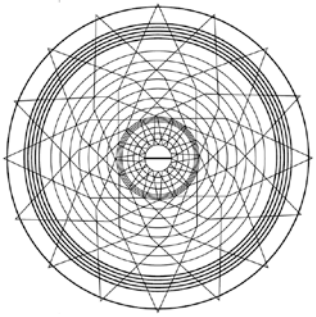
2. The development of the theory of the information war

After the victories of the Red Army in the battles of Stalingrad and Kursk the leader of the British Empire W. Churchill had devised a plan in Quebec (August 1943) to wage information war against the USSR. This plan was later completed and clarified by A. Dulles, a director of CIA and the Council on Foreign Relations.

The coming to power of M. Gorbachev was a determining factor in ensuring the realization of Churchill and Dulles's covert plans to break up the USSR by informational and ideological means.

The breakup of the Soviet Union was the main result of the First World Information war. The phrase «information war» itself was first used by A. Dulles in his book in 1967. After coming to power, M. Gorbachev deliberately destroyed the Soviet Union. But the information war against Russia did not stop after the unraveling of the USSR. In 2011 a series of color revolutions orchestrated by Western intelligence services in the Middle East marked the beginning of the Second World Information war, the main purpose of which is to break up Russia.

The years following the third inauguration of V. Putin are characterized by the robust restoring of Russia's status and position as a great power and the gradual



blocking of the Western channels of financial support for the liberal opposition. All of this took place against the backdrop of the rapid deterioration in the situation in the Middle East and Eastern Europe as well as the intensifying Western efforts to initiate a direct military aggression against Syria, with the further escalation of chaos spreading to the Caucasus and Central Asia.

The main outcome of 2017 is a global geopolitical Victory of Russia in the Middle East as a result of ISIS's defeat.

1. On the Syrian territory Russia succeeded in defeating ISIS, created by the Western intelligence services (MI6, CIA, Mossad) in order to cause Chaos in Eurasia and destabilize Russia.
2. Russia managed to create a powerful geopolitical triangle (Russia, Turkey, Iran) in order to stabilize the situation in Syria, and therefore in the Middle East as a whole, without the involvement of the main countries that ignited the so-called Arab Spring – USA, Great Britain, Israel and France. This is a good new model for resolving the international crises.
3. A brilliant one-day working visit made by V. Putin to Syria, Egypt and Turkey underpinned Russia's geopolitical victory.
4. A triumphant press conference held by V. Putin on December 14, 2017 underpinned Russia's geopolitical victory in the information space (the anecdote about a dagger, a story of how Russian pilots escorted President's plane as it prepared to land at our airbase in Syria, etc.).
5. The telephone call received by Putin from Trump after the conference reflected the established geopolitical order.
6. On April 4, 2018 Presidents of Russia, Iran and Turkey signed a joint statement on Syria.

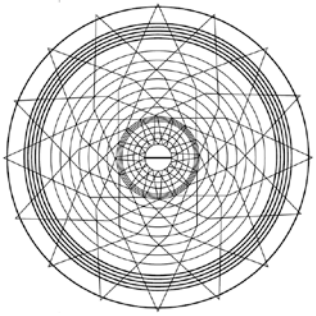
Along with the positive developments there are still several causes for concern that pose a risk to the national security of Russian state, particularly in the sphere of information and ideology.

In 1997 I defended a doctoral thesis, in which I outlined the methodology of conducting information confrontation (this term was first used by Russian President V. Putin in his address in Krasnodar on September 12, 2012).

In my thesis I emphasized that the information confrontation in a broad sense (in all spheres) should be distinguished from the information confrontation in a narrow sense (in a particular sphere, for example, political).

Information confrontation – is a confrontation between sides which manifests itself in the use of special (political, economic, diplomatic, military and other) methods, ways and means to influence the information environment of the opposing party and to defend one's own in pursuit of the desired objectives.

At the same time the beginning of 21st century was marked by a sharp increase in the volume and number of communication flows. The following statistics may serve as an example of this. For example, over the period from 1994 to 2018 the number of



internet users in Russia has risen by more than 600 times and has reached 103 million people. Therefore, the opportunities to influence Russian population through communication, including in a negative way, have dramatically changed.

At present the world's leading countries (particularly the USA and Great Britain) have a powerful communication potential which could help them to fulfil their hidden agenda, especially in view of the fact that there are no international legal norms of conducting information confrontation.

The situation in the world is influenced by various powerful communication flows. Some figures are given below as an illustration of the global nature of communication flows, particularly in social media:

- Facebook, more than 2 billion users
- Vkontakte, more than 460 million users

On the whole we underestimate what can be achieved in social networks. Most notably, in Russia there is a lack of a state-owned internet holding, about which I've been talking for several years now, that could operate both on the external and the domestic levels.

It should be noted here that Americans adopted the doctrine of information operations, in which the term offensive information operations was first introduced, as far back as 1998. There were no social networks back then, but the key principle, the main methodological conclusion outlined in this official public document was that these operations could take place in times of peace.

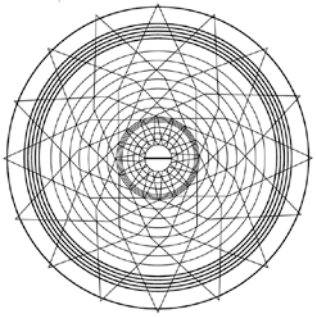
And in 2006 Americans issued a new document clarifying the previous one and declaring social media and internet the principal field for information operations. It means that these operations are based on the postulates of 2006, according to which social networks are the principal domain of information warfare, and create new «information bumping fists».

A media law in Russia has recently been amended with regard to the foreign ownership of Russian media outlets and the level of foreign ownership was reduced from 50 % to 20 %. American information law has been in place since 1948 and it limits foreign capital in American media outlets to 25 %.

There is no compulsory re-registration process for mass media in our country as well. Only the newly created media outlets will fall under the new rules on ownership, despite the fact there are media outlets in Russia with 100 percent foreign equity. Three federal TV channels in Russia have 100 per cent foreign equity.

There's also a problem with owners of media outlets, social media, social services, providers – these too have problems relating to foreign ownership. Let me remind that it was impossible to determine who owns the largest airport in Russia for two years, and I believe that the information environment is no less problematic in that regard.

We are lagging behind when it comes to regulation. The external information onslaught will be growing in intensity, and we need to strengthen ways to counter it. That is why Russia needs a specially appointed official responsible for the activities in this area. And we do not have such person yet. In the USA such a mechanism is integrated into the intelligence services. The director of U.S. Cyber Command is



simultaneously the head of the Department of Homeland Security. It means that in normal times he is the senior figure in the Department of Homeland Security whilst also serving as a senior figure for all 18 intelligence services of the country during information warfare operations. There have been several attempts in the same direction in our country but they failed to produce a coordination structure.

In 2009 Obama administration embraced the doctrine developed by a former high-ranking official of the State Department and U.S. Department of Defense and a Harvard professor Joseph Nye. A prestigious Princeton University graduate and a long-time lecturer at Harvard, he is justly considered to be the chief ideologist of the United States.

In January 2006 Joseph Nye outlined his ideas in Foreign Policy magazine. And after that, in the same year, the Center for Strategic and International Studies had set up a bipartisan Commission for the development of a new strategy co-chaired by former Deputy Secretary of State Richard Armitage and Joe Nye.

18 prominent Americans became members of this commission. In November 2007 this bipartisan commission submitted a strategy to the Congress offering for the first time the concept of using «smart power» as a combination of «hard» military and economic power and a «soft» power of public diplomacy. The resulting consensus of experts and analytical circles established a basis for developing the new doctrine of the Obama administration.

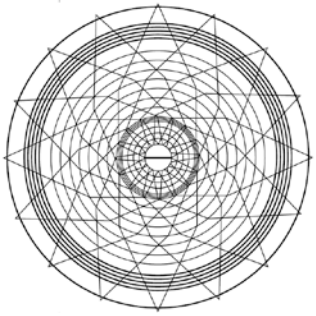
As far back as 2010 the doctrine of SC, a new concept of conducting the global offensive information war was developed. Strategic communications are a new doctrine of conducting the information war, adopted as an extension of the doctrine of offensive information operations (1998) that had been actively developed by the State Department, the U.S. Department of Defense and other governmental and non-governmental institutions and organizations of the country. This concept refers to a range of communication measures aimed at deliberate communication targeting of the core audiences in other countries (hostile as well as allied and neutral).

This includes such means as coordinated information campaigns, social media, indoctrination and brainwashing of the population, various informational and propagandistic policies and schemes. In the United States the main structures that carry out the strategic communications doctrine include the State Department, the U.S. Department of Defense, the United States Central Command, U.S. Cyber Command, Special Operations Command, United States Agency for International Development, non-governmental organizations.

Middle East was the first testing ground for carrying out the strategic communications doctrine. In March 2013 the doctrine of US strategic communications was further developed in practice with the setting up of the Strategic Communications Center in Latvia, literally serving as a command centre responsible for conducting information warfare operations against Russia, in the closest possible proximity to Russia's borders.

The coup d'état in Ukraine in 2014 became the trademark of the success of this new doctrine, particularly in the question of global manipulation of tens of millions of

© Communications. Media. Design, Vol. 3, №3, 2018



people through the use of the latest information and technological means. 16 officers of the NATO Cyber Centre who arrived from Estonia to Kiev on March 9 2014 vigorously carried out a variety of anti-Russian activities in the information space, particularly in social media.

It should be noted that at the end of November 2013, precisely on the eve of the coup d'état in Kiev, Great Britain's minion Estonia witnessed the largest military exercise in the area of conducting the information war in the cyberspace in the history of NATO (Cyber Coalition 2013). Almost 500 people took part in the exercise – more than 100 employees of the NATO Cyber Centre in Tallinn and more than 300 officers – member and partners of the Alliance – from 32 countries remotely.

It is possible that the scenario of this exercise involved the possibility of waging information war against Russia (the supposedly fictitious country Botnia), including the information support in the cyberspace for the organization of the coup d'état in Kiev. Afterwards London, the main host of the NATO Cyber Centre, considers plans to create an army of internet trolls, numbering 2000 people, in support of this. It means that the information confrontation in social networks will only increase.

Finally, attention should be drawn to the creation of new special structures (U.S. Cyber Command) and the active communication offensive strategy of the new organizations such as the British-American Communication Sledgehammer (CS), attempting to influence the decision-making system in Russia (sanctions, etc.).

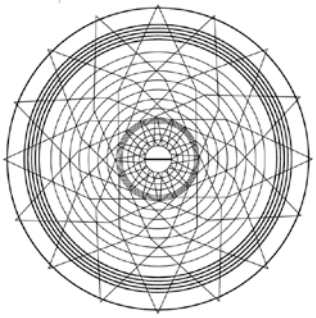
British-American Communication Sledgehammer is a system of British-American government bodies, exerting influence on the decision-making process in Russia in order to achieve their objectives in the conduct of information war against Russia. Communication Sledgehammer consists of the U.S. State Department, the Foreign Office, British and American media outlets, the system "ECHELON", the CIA, MI6, U.S. National Security Agency, Government Communications Headquarters and special operations forces.

3. On pre-emptive and proactive measures

The ability to undertake pre-emptive and proactive measures becomes a defining advantage in the course of the intensifying Hybrid World War.

It cannot be said that the leadership of our country doesn't understand the importance of this sphere. It isn't the case. The Russia Today was established and has been successfully operating; Dmitry Kiselyov, Konstantin Syomin, Arkady Mamontov and a number of other journalists do a great job on television. These information efforts are partially underway but, considering the long-standing systematic effort being made against us, it requires the systematic strategic response that we do not have yet.

Apart from the response to the growing acts of hybrid warfare being waged against Russia, it is important for Russian authorities and largest corporations to intensify their efforts in the area of information. It is not very promising to be confined to the defensive position. It is necessary not only to take pre-emptive measures and



countermeasures, but actively undertake well thought-out systematic steps that are offensive in nature.

The results of an expert survey conducted by me in March 2018 are of interest in this context.

In your opinion, how effective is the Russian system of the information confrontation (on a scale from 1 to 10, overall scores)

A. in the course of operation to defeat ISIS in Syria = **8**
B. in the course of the so-called «hacking scandal» in the U.S. presidential election = **3,5**
C. in the course of the doping scandal with Russian athletes **= 3**
D. in the course of the scandal with the seizure of Russian diplomatic property in the United States - **2,5**
E. in the course of the scandal with the alleged poisoning of the traitor Skripal in British Salisbury on March 2 2018 - **3,5**

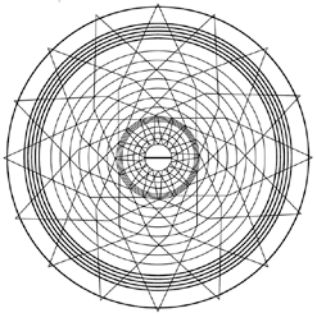
The biggest challenge facing Russia is the lack of institutional mechanisms, coordination structures. To effectively conduct the information confrontation, in my opinion, The Information Security Committee of Russia should be established to which various professionals in the field of information from different agencies such as FSB, the Ministry of Internal Affairs, Federal Protective Service, Foreign Intelligence Service, Ministry of Foreign Affairs, state media and other agencies involved in the system of conducting information operations (defensive and offensive) could be assigned.

We also need a The Presidential Council of State and the Regional Councils for information confrontation, the respective adviser to the head of the state should be appointed. Finally, there is an urgent need for the state-owned internet holding. It would be also advisable to redirect our submarines with cruise missiles towards the information and economic command centers in the West. It is sufficient to promise that in the event of military aggression against Russia they will be immediately destroyed. It will serve as a strong deterrent.

The Russian system of information confrontation could be set up in the following way:

1. The Presidential Council of State for information confrontation (the executive and legislative branches of government, the mass media, business and civil society).
2. Regional Councils for information confrontation, headed by the authorized representatives of the Russian President in the federal districts.
3. The Information Confrontation Adviser to the Russian President.
4. The Coordination Council for information confrontation, headed by the Russian Minister of Foreign Affairs.
5. The interdepartmental coordination centre for countering ISIS at an information and ideological level.
6. Communications Centre to stabilize the situations in the countries of the Middle East and the Eastern Europe after the «color revolutions» that took place there.

© Communications. Media. Design, Vol. 3, N°3, 2018



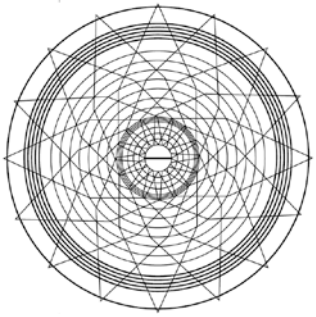
7. The Russian Information Security Committee (Cyber Security Service, The Information Counterintelligence Service, the Situation Centre for analysis and forecast, The Bureau of Information Special Forces for conducting the operations abroad).

Amidst the Second World Information War Russia should focus its efforts on the following areas:

1. Laying the foundation of a national system to counter the information war operations against the Russian leadership and population.
2. The creation of national legislation aimed at countering «color revolutions» technologies.
3. Detection and diagnosis of the activities of negative communicators seeking to undermine the information integrity of Russia. The ongoing monitoring of the blogosphere and social media in order to stop the negative information aimed at promoting extremism and terrorism, inter-ethnic and interfaith discord from spreading in the Russian information space.
4. The preventive blocking of all flows (financial, information, organizational) and structures of foreign and oligarchic support for the radical and extremist opposition in Russia.
5. Strengthening information sharing and international cooperation with our allies in the military-security, financial, economic and information-psychological spheres to take the necessary steps for detecting and tackling the threats to the national security of Russia.

Summary

This article describes the role of strategic communications, information and hybrid warfare in the world politics. The information onslaught of the West will be growing in intensity. This is demonstrated by the strategic offensive information operation conducted by MI6 (the alleged poisoning of the traitor Skripal). That's why the appropriate countermeasures should be taken and enhanced. The theoretical approaches to **setting up a Russian system of information confrontation** are outlined in the article.



REFERENCES

Bartosh A.A Gibridnaya voyna stanovitsya novoy formoy mezhgosudarstvennogo protivoborstva. 7 April 2017. URL: http://nvo.ng.ru/concepts/2017-04-07/1_943_gibryd.html

Gerasimov V. V. Vystuplenie na Nauchno-prakticheskoy konferentsii "Voennaya bezopasnost' Rossii: XXI vek", Moskva, 14 February 2013. URL: http://arm-ob.ru/interviy/

Ishchenko R. Matritsa gibridnoy voyny, ili Zachem nuzhen informatsionnyy genshtab. 20 September 2016. Rostislav Ishchenko, MIA "Rossiya segodnya"

Klimenko S. (2015). Teoriya i praktika vedeniya "Gibridnykh voyn" (po vzglyadam NATO) 2015. - Zarubezhnoe voennoe obozrenie, N°5, P.109-112

Lassuell G. (1929). Tekhnika propagandy v mirovoy voyne. Moscow-Leningrad.

Lisichkin V.A. Shelepin L.A. (2000). Tret'ya mirovaya informatsionno-psikhologicheskaya voyna. Moscow.

Mal'chikova V. Interaktivnoe veshchanie SShA, kak sredstvo vedeniya «gibridnoy voyny». Moscow, 16 January 2018 URL: http://vpoanalytics.com/2018/01/16/interaktivnoe-veshhanie-ssha-kak-sredstvo-vedeniya-gibridnoj-vojny/

Panarin I.N. (2016). Gibridnaya voyna protiv Rossii (1816-2016). Moscow.

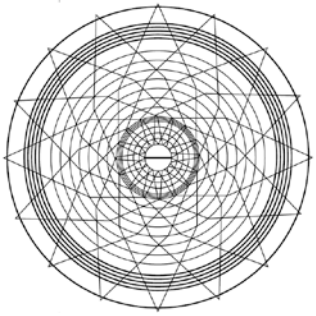
Panarin I.N. (2017). Gibridnaya voyna: teoriya i praktika. Moscow.

Panarin I.N. (2014). Informatsionnaya voyna i kommunikatsii. Moscow.

Ponomareva E.G. Tekhnologii smeny politicheskikh rezhimov. Natsional'naya bezopasnost', Minsk, N°2.

Pukhov R.N. Mif o «gibridnoy voyne». Nezavisimoe voennoe obozrenie. 29.05.2015

© Communications. Media. Design, Vol. 3, N°3, 2018



СТРАТЕГИЧЕСКИЕ КОММУНИКАЦИИ И МИРОВАЯ ПОЛИТИКА

Панарин И. Н.
доктор политических наук,
глава Ассоциации «Информационный спецназ»
(Москва, Россия)
jsjyoti@gmail.com

Аннотация:

В представленной статье автор дает характеристику текущей гео-политической и гео-экономической ситуации, в которой оказалась Россия, а также делится некоторыми своими соображениями относительно инструментов и методик ведения гибридных войн. В числе рассматриваемых техник и инструментов проанализированы такие явления, как дезинформация, терроризм и другие.
Автор указывает на риски текущей ситуации и необходимость разработать новую коммуникационную стратегию для России, которая позволила бы защититься от информационных и гибридных атак. Приведены отдельные примеры таких атак, а также возможные стратегии информационного менеджмента в будущем.
В конце статьи автор дает некоторые общие рекомендации относительно усиления коммуникационной стратегии, направленной не только на защиту, но и на завоевание новых позиций на мировой геополитической и гео-экономической арене.

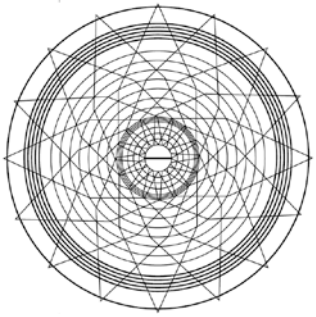
Ключевые слова: социальные медиа, гибридная война, информационная война, Россия, Украина, Великобритания, Владимир Путин, инструменты пропаганды

БИБЛИОГРАФИЯ

Бартош А.А. Гибридная война становится новой формой межгосударственного противоборства. 7 апреля 2017 года http://nvo.ng.ru/concepts/2017-04-07/1_943_gibryd.html

Герасимов В. В. Выступление на Научно-практической конференции "Военная безопасность России: XXI век", Москва, 14 февраля 2013 г. ресурс: http://arm-ob.ru/interviy/

Ищенко Р. Матрица гибридной войны, или Зачем нужен информационный генштаб 20 сентября 2016. Ростислав Ищенко, МИА "Россия сегодня"



Клименко С. (2015). Теория и практика ведения "Гибридных войн" (по взглядам НАТО) 2015. Зарубежное военное обозрение, №5, С.109-112

Лассуэлл Г. (1929). Техника пропаганды в мировой войне. М.-Л..

Лисичкин В.А. Шелепин Л.А. (2000). Третья мировая информационно-психологическая война. М.

Мальчикова В. Интерактивное вещание США, как средство ведения «гибридной войны». М., 16 января 2018 г. - http://vpoanalytics.com/2018/01/16/interaktivnoe-veshhanie-ssha-kak-sredstvo-vedeniya-gibridnoj-vojny/

Панарин И.Н. (2014). Информационная война и коммуникации. М.

Панарин И.Н. (2016). Гибридная война против России (1816-2016). М.

Панарин И.Н. (2017). Гибридная война: теория и практика. М.

Пономарева Е.Г. Технологии смены политических режимов. Национальная безопасность, Минск, №2.

Пухов Р.Н. Миф о «гибридной войне». Независимое военное обозрение. 29.05.2015

© Communications. Media. Design, Vol. 3, №3, 2018