STATE POLICY AGAINST INFORMATION WAR

DMITRY SHIBAEV,
North-Western Institute (branch) of Kutafin Moscow State Law University
(Vologda, Russia)

NINA UIBO,
North-Western Institute (branch) of Kutafin Moscow State Law University
(Vologda, Russia)

DOI: 10.17589/2309-8678-2016-4-3-136-156

The most recent and effective method to resolve a conflict between countries is information war. Information warfare, i.e. propaganda, information sabotage, blackmail, could be more damaging than the effects of the traditional methods of war. The government must be prepared to prevent and counteract the bleeding-edge techniques of warfare that is to work out measures, to oppose enemy's information weapons , to gain information superiority , to develop a society that is immune to disinformation, to elaborate a concept of information warfare counteraction.

The authors have examined both foreign and Russian sources of law which define the requirements for the government activities to oppose information warfare. They also refer to the opinions of foreign and Russian researchers, politicians and public figures who have commented on the concept and features of such political and legal constructs as information warfare and information weapons. The problem of information warfare must be identified as a profoundly serious and damaging threat. This paper provides the features of information warfare and the methods to resist it as well as the proposals to amend the domestic legislation to create conditions for an accurate understanding of this political and legal phenomenon. In addition, it points out that the amendment of the Information Security Doctrine is not sufficient to counterbalance the threat of information warfare. In a certain document it is necessary to recount all notions, requirements and methods for the government actions aimed to gradually change the situation, particularly, the development of sectoral (information security) legislation, specialists training to be able to deal with informational and psychological aggression forming public opinion through the government-run mass media, etc.

Keywords: information war (IW); information weapons; methods to counteract information warfare techniques; individual, society; state, defense; cyber war; information superiority; information security; government-run mass media.

Recommended citation: Dmitry Shibaev, Nina Uibo, *State Policy Against Information War*, 4(3) Russian Law Journal 136-156 (2016).

1. Socio-Political Aspects of Information Warfare and Information Security

Up to now, speaking specifically about the countries with nuclear status, the use of conventional weaponry has been regarded as an ultimate measure to resolve conflicts. The perspective to get involved into large-scale military hostilities and to pose danger to its citizens is not a priority for any state under any condition. At the same time, the issue of repartition of economic and political spheres of influence is critical. Struggle for new markets, energy resources, political 'points' causes stress in the world. For example, the Georgian-Ossetian-Russian conflict, Egypt, Syria, Turkey, Libya, Ukraine. In all those cases the conflict was aggravated with information components like discontent with the current regime, a provoked conflict, the use of social networks to rally and control protests, spreading a negative image of the legitimate government through television and radio. If all of the above-mentioned are meticulously prepared, exploited on time and based on true or false drawbacks of the authorities then they will destroying the government much more effectively than costly (in terms of human and economic losses) military operations.

The use of information war methods takes different forms and all of them are carried out through protests for coups or for substantial weakening, in political, economic and social terms of the current government. These are information warfare and information war (IW) components that are used for the so-called 'color' revolutions.[1]

It is worth mentioning that according to a well-known expert I.N. Panarin, there have already been two global information wars in the history of the human race. As for Russia, it lost the first world information war (1943–1991). Now the second world information war is being waged against it. According to the analyst, the United States have started both wars. In particular, he points out that the statesman Henry Kissinger was one of the main ideologists of the first information war against the Soviet Union. The aim was to set the 'fifth column' inside the Soviet state which has undoubtedly contributed to the disintegration of the country. The Central Intelligence Agency (CIA) Director Allen Dalles also contributed to the defeat of the USSR. In the

[1] Gene Sharp, Dr. The Methods of Nonviolent Action (Boston, Porter Sargent 1973), available at <http://www.quakerquaker.org/profiles/blogs/dr-gene-sharps-198-methods-of> (accessed Apr. 26, 2016).

fall of 1945 he formulated the concept of information war against the Soviet Union and organized the 'Anti-Stalin operation' (after Stalin's death Khrushchev, Gorbachev came to power in the country).[2] They were, in fact, controlled from abroad.

The American spy George Frost Kennan in 1945 identified the main direction of the information war against the Soviet Union in the postwar period. It must have been covert information operations to influence the decision-making system in the Soviet Union during the transition period when the political elites changed. G. Kennan revealed the difficulties of the government transition in the USSR. Every time there was a change in the government of the USSR, the political struggle flared up among the cronies of the former head of the country as well as among his opponents. In addition, G. Kennan confirmed his findings with the analysis of the negative experience of the information operations of the British Empire Intelligence in Russia. Thus, in 1910 the British Intelligence MI-6 achieved the appointment of Sazonov to the Minister of Foreign Affairs with the Russian Empire, who 'took Herculean efforts to organize Russia's entry into World War I, which was absolutely futile for Russia.'

According to I.N. Panarin, the purpose of the second global information warfare was "the elimination of an alternative model for the development of the world which is fundamentally different from the model of liberal colonialism" based on the lack of spirituality, slave trade, drug trafficking and financial fraud. I.N. Panarin counts the start of the second information war beginning with the year 2000, when V.V. Putin headed Russia. 'Anti-Putin operation' began after 24 September 2012 when the Congress of 'United Russia' adopted Putin's pre-election program which included elements of a new ideology. That new ideology was based on the article dated 30 December 1999 with the key words: 'patriotism, statehood, nationhood (gosudarstvennichestvo), social solidarity.' Moreover, I.N. Panarin emphasizes that 'during 'Anti-Putin' operation, basically the same technique and technology of lies and false information were used like in 'Anti-Stalin' operation'. The only difference is availability of a wider variety of new contemporary media and mass communication options, i.e. Internet, Global TV, social networks, networks of Non-governmental organizations (NGO) and paid bloggers.'[3]

The speeches of experts and journalists in various television and radio programs may be considered as one of the manifestations of information war. For example, on 1 November 2015 on TV channel 'Russia-24' the subject of the author's program 'Sunday Night with Vladimir Solovyov' was the information war between Russia, Western European countries and the United States.

---

[2] Панарин И.Н. Первая мировая информационная война. Развал СССР [Panarin I.N. Pervaya mirovaya informatsionnaya voina. Razval SSSR [I.N. Panarin, The first world information war. Collapse of the USSR]], available at <http://www.x-libri.ru/elib/panrn000/> (accessed Nov. 25, 2015).

[3] Панарин И.Н. Информационная война: Операция «Анти-Путин» [Panarin I.N. Informatsionnaya voina: Operatsiya 'Anti-Putin' [I.N. Panarin, Information war: Operation 'Anti-Putin']], available at <http://www.km.ru/spetsproekty/2012/01/16/otnosheniya-rossii-i-ssha/informatsionnaya-voina-operatsiya-anti-putin> (accessed Nov. 11, 2015).

With regards to the concept of 'information warfare' the program participants expressed different opinions. Vladimir Ryzhkov (the chairman of the social movement 'Russia's Choice') used the word 'prejudice' when speaking of information war. He exemplified saying that an American journalist did not necessarily write by command from the US State Department, in other words, 'if he has been prejudiced against the Russian authorities, he writes about it because he thinks this way'. Further, V. Ryzhkov said that Russia had 'immense prejudice towards the West' and that the Russian state-controlled media 'add fuel to the fire very often' and consequently 'a huge burden of prejudice on both sides had been accumulated making the situation extremely dangerous.' The social activist claimed that it should not be simplified and that the Europeans and Americans 'maintain their own stereotypes', and the Russians stick to their own stereotypes. The interpretation matters because if every day one keeps saying 'the entire West hates us, all in the West want to destroy Russia, it is a lie.'[4] Leonid Gozman (the president of the fund 'Perspective') observed that the image of any country could be portrayed to the world with the tools of information warfare in the way one wants.

The French journalist Dmitry de Koshko, a representative of the news agency 'Agence France Presse' referred to the use of mass media as a means to achieve the objectives of information war. He believes that civil society needs complete and balanced information to function, but it doesn't have it in France at present. He said that in March 2015 the General Gomar had been questioned by the Defense Committee of the National Assembly of France, particularly what kind of relations were between France and NATO. The General reported that the Americans because of their influence in NATO had been trying to impose incorrect information on the Frenchmen. It also concerned the events in eastern Ukraine ('they tell us that Russians fight there and we have checked – there are Russian soldiers there, of course, but they are not waging a war'). Gomar argued that the information was available to the public on the network Internet, but none of the French journalists published it. On the contrary, they (the French journalists) continued to write that Russian troops were fighting in the east of Ukraine.

The opinion of Charles Bausman, a representative of the United States, was also noteworthy. He believes that the problem of America is that the media are in the hands of a very narrow group of people who conduct aggressive policy against Russia and the countries of the Middle East. These people determine everything. They offer relevant materials to US journalists and give them jobs. Bausman underlines that such policy does not come from the official representatives of the government, but from 'private capital' or transnationals.

Vladimir Solovyov gave one more fact of the information war against Russia. In his words, the site 'The Peacemaker' had been created on the NATO domain. It was supported by the advisor of the Head of the Ministry of Internal Affairs of Ukraine Anton Gerashchenko. Russian opposition posted there the information and personal

[4] Воскресный вечер с Владимиром Соловьевым [Voskresnyi vecher s Vladimirom Solov'evym [Sunday evening with Vladimir Solovyov]], available at <http://www.pravda-tv.ru/2015/11/02/185898> (accessed Nov. 27, 2015).

data on people who had political views different from the views of US leadership. Also on this site the information was published about the families of the Russian soldiers who were in Syria with a view to further influence on them. V. Solovyov said that in the United States, a person for the same offense would inevitably be punished if those acts were committed, but against US troops. 'Lie is never for the benefit of good, every journalist of any country should understand it, regardless of the political objectives he is trying to solve' V. Solovyov summed up the discussion.

One can see that the types and forms of information warfare and technologies of information war are quite diverse. At the same time arises the question why, knowing the general principles of information warfare technologies and methods of their use, do more countries become their victims?

In our opinion, the reason is the lack of research on the issue of protection from the information weapons. Currently, much more attention is paid to the modernization of real weapons, to the enhancement of the combat capability of the army (which is very important, no doubt), but at the present stage it is not sufficient.

Politicians (most often – demagogically) proclaim the principle of the united world without shocks and global problems in harmony with the principles of democracy of a free society, tolerance and unipolar world.[5] However, the 'preacher' of the unipolarity and democratic values Henry Kissinger in his work called 'Henry Kissinger's new world order' indicates that it is doubtful that the world order can be maintained by some calls for the rule of law, not backed by the appropriate strategies.[6] Only consciousness and voluntariness cannot help to avoid shocks and unrest. This has been reflected in the recent political and legal development in the Russian Federation, namely, the development and adoption of a new Military Doctrine of the Russian Federation in 2014.[7] Especially it is recognized as a characteristic feature of today's military conflicts, the comprehensive use of military force, political, economic, information and other non-military measures implemented with the extensive use of the protest potential of the population, political forces and social movements financed and managed from abroad through social networks and media services and jurisdictionally inaccessible for the country which is the goal of the information influence in question. Actually, a military doctrine is relevant for use within or in preparation for potentially possible military action. In the Doctrine a counteraction refers to an external enemy but the information war is mostly waged from the inside by the so-called 'fifth column.'

---

5 *Id.*, John L. Sullivan, James Piereson and George E. Marcus, *Political Tolerance and American Democracy,* 89(4) Am. J. of Soc. 963–966 (1984) <http://www.jstor.org/discover/10.2307/2779266?sid=21105059805761&uid=4&uid=2> (accessed Apr. 26, 2016).

6 Mark Peffley, Robert Rohrschneider, *Democratization and Political Tolerance in Seventeen Countries: A Multi-level Model of Democratic Learning,* available at <http://www.uky.edu/AS/PoliSci/Peffley/pdf/WVSPRQFinal_1-31-03_.pdf> (accessed Apr. 26, 2016).

7 *Henry Kissinger on the Assembly of a New World Order*, The Wall Street Journal, available at <http://www.wsj.com/articles/henry-kissinger-on-the-assembly-of-a-new-world-order-1409328075> (accessed Apr. 26, 2016).

In parallel with the improvement of the army, it is imperative to accomplish a complex of steps to ensure the informational security within the country in peacetime. The Russian Federation has adopted and applied the Information Security Doctrine, but in our opinion, it is not an adequate protection against information warfare. The Doctrine as a summation of official views on the goals, objectives, principles and guidelines of information security of the Russian Federation[8] does not fully correspond to modern realities. It was designed in 2000 when the technology of 'color revolutions' had not been sufficiently tested yet, or, at least, in the countries similar to the Russian Federation in polity and mindset. At that time Russia had not employed such means of mass communication management to control public opinion as the Internet and social networks, in particular. Today all these components are available in the Russian Federation for the information war to succeed. Therefore, in our view, it is crucial to revise approaches to combat information warfare and further elaborate the Doctrine to match contemporary realities.

2. Concept and Features of the Definition of 'Information War'

To begin with, it is essential to define two substantial concepts. They are: information war and information warfare. So far there have been no distinct characteristics of these definitions in the Doctrine, but the phrases occur twice:

1. the first in p. 3 of the Doctrine listing the external threats to information security, i.e. the development of the concepts of information war by a number of states which provide the production of malware and devices of hazardous impact to the information domains of other countries; the disruption of normal functioning of information and telecommunication systems, preservation of information resources and gaining unauthorized access to them;

2. the second in p. 9 of the Doctrine as a measure to implement the state policy of information security of the Russian Federation, in other words, a complex to neutralize the threats of information warfare.

Neither the Doctrine in force[9], nor the draft of a new doctrine[10] on information security of the Russian Federation, (the draft was being developed during 2015), indicate the information war as an objective. We keep the view point that the lack of a clear definition hinders further efforts to identify and counteract it.

---

[8] Военная доктрина Российской Федерации [Voennaya doktrina Rossiiskoi Federatsii [Military doctrine of the Russian Federation]], available at <http://news.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf> (accessed Apr. 26, 2016).

[9] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) [Doktrina informatsionnoy bezopasnosti Rossiiskoy Federatsii [Information Security Doctrine of the Russian Federation (approved by the President RF 09.09.2000 No Pr-1895)]], Rossiiskaia Gazeta [Ros. Gaz.] Sept. 28, 2000.

[10] Approved by the working group of the Interdepartmental Commission of the Security Council of the Russian Federation for Information Security on 5 October 2015.

However, several legal acts, namely, the Order of the Government of the Russian Federation dated July 7, 2014 No 1271-p[11] and the Order of the Government of the Russian Federation dated September 17, 2013 No 1672-p[12] contain a holistic notion of information warfare. The information war is regarded in them as:

– A confrontation between two or more nations in the information realm with the aim to damage information systems, processes and resources, critical and other objects, to undermine political, economic and social systems, to psychologically manipulate population on a mass scale to destabilize society and state and to force government to make decisions in the interests of its adversary;

And information weapons as:

– Information technology, tools and methods used for the purpose of information warfare.

In scientific literature two interrelated concepts are used. They are 'information war' and 'cyber war'.[13] In our opinion, these notions are neither equivalent, nor interchangeable. They are correlated as a part and a whole. Information war is the whole and it includes actions, environment and the instruments for these actions. As to cyberwar, it implies environment but the realm of cyberspace alone, and its instruments include electronic means of communication. In broad sense, information confrontation (war) can be carried out, in addition to the most popular, electronic tools by a wider variety of media options such as television, radio, newspapers, etc. One can safely say that however, the use of cyberspace, i.e. Internet and alternative intra- and extra networks, is the cheapest and simultaneously the most effective vehicle of information warfare. In general, communication is considered by many vital aspects of information war.

Thomas Rona, a scientific adviser to the US Ministry of Defense at the White House, was the first to use the concept of 'information war'. In 1976 he discerned some signs of information war in his report 'Systems of weapons and information war' for Boeing[14] Company. They were as follows:

– increase of the information volume of one's own;

---

[11] Проект доктрины информационной безопасности РФ [Proekt doktriny informatsionnoy bezopasnosti RF [Draft of Information Security Doctrine]], available at <http://infosystems.ru/assets/files/files/doktrina_IB.pdf> (accessed Nov. 28, 2015).

[12] Распоряжение Правительства РФ от 10.07.2014 № 1271-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности» [Rasporazhenie Pravitelstva RF ot 10.07.2014 №1271-p 'O podpisanii Coglashenia mezhdu Pravitelstvom Rossiiskoy Federatsii I Pravitelstvom Respubliki Kuba o sotrudnichestve v oblasti obespechenia mezhdunarodnoi informatsionnoi bezopasnosti' [Resolution of the Government of the Russian Federation of 10.07.2014 № 1271-p 'On signing the Agreement between the Government of the Russian Federation and the Government of the Republic of Cuba on cooperation in the field of guaranteeing international information security']], Официальный интернет-портал правовой информации [Ofitsialnyi internet-portal pravovoi informatsii [Official internet-portal of the legal information], available at <http://publication.pravo.gov.ru/page.aspx?110913> (accessed Apr. 26, 2016).

[13] UK cyber security a top priority for UK Government: press release, available at <https://www.gov.uk/government/news/uk-cyber-security-a-top-priority-for-uk-government> (accessed Feb. 20, 2016).

[14] Thomas P. Rona, Weapon Systems and Information War (Boeing Aerospace Co., Seattle, WA 1976).

– hampering access to truthful information for enemy;
– spoofing information flows for enemy;
– significance of information flows for enemy's actions.

Many other scientists have also developed their approaches to the definition of 'information warfare'. According to G.G. Pocheptsov, the theory of information warfare has evolved several stages. The first stage was in the early 1990s. A group of scientists of the USA Air force Aviation University studying the war of the future formulated the requirements for such war and a soldier's brain was said to be the weakest element on the battlefield. In particular, John Stein in 1995 in his article called 'Information war' defined information war as a means to achieve national goals through information.[15] In 1994 R. Szafranski underlined the importance of the mental dimension and the highest spiritual values: knowing the system of enemy's values, one can communicate with his brain and consequently impose one's will.[16]

The second stage was in the late 1990s and was characterized by the activity of the US expert on international relations J. Arquilla, who first highlighted the fundamental problems of information strategy, cyber war and network warfare including information war.[17] Cyber and network wars are, in fact, varieties of modern conflicts. To be more precise, a cyber war is a conflict of high and medium intensity, but a network war is a low-intensity conflict or operation different from war. For him the term 'information war' is too broad since it tries to encompass everything, though, on the other hand, it is too narrow due to its reference to restricted high-tech issues of security and susceptibility of cyberspace.

In the third phase (2000s) the military were active who due to the result of the wars of the past two decades gave up the traditional methods of war and focused on the use of the so-called 'soft force' and particularly the 'operations of influence'. Nevertheless, no significant expansion of the theoretical framework was made at that time. One of the representatives of that stage M. Libicki, defined information war as an attack of information on the data[18], i.e. when the opponents tried to prove that their information was more plausible than the information offered by their rivals.

Under 'information war' G.A. Atamanov implies a kind of 'confrontation of social systems, which admits physical destruction of infrastructure of opposing systems, IT being a major resource for it.'[19]

---

[15] *Почепцов Г.Г.* Информационная война: определения и базовые понятия [Pocheptsov G.G. Informatsionnaya voina: opredeleniya i bazovye ponyatia [G.G. Pocheptsov, Information war: definitions and basic concepts]], available at <http://psyfactor.org/psyops/infowar25.htm> (accessed Nov. 25, 2015).

[16] Szafranski R. Neocortical warfare? The acme of skill (J. Arquilla, D. Ronfeldt eds., Santa Monica 1997).

[17] Arquilla J., Ronfeldt D. The advent of netwar, available at <http://www.rand.org/pubs/monograph_reports/MR789.html#toc> (accessed Apr. 27, 2016).

[18] Libicki M. Conquest in cyberspace. National security and information warfare (Cambridge 2007).

[19] Атаманов Г.А. Информационная война: экспликация понятия [Atamanov G.A. Informatsionnaya voina: ekcplikatsiya ponyatiya [G.A. Atamanov, Information war: explication of the concept]], available at <http://www.naukaxxi.ru/materials/254/> (accessed Nov. 26, 2015).

As for the international law, it does not enshrine the concept of 'information warfare', however, domestic legislations of some countries have such a term.

For example, the Chinese military strategy[20] specifies the information war in broad and narrow senses. In a narrow sense it is military battles in the area of command and control of troops, but in a broad sense it is large-scale hostilities with the prevalence of an information component characterized by the use of specially designated military forces and high precision weaponry. Thus, according to the Chinese national law, information war is one of the ways of warfare.

A.V. Manoilo[21] has summarized the key notions of information warfare. Some excerpts from his survey are given below.

One of the most prominent think tanks in the field of informational confrontation, L.L.M. V.I. Tsymbal[22] also points out that the notion of information war has broad and narrow senses. In a broad sense it is one of the ways of confrontation between two countries which is carried out mainly in peacetime, where the civilian population, society, state administrative system, the structure of production management, science, culture along with the armed forces are the targets for influence.

In a narrow sense, information war is a kind of hostilities or direct preparation for them, which aims to achieve an overwhelming advantage over enemy in the process of receiving, processing and using the information to develop effective administrative decisions and also successful implementation of activities to dominate over its opponent on that basis.

V.S. Pirumov[23] defines information war as a new form of struggle between two or more parties, which is a purposeful use of special means and methods of influence on the enemy's information resources and protection of one's own information resources to achieve the assigned objectives. In his opinion, in times of peace the information war is mostly hidden. Its main task is, on the one hand, to carry out political and psychological operations against the enemy and, on the other hand, to ensure the information security of the influencer. In a situation of real confrontation of states, the forces and means of information warfare solve such tasks as:

---

[20] China's Military Strategy <http://eng.mod.gov.cn/Database/WhitePapers/index.htm> (accessed Apr. 26, 2016).

[21] Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны [Manojlo A.V. Gosudarstvennaja informacionnaja politika v uslovijah informacionno-psihologicheskoj vojny [Manoilo A.V. State information policy in conditions of information-psychological war]], available at <http://psyfactor.org/lib/psywar25.htm> (accessed Apr. 26, 2016)

[22] Цыбмал В.И. *О концепции информационной войны*, 9 Информационный сборник «Безопасность» 35 (1995) [Tsybmal V.I. *O kontseptsii informatsionnoi voiny,* 9 Bezopasnost 35 (1995) [V.I. Tsybmal, *On the concept of information war*, 9 Security 35 (1995)]].

[23] Пирумов В.С., Родионов М.А. *Некоторые аспекты информационной борьбы в военных конфликтах*, 5 Военная мысль 44–47 (1997) [Pirumov V.S., Rodionov M.A. *Nekotorye aspekty informatsionnoi borby v voennyh konfliktah,* 5 Voyennaia mysl 44–47 (1997) [V.S. Pirumov, M.A. Rodionov, *Some aspects of information struggle in military conflicts* 5 Military thought 44–47 (1997)]].

– The massive exposure of the enemy's information resources and the prevention of the reduction of the combat capabilities of its own forces;

– The implementation of measures to lower the level of the enemy's moral and psychological stability and the neutralization of information that affects the morale of its own troops;

– Intelligence activities and covert character of the most critical military operations of its own armed forces, etc.

Professor S.P. Rastorguev[24] defines information war as open and covert targeted informational impact of information systems on each other in order to get certain gains in the material sphere. It is a very good definition which highlights the two basic features of information war. The main objective of the information war (information-psychological) at the tactical level is to have certain material benefits but in the process of information warfare some participants of the confrontation receive these benefits, while others lose them. For those who lose, these losses may serve as a quantitative expression of the material damage caused by war.

A number of foreign scientists[25] define the concept in question as a class of methods, including the collection, transportation, security, denial, disruption and distortion of information which are used to maintain an edge over the adversaries[26]. One can safely say, foreign researchers in most part in essence do not contradict the viewpoints of Russian scientists but expand the concept with the methods of information warfare.

3. Proposals for Amendment of the Information Security Legislation

We consider it would be logical to amend section 1, paragraph 2 of the Information Security Doctrine and to incorporate the characteristics of the concept of 'information war' in terms of the following legal acts – the Order of the Government of the Russian Federation dated 7 July 2014 No. 1271-p and 17 September 2013 No. 1672-p expanding them with the viewpoints of S.P. Rastorguev and V.I. Tsymbal.

Information warfare is a confrontation that is a targeted open and covert informational impact of two or more states in the information realm carried out mainly in peacetime with the aim to damage the information systems, processes and resources, critical and other objects, to undermine the political, economic and social systems, to psychologically influence the population on a mass scale, to destabilize

---

[24] Расторгуев С.П. Информационная война [Rastorguev S.P. Informatsionnaya voina [*S.P.* Rastorguev, Information war]] 35–37 (Moscow, Radio i Svyaz, 1999).

[25] *Id.*, Martin C. Libicki, What is Information Warfare? (Washington DC, Institute for National Strategic Studies, 1996); John Arquilla and David Ronfeldt, The Advent of Netwar 3 (Santa Monica, RAND 1996); Winn Schwartau, Information Warfare (New York, Thunder's Mouth Press 1996).

[26] Ajay Singh, Information Warfare: Reshaping Traditional Perceptions gives this definition, available at <http://www.idsa-india.org/an-mar-4.html> (accessed Apr. 26, 2016).

society and the state and, in fact, controlled from abroad (as well as to force the state to take decisions in the interests of its adversary.

The authors propose to supplement the concept given in the RF Government Decrees with the provisions of the aforementioned scientists:

1. Features (in particular, latency) of informational influence which help to identify individual information flows as a part of the information war and to stop them or distort.

2. The time, mostly in peaceful times, when the forces and means of counteraction of both public and social sectors are not in a belligerent situation. In other words, there is no mass propaganda, no martial law and no censorship, etc.

Section 2 of the Doctrine in question should include the characteristics and threats of information warfare and methods to fight them. We'll mention but a few. They are:

I. Principal ways to achieve information superiority in information war should be specified. These may include:

1. Covert management of both the activities of an enemy government and the information (including information-psychological) processes which predetermine the social, political, economic, spiritual system of relationships of a rival state;

The most relevant and effective way of control is the use of 'agents of influence', i.e. persons having certain powers (employees of public authorities) or able to influence the authorities with material gains or moral incentives.

There are such persons in today's Russia and at his press conference 'Direct Line with Vladimir Putin' the President clearly stated that as it turned out today ... during the period of Chubais's work in the government there had been salaried CIA employees as advisers in his surroundings.[27] The presence of such 'agents of influence' creates problems not only with the protection of state top secrets but also violates the national interests, for example in the form of distortion of the processes of international cooperation with the existing or potential alliesif they do not fall within the scope of interest of a foreign state having introduced these 'agents of influence'.

Violations of the state's interests in the sphere of the national economy are also feasible. For example, a biased selection of suppliers of technology or equipment predetermines the dependence of state from foreign countries for many years to come and even if the contract is not a long-term one, the recipient becomes dependent on the technology supplied and will have to seek for the same provider. The agents of influence are no longer needed but they have done their job.

The spiritual life of society is another important element in the activities of the agents of influence. Different sects and religious movements, making use of the right to religious freedom and preaching their own beliefs on the territory of the state under information war attack, limit the endeavour of the traditional church to support the people who joined those sects. Sectarianism, especially totalitarian,

[27] Прямая линия с Владимиром Путиным [Pryamaya linia s Vladimirom Putinim [Live with Vladimir Putin]], available at <http://kremlin.ru/events/president/news/17976> (accessed Feb. 10, 2016).

exponentially increases the number of agents of influence recruiting them from among the citizens of the victimized nation. In addition, a sectarian church itself is able to invent a pretext for information war. In that case, there was an explosion in the prayer house of Russia's largest community of the sect of Baptists-Initsiativniks in Tula. The Law enforcement agencies investigated the case and the cause of the explosion was named. It was a gas leakage. The explanation did not satisfy certain individuals. Later, at the hearings of the 'Helsinki Commission' of the US Congress Andrey Ohotin, a representative of the Association of the Independent Russian Baptists, insisted on his version of a terrorist act against the Baptists. He claimed that the explosion had been committed intentionally in order to destroy the representatives of the management of the Ivanovo Baptists who had visited Tula those days. The reaction of the US Congress aimed to deteriorate Russia's reputation follows such speeches immediately. The US House of Representatives has made a frankly anti-Russian resolution based on the Baptists' statements. The congressmen have expressed dissatisfaction with 'the violation of the rights of the believers and the restriction of religious freedom in Russia'. The essence of the draft prepared by the Helsinki Commission of the Congress is that the rights of the non-traditional beliefs in Russia are infringed in terms of registration and their activities.[28]

2. Unconcealed Informational and Psychological Aggressions

The latest and most striking example of aggression is the TV show 'World War Three: Inside the War Room' on BBC-2 which simulated the situation of Russian attack on Latvia. According to Alexander Veshnyakov, the Russian ambassador to Latvia, it is a dangerous provocation because 'the scenario is completely contrived pursuing political goals like:

– first, to engage in the information war to demonize Russia;

– second, to justify the demands of the military and political lobby for a four-time increase of NATO costs in Europe;

– the third is to discredit any political force both in Latvia and in Europe which take Russia impartially and act pragmatically towards it.'[29]

The above information is not a single provocation. Last fall (2015), the Norwegian television broadcasted the series 'Occupation' which depicted a similar hypothetical situation of the occupation of Norway by Russia 'to protect EU energy security'. The series caused the protests from some Russian politicians and the Russian Embassy in Norway. The Russian Embassy in Norway said that the authors of the series had decided in the

[28] From materials of Tula information consultation center regarding sect <http://olds-sektain.1gb.ru/08/sen6.htm> (accessed Feb. 10, 2016).

[29] Посол РФ в Латвии: Телешоу на BBC-2, моделирующее нападение на Латвию, демонизирует Россию [Posol RF v Latvii: Teleshou na BBC-2, modeliruyshchee napadenie na Latviu, demoniziruet Rossiyu [Embassador RF in Latvia: TV-shows on BBC-2, which is modeling aggression on Latvia, demonize Russia]], available at <http://www.rosbalt.ru/exussr/2016/02/04/1486561.html> (accessed Feb. 10, 2016).

worst traditions of the 'cold war' to intimidate the Norwegian TV-viewers with a 'threat' from the East, though actually there has never been any of the kind whatsoever. 'Although the authors of the series do their best to emphasize the fictional plot, allegedly, having nothing to do with reality, however, the film shows real countries, and, unfortunately, the role of the aggressor was assigned to Russia,' - the Embassy commented. [30]

The technology of the information and psychological attacks is worth mentioning here. Its first and foremost target is not the state but the population of the attacker. The aim is to disseminate anxiety and mistrust and to mobilize in the face of an external enemy. The result of such attack is a significant change of the public opinion of the attacker against the attacked. The victimized nation becomes the aggressor and no arguments can be admitted to justify it.

Core technologies of information warfare should be indicated. They include, in particular:

1. Information asymmetry, i.e. counter information or disinformation. The matter is that the denial or considerable decrease of importance or turning some positive enemy's information report into an insignificant one should follow each information item and, which is better, the greater amount of the news broadcasted. It is crucial to use the so-called 'information wave', i.e. when refutation is published with reference to an expert, some prominent politician and public figure, other famous person, publishing house, organization, etc. Other publications will reproduce the information in question mentioning the expert's comments. The third or fourth reprints of the information are sure to be indexed on behalf of this expert or politician and public figure or publishing house. It will take the attacker at least a couple of days to rebut and consequently, only a smaller part of the misinformation wave may be blocked.

2. Information superiority, i.e. functioning of mass media, public associations and political parties beyond the control of an enemy-state in its information realm. Mass media is said to be capable to redefine spirit using the information warfare technique.

The ability to form public opinion, not only within a country but also across boundaries, allows politicians to manipulate the population, for example, before the elections or other socially significant events, using popular discontent with the current public authority wishing in their turn to remain in its place. Manipulation methods are diverse and include statements on the facts of corruption of higher officials of the state or their cronies in mass media.

A case in point is 'Lisa's case'[31] that added to the political tension in Germany.[32] The fact of a possible rape of a Russian girl by migrants in the wake of events in

---

[30] By materials of BBC Russian Service, available at <http://www.bbc.com/russian/international/2016/02/160203_world_war_three_war_room_bbc> (accessed Feb. 10, 2016).

[31] Бедная Лиза [Bednaya Liza [Poor Liza]], available at <http://www.rg-rb.de/index.php?option=com_rg&task=item&id=17640&Itemid=13> (accessed Feb. 10, 2016).

[32] Нападения в Кельне: беззащитность и ярость немцев [Napadeniya v Kelne: bezzaschitnost' i yarost' nemtsev [Attacks in Cologne: helplessness and fury of the Germans]], available at <http://www.bbc.com/russian/international/2016/01/160110_germany_cologne_vulnerable> (accessed Feb. 10, 2016).

Cologne did not ease the removal of tension in German society. On the contrary, this incident augmented political problems for the German leadership. This and other facts of stuffing the information realm of foreign states with the views contrary to their generally accepted and acceptable public opinions resulted in Christopher Walker's statement. Christopher Walker, the Vice-President of National Endowment for Democracy (NED) said that 'the American and European media must be more proactive to oppose the Russian channels RT and Life News as well as other media from the countries that pose a threat to the United States.'[33]

The efforts of Russia concerning its dominance in the media have been successful. On the one hand, 'Russia Today' (RT) and 'LifeNews' are critically important means of mass media in a number of languages. Their influence has been acknowledged by foreign journalists. The Russian channels have been creative in their pursuit of competitive advantages over the pro-government foreign media in their own territory. According to Josh Kucera, a journalist, who covers the events in Russia and the former Soviet republics, RT talks about the US in the same way as the American media talk about Russia focusing on the negative trends and interviews with dissidents. In general, in the USA the RT Channel has taken up the niche similar to 'Democracy Now' or 'Al Jazeera', i.e. it highlights topics and opinions which contain too much criticism for them to get into Russian mainstream media. As Kevin Gosztola put it in his remarkable response to Assange's program: 'it is high time for the critics to accept the fact that, even though the channel is biased, some of its programs translate explicit and sometimes harsh but necessary criticism of our government, which can hardly ever be transmitted by the American channels.'[34]

On the other hand, as for the protection of the domestic Russian information space, it has been defined at the legislative level. At the end of 2014 Article 19.1 of the Federal Law 'On mass media' was amended to limit foreign capital to less than 20 percent in the total amount of the authorized capital. Previously, foreign investments were limited to 50 percent and it gave the foreign nationals ample opportunities to determine the principles and topics for press and TV-or radio channel. In addition, the practice of licensing broadcasting media companies and business enables the authorities to restrict the number of unwanted mass media without giving rise to claims about the freedom of media being infringed.

3. Information and legal domination implies the participation and the right to vote in as a large number of international organizations as possible to be able to respond quickly to the information challenges and to clarify one's own point of view to the international community.

---

[33] Cristopher Walker, *The Hijacking of 'Sofr Power'*, 27(1) J. of Democracy (2016) <http://www.ned.org/wp-content/uploads/2016/01/January-2016-JOD-Hijacking-of-Soft-Power-Christopher-Walker.pdf> (accessed Feb. 13, 2016).

[34] Гленн Гринуолд, Нападки на RT и Ассанжа многое говорят о самих критиках [Gleen Greenwald, Napadki na RT i Assanga mnogoe govoryat o samih kritikah [Gleen Greenwald, Abuse on RT and Assang say more about their critics]], available at <http://inosmi.ru/world/20120420/190851187.html> (accessed Feb. 13, 2016).

This is an extremely important element of the information warfare technology based primarily on its legitimacy and publicity. Costly participation and representation at most political and economic organizations and events, namely, the United Nations, the UN Security Council, the Parliamentary Assembly of the Council of Europe, the Shanghai Cooperation Organization, etc. eventually entail large expenditures but create a platform to comment and express opinions and views at the international level. With regard to Russia PACE restrictions, in fact, they are the methods of information warfare. If Russia had been given a chance to argue PACE on par on the situation with the Crimea and the associated events as well as the situation in Donbass, the Russian Federation would have been able to persuade or at least to explain its point of view on the political circumstances. The absence of Russia in PACE takes the information war against Russia to a new level since Russia can not defend itself and act on the information offensive. According to some experts, for Russia there is no need either for a membership or for a vote in PACE. We consider it fundamentally wrong because eventually Russia's non-participation entails a single point of view on current events. As a matter of fact, in the situation with PACE Russia has lost its information confrontation.

4. Latent technique of information warfare, i.e. secret and anonymous disposition of information and psychological influence. One can do it under the guise of someone else's banner from anywhere within the realm of cyberspace and on-line identity may not serve as proof of real world identity. Subsequently, it is strenuous to charge the country in question of deliberately carrying out counter-information activities.

The 'agents of influence' are commonly used for this purpose. They are introduced into the elements of the state and subsequently get certain powers to act on behalf of the government but in the interests of an attacker. Moreover, the use of coalitions creates the complexity of confrontation, which makes it difficult to blame any particular country for the attack.

5. The use of the lack of clear legal definitions in the international and national legal standards in order to unleash military aggression and damage the national interests of opponents in a peaceful environment. At present stage Russia is not adequately protected by domestic law concerning the qualification of information war, methods of counteraction and penalties for illegal activities. The amendment of the current Doctrine on information security or the finalization and adoption of the draft of a new doctrine amending the Criminal Code of the Russian Federation in terms of liability for the mediation or organization of information aggression are urgent to date. But it will be a mistake to be limited with the national legislation. It is necessary to propose appropriate and relevant changes into the fundamental international instruments of the United Nations (UN), Shanghai Cooperation Organization (SCO), Collective Security Treaty Organization (CSTO), Commonwealth of Independent States (CIS), etc. at the level of the President, the RF Government, the Ministry of Foreign Affairs to ensure international cooperation and harmonization of national legislations in matters of information war confrontation.

6. Combination of information-psychological warfare waged by a participant of a coalition with information-psychological struggle of the same member of the coalition against its other members to achieve certain private benefits, as a rule through bribery or promises of political and economic advantages before the rivals. Coalition is the most essential principle to unleash information war. Allies or 'agents of influence' in governmental bodies, under the 'guidance' of which joint information actions are carried out, produce sufficient conditions for successful operations of information warfare, propaganda, information sabotage, etc. To oppose a coalition to another coalition of one's own should be set up. In addition to it, a great number of national and foreign coalition media covering the possible largest area of the country should be instrumental for counter-propaganda. The above-mentioned situation in PACE with regard to Russia is the example of such coalition and the use of propaganda techniques. Initially the resolution on withdrawal of the Russian delegation and its deprivation of vote in PACE was not adopted unanimously. Several EU countries opposed to such measure. On the contrary, they insisted to give Russia more time to create discussion opportunities with it. However, Polish, English and a number of other delegations formed a coalition with the requirement to uphold the unity of the EU countries' views on the issue, persuading and applying other methods, mostly of economic nature and pressed the adoption of the resolution in question.

Similar cases of the formation of coalition forces to conduct information warfare must be taken into account in order to prevent or reduce their efficiency. Besides, counter-propaganda events should be implemented well in advance. The event of natural gas delivery from Russia to Genichesk, Ukraine in winter 2016 may serve a good example, purposely, widely highlighted in mass media.

7. Creation of the atmosphere of distrust, suspicion and antagonism in the information system of the state power and administration of an opponent state to destabilize it. To stymie public authorities in the attacked country is extremely difficult and as a rule, 'agents of influence' are used for this purpose. But their introduction is really a time consuming and challenging task. That is why international agreements are often used to exclude alternative ways for the state in a situation of information war but they are worded and signed on conditions unfavorable for the aggrieved party. As a rule, the attacked state is placed under international pressure to make it sign an obscure document to its own disadvantage as it will find out in future. In the final analysis, the reference to the document turns out to be an element (weapon) of information war. The attacker refers to it on a regular basis citing and pointing out that another party to the agreement has failed to fulfill the obligations. False information is often used to create the atmosphere of mistrust and hostility to all other proposals and options to address the obligations in question. The information coming from a knowledgeable person about an imminent change in the economic, political and social situation, however, is able to push the attacking party to take a wrong decision.

8. Information dependence of an enemy state from continuous streams of external or alternative information resources. Some countries have already made attempts

to monopolize information. Currently there is no state in the world depending exclusively on the information flow from the outside. Nevertheless, to make the state information-dependent is quite feasible. Typically, this is achieved by establishing a sufficiently large number of mass media in the country, advertising them on a mass scale, promoting them with lotteries, talk shows and thus, creating their images as being unbiased, true to facts and relevant. One of the similar methods to form the information dependence is to promote the studies of the culture and features of another state. The channels RT and LifeNews, which broadcast in the US and other countries, may serve good examples in this respect. Both RT and LifeNews speak of Russia, its political, economic, social and cultural life, thereby maintaining the interest of the citizens of these states to obtain information not from the government-run channels, which do not have such an information package. Another example was the fact of demonstrating the film Masks of revolution directed by Paul Moreira on the French channel Canal +. Since the public channels do not provide such information, the French have to seek for alternative information sources. Given the high rating and the fact that the citizens are really interested in alternative views, Canal + demonstrated this film several times. One can safely say, the lack of alternative opinions on formal channels and other information sources entails its search somewhere else.

9. Destabilization of the situation within the country (geopolitical entity) to impose an external crisis management. The most striking example is the practice of the so-called 'color revolutions' or any other destabilizing factor that makes the economic and political sovereignty of the state depend on the external control. Recent political events mentioned at the beginning of the paper have proved the established and common practice of such revolutions. Stable functioning of the elements of the state including military, police, economic and the last but not the least, it is worth mentioning that law-making can protect from such destabilizing factors and activities.

10. Information-psychological expansion. It means herein efforts to pursue national interests in a non-conflict penetration into the sphere of social and spiritual relations of society with the aim in a gradual, smooth and undetectable way to change the system of social relations along with the lines of the source of expansion. Another aim is to displace the foundation of national ideology and national values and substitute them with foreign values and ideology. The last but not the least is to increase the extent of its influence and presence and to establish control over strategic resources, information and telecommunication structures as well as national media, and step up propaganda efforts of its own media in the information field of the victimized state.[35]

11. Age-brainwashing by the media particularly means the use of television for corruption and change of consciousness of mostly children and adolescents, as a rule, being an insufficiently socialized segment of society. Films, cartoons, topic programs are aimed to reject everything domestic and traditional and to adopt alien

[35] Манойло А.В. Государственная информационная политика в особых условиях [Manoilo A.V. Gosudarstvennaya informatsionnaya politika v osobyh usloviyah [A.V. Manoilo, State information policy in special circumstances]] (Moscow, MEPHI 2003).

values often being the values of a foreign state. Some experts say that consciousness becomes something which may be down-loaded and fighting false information is only a part of the challenge;[36]

Modern television is a very effective means to form hypnotic passive TV-addiction of TV-viewers which contributes to a lasting consolidation of certain psychological attitudes. The nervous system (especially of children) is unable to withstand such an intense process of visual and mental perception. As a result, 15–20 minutes of watching TV is followed by a protective response in the form of a hypnotic brake condition which severely limits the perception and processing of information, on the one hand. On the other hand, it strengthens the processes of capturing and imprinting information but eases the programming of behavior.[37] The thing is that thousands of domestic and foreign films which contain scenes of violence, produce a continuous flow of malice and cruelty in mass media, movies, on TV / video / computer screens, not subjected to age restrictions. Scenes of violence often replace a good scenario since violence impacts and affects directly human sub consciousness causing negative feelings and emotions and giving no food for human mental faculties. Thus, the media gives the way for the degradation of the younger generation. The media impair the ability of adolescents and youth to perceive reality properly. Young people begin to live in a fictional world.[38] The Federal Service for Supervision of Communications, Information Technology and Mass Communications takes efforts to identify and block the information that could harm child's health and education.[39] Besides, it strives to license and control television and radio content as well as diffusion of information on the Internet. Essentially, these are some of the ways to confront expansion of pernicious and harmful information. To contravene information in cyberspace is the most complicated task because a significant part of the information resources providing harmful and subversive information are beyond the Russian jurisdiction. Nevertheless, it is necessary and feasible to technically block access to these resources and the Russian law allows doing it. Further, it is imperative to continue collaboration with international lawmakers to combat such information at the transnational level.

---

[36] Ловцов Д.А. *Канал 2х2: юмор, сарказм… экстремизм?* 11 Закон 28-29 (2008) [Lovtsov D.A. *Kanal 2x2: yumor, sarkazm… ekstremizm?* 11 *Zakon* 28–29 (2008) [D.A. Lovtsov, *Channel 2x2: humour, sarcasm… extremism?* 11 Statute 28–29 (2008)]].

[37] Гримак Л.П. Резервы человеческой психики [Grimak L.P. Rezervy chelovecheskoi psihiki [L.P. Grimak, Resources of human psyche]] 86 (Moscow 2010).

[38] Зелинский С.А. Тема 1. Глубинная психология масс (современные психотехнологии манипулирования [Zelinskii S.A. Tema 1. Glubinnaya psykhologia mass (sovremennye psikhotehnologii manipulirovania) [S.A. Zelinsky, Topic 1. Mass depth psychology (modern manipulative behavior psychotechnology)]], available at <http://psyfactor.org/lib/zln0.htm> (accessed Feb. 13, 2016).

[39] Федеральный закон № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" [Federal'nyi Zakon RF "O zashchite detei ot informatssii, prichinyayushchei vred ih zdorov'yu i razvitiy" [Federal Law of the Russian Federation On Protection of Children from Information Harmful to Their Health and Development]] eds. from 29.06.2015, Rossiiskaia Gazeta [Ros. Gaz.] Dec. 31, 2010.

In addition to the process of developing and bringing the Doctrine in accordance with the current state of domestic and international relations, it is critical to amend the provisions of the Criminal Code of the Russian Federation which determine the penalties for the use of information warfare technologies. The fact is that Russian law does not establish liability either for the activities like the use of information technology to counter (information warfare), or for the appeals to conduct such war itself. Taking this into account we consider it expedient to propose the appropriate changes in the Russian legislation, namely, to supplement the Criminal Code of the Russian Federation with Article 354.2 'Violation of the national sovereignty of the Russian Federation in the information sphere':

1. Calls to implement IT and computer-aided information war acts aimed to achieve the information superiority over the state but caused no harm to the national security of the Russian Federation in the information sphere or violation of the national sovereignty of the Russian Federation in the global information space shall be punished with a fine not exceeding one hundred thousand rubles or the salary or other income for the period of up to two years, or by community service for up to two years, or imprisonment for up to one year.

2. The same acts that caused harm to the national security of the Russian Federation in the information sphere and violation of the national sovereignty of the Russian Federation in the global information space shall be punished by a fine of up to five hundred thousand rubles or the salary or other income for a period of up to five years, or community service for up to four years, or imprisonment for a term from two up to three years.

3. Acts, stipulated by part 2 of this Article, committed with the use of mass media shall be punished by a fine of three hundred thousand to eight hundred thousand rubles or the salary or other income for a period of three to five years or community service for up to five years with disqualification to hold certain positions or engage in certain activities for up to four years or without it, or imprisonment for up to six years, with disqualification to hold certain positions or engage in certain activities for up to four years.

The said corpus delicti and liability correlate with the acts under Article 'Public calls to unleash aggressive war' in terms of gravity of the offense. This novelty in the Criminal Code of the Russian Federation will eliminate a gap in the legislation and set out the conditions for the proper classification of a criminal act. Finally, it will strengthen the security of the state and society in the most vulnerable field of information. In particular, the Program of the Russian military-historical society (RVIO)[40] emphasizes that ideology and young people's minds and sentiments are the most problematic elements of the state information policy. As a rule, failure and defeat in this segment will result in losses in many others, i.e. military, industrial,

[40] Российское военное общество [Rossiiskoye voennoe obshchestvo [Russian military society]], available at <http://histrf.ru/ru/rvio> (accessed Feb. 19, 2016).

scientific, engineering and social. However, the worst result of the defeat in question is the distortion and disappearance of patriotic ideas and 'brain drain'.

In the last decade the state-of the-art methods of rivalry between the states have changed and become latent concerning opposition in the information space. With the acceleration of globalization, information rivalry is more and more seen as the appropriate tool of influence on the international political arena. By focusing on its in-depth analysis it is essential to carefully define the definition of 'information war' in legal terms. To begin with, lawmakers should at the level of national law to establish responsibility to prevent and avoid information war against Russia. At the same time it is crucial to initiate appropriate changes in the fundamental international instruments, especially the Shanghai cooperation organization, the Organization of the collective security treaty, 'Agreement on cooperation of the Commonwealth of Independent States in the field of information security', the basic UN documents.

In conclusion, the problem of information warfare must be identified as a profoundly serious and damaging threat. The paper provides the characteristics of information warfare and methods to resist it as well as the proposals to amend the domestic legislation to create conditions for an accurate understanding of this political and legal phenomenon. In addition, it emphasizes the view point that the amendment of the Information Security Doctrine is not enough to counterbalance the threat of IW. In a certain document it is necessary to recount all notions, requirements and methods for the appropriate government actions to gradually change the situation. To maintain information sovereignty it is crucial to develop information security legislation, training specialists to be able to counter information-psychological aggression and to form public opinion through the media and to step up propaganda efforts, etc.

This article's aim is not to be exhaustive on the matter but to describe the general framework, analyze the core concepts and key distinctions which are sometimes confused and eventually widen our thought regarding relevant legal proficiency.

References

Arquilla J., Ronfeldt D. The Advent of Netwar 3, available at <http://www.rand.org/pubs/monograph_reports/MR789.html#toc>.

Rona T.P. Weapon Systems and Information War (Boeing Aerospace Co., Seattle, WA, 1976).

Sullivan J.L. Piereson James and Marcus, George E. *Political Tolerance and American Democracy,* 89(4) Am. J. of Soc. 963–966 (1984) <http://www.jstor.org/discover/10.2307/2779266?sid=21105059805761&uid=4&uid=2>.

Peffley M., Rohrschneider R. Democratization and Political Tolerance in Seventeen Countries: A Multi-level Model of Democratic Learning, available at <http://www.uky.edu/AS/PoliSci/Peffley/pdf/WVSPRQFinal_1-31-03_.pdf>.

Libicki M. Conquest in cyberspace. National security and information warfare (Cambridge 2007).

Libicki M. What is Information Warfare? (Washington DC, Institute for National Strategic Studies, 1996).

Manoilo A.V. State information policy in conditions of information-psychological war <http://psyfactor.org/lib/psywar25.htm>.

Manoilo A.V., State information policy in special circumstances (Moscow, MEPHI 2003).

Schwartau Winn, Information Warfare (New York, Thunder's Mouth Press 1996).

Singh Ajay, Information Warfare: Reshaping Traditional Perceptions gives this definition, available at <http://www.idsa-india.org/an-mar-4.html>.

Szafranski R. Neocortical warfare? The acme of skill (J. Arquilla, D. Ronfeldt eds., Santa Monica 1997).

Почепцов Г.Г. Информационная война: определения и базовые понятия [Pocheptsov G.G. Informatsionnaya voina: opredeleniya i bazovye ponyatia [G.G. Pocheptsov, Information war: definitions and basic concepts]], available at <http://psyfactor.org/psyops/infowar25.htm.> (accessed Nov. 25, 2015).

Information about the authors

Dmitry Shibaev (Vologda, Russia) – Associate Professor, Head of Department of Social Science, Humanities and Legal Computer Science of North-Western Institute (branch) of Kutafin Moscow State Law University (MSAL) (32 Mira str., 160001, Russia, Vologda; e-mail: 013600@inbox.ru).

Nina Uibo (Vologda, Russia) – Associate Professor of Department of Social Science, Humanities and Legal Computer Science of North-Western Institute (branch) of Kutafin Moscow State Law University (MSAL) (32 Mira str., 160001, Russia, Vologda; e-mail: 013600@inbox.ru).