STUDIA UNIVERSITATIS MOLDAVIAE, 2022, nr.11(01)
Seria "Științe economice și ale comunicării" ISSN 2587-4446 E-ISSN 2587-4454 p.129-135

CZU: 659.3:004.73(73 + 470) **DOI: https://doi.org/10.5281/zenodo.5816643**

A COMPARATIVE ANALYSIS OF INFORMATION WARFARE THEORIES IN THE US AND RUSSIA'S OFICIAL DOCUMENTS

Violeta STRATAN İLBASMIŞ

Turcia, Izmir

This paper discusses the Russian and American information warfare theory perspectives pointed out in these countries' official documents. In order to provide an exhaustive presentation of the theoretical differences, several official documents were consulted and the most relevant features were emphasised in the paper. The article argues that both approaches are in no way a new phenomenon. After underlining the essential theoretical concepts and related terminology, the article focuses on pointing out the main differences and similarities between these two countries' information warfare theories. The article concludes that both Information Warfare perspectives are continuously evolving and developing. Also, it should be mentioned that the USA documents are focusing more on the technical area of information warfare, whilst the Russian theory, in addition to technical dimension, emphasizes the information-psychological aspect of this concept as well.

Keywords: *information warfare, USA, Russia, information strategy, information dominance, mass media, information security, modern conflicts, propaganda.*

O ANALIZĂ COMPARATIVĂ A TEORIEI RĂZBOIULUI INFORMAȚIONAL ÎN DOCUMENTELE OFICIALE ALE SUA ŞI RUSIEI

În acest articol sunt analizate teoriile războiului informațional din perspectivă americană și rusă, teorii care se regăsesc în documentele oficiale ale acestor două țări. Pentru a oferi o prezentare exhaustivă a diferențelor teoretice ale acestor teorii, au fost analizate surse oficiale și cele mai importante aspecte au fost accentuate în acest articol. Se menționează că ambele perspective, atât cea rusă, cât și cea americană, nu reprezintă un fenomen nou. După ce au fost subliniate conceptele teoretice esențiale și explicată terminologia aferentă, în articol sunt prezentate principalele diferențe și afinități dintre teoriile propuse de aceste două țări. Autorul conchide că ambele teorii sunt în continuă evoluție și dezvoltare. De asemenea, trebuie de menționat că documentele părții americane se concentrează mai mult pe dimensiunea tehnică a conceptului de război informațional, în timp ce teoria rusească, pe lângă dimensiunea tehnică, pune un mare accent pe dimensiunea informațional-psihologică a acestui concept.

Cuvinte-cheie: *război informațional, SUA, Rusia, strategie informațională, dominare informațională, mass media, securitate informațională, conflicte moderne, propagandă.*

In 21st Century, the world balance of forces between the United States and Russia has been changed due to the emergence of frequent dissensions between these two countries. The diplomatic debates and peace treaties signed immediately after global conflagrations like World Wars I/II and Cold War were not able to settle down the state of affairs in Europe or on other continents. The eagerness or simply geopolitical interests of global players gave birth to new disputed territorial problems. So, to speak, modern times brought up new threats to the global balance of power and collective security. Both Russia and U.S. are incontestable geopolitical actors and most of the times their sphere of influence intertwines. The recently emerged Ukrainian crisis is just an example in this sense. Immediately after the collapse of the Soviet Union, Russia was in a weak position, firstly economically, ideologically and socially and for many years in a row, it was characterised by a lethargic and apathetic spirit. While the West was flourishing from many perspectives, Russia was still in the search of its own identity. Once NATO and European Union started to get closer to Russia's borders and to spread their influence towards ex-soviet countries, Russia has changed its foreign policy strategies and tactics, focusing mainly on information warfare strategies. In 2014, European Union and Ukraine signed the Association Agreement and Russia was forced to react in a way. European Union's offer to Ukraine was the reason of Ukrainian turmoil (that is still going on), in which global powers engaged to play different roles (enemies or friends, the peacemaker, the mediator, the aggressor etc.).

Over the past 10 years, both Russia and United States have developed their own concepts of information warfare. Due to the fact, that most of the media outlets, but also academic sources are focusing their views and studies mainly on Russia's information warfare by making out of it the main culprit of regional destabili-

sations and turmoils (like the one from Ukraine), the author of this article considered appropriate to outline the differences and similarities of information warfare theories both in the US and Russia's official documents. Only by comparing these two geopolitical actors' information warfare theories, the tstrengths and weaknesses of these theories could be highlighted.

Information warfare has as objective to create a favourable political, cultural, and psychological information environment through distortion of reality for the purpose of attaining specific political goals. Information warfare enforcement helps to position geopolitically each of these two countries and the success depends on how well and how much these countries are involved in this process. The literature consulted in this sense helped to identify the answers to these questions: why information warfare is important to analyse from a scientific perspective and why it is so important the study of information warfare concept. It opens new ways to conduct political and military operations. Also, because we live in the era of active information development where the increasing role of information and knowledge is hard to deny. Information warfare is not a new concept by any means, but the novelty is that it is being conducted in new ways via new channels.

General characteristics of information warfare. A note on terminology

Although the term "information warfare" (IW) is not a new one, it is still shrouded in controversy, but it is widely used in today's news. Thomas N. Rona reportedly coined the term "information warfare" in 1976 in a report delivered to Boeing Company, titled "*Weapon systems and Information Warfare*" offering the following definition: "*The strategic operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives* [1]." Since then, many definitions emphasized its military dimension [2-5]. However many definitions stressed its psychological aspects or in other words, the effect it can have on people and their behaviour. For a long time, the term "information warfare" did not even have a precise definition, maybe that is why often, it is misinterpreted and points to high-tech weapons which are used in mass armies.

In its largest sense information warfare is a concept indicating the use and management of information and information technologies in order to obtain a competitive advantage over an opponent. In the military treaty of Sun Tzu *"Art of war"* it is mentioned that information plays a crucial role in the victory over your enemy and it is considered to be a tool of "soft power". Winning a war might mean more information, but it definitely does mean better information [6]. Specifically, we talk about information warfare as a range of "*actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary*" [7, p.8-14]. This group of techniques could be used as well to spread propaganda, disinformation or misinformation, to manipulate the adversary, consequently information warfare is closely linked to psychological warfare. In terms of information-psychological warfare, the goal of the information is "*to control or shape the behaviour of enemy organisms, but without destroying the organisms. (...) regulating, the consciousness, perceptions and will of the adversary's leadership: the enemy's neocortical system*" [8, p.41-55] – in other words, it is known as neocortical warfare. Being mentioned and used for the first time in the United States of America it gained a more technological and militaristic feature. Some researchers have stated that information warfare is not a term with a single meaning, but it is rather an umbrella term with several distinct forms of warfare: electronic warfare, psychological warfare, economic information warfare or cyber warfare. Whilst American scholars tend to use it in such linguistic constructions, Russian scholars, when using the concept of information warfare are focusing more on its human dimension.

Conventionally, it is considered that the first information warfare was the First Gulf War in 1991, when İraqi coalition forces entered Kuwait. Rabinovitz and Jeffords called the First Gulf War a "media event" when American media were "*reconstructing history, controlling the dissemination of information, creating social consensus, and solidifying national identity*" [9, p.1-17].

Speaking about mass-media in this context, it is important to stress out that traditional media is still playing an enormous role in defining the 21st century war. Speaking particularly about television, it was undoubtedly the best invention used strategically and gaining constantly importance and influence in 1920 – 1930s. Visual information spread by television has become an important weapon in the information war conducted by international actors. What is important to mention is that nowadays media products are collected, processed and disseminated through electronic means (new media) which amplifies the meaning and the importance of

information warfare as a paradigm. Mass media is believed to be an important factor in the formation of a country's foreign policy. Media plays an important role in shaping international or national public opinion. Mass media has become a tool for national governments, with the help of media politicians or governments are waging wars against their enemies and by applying efficiently propaganda techniques, manipulation, misinformation or disinformation, demonization of the enemy, oversimplification and the substitution of facts with opinions, they are winning these battles.

Information warfare in Russian official documents

Information Security Doctrine of the Russian Federation (2000) was officially published only 125 days after the first inauguration of Putin as the president of the Russian Federation. This suggests the importance that information has and the priority given to it in terms of Russia's security issues. One of the most important intentions of the Russian government specified in the doctrine was to develop the Russian information services industry and use the government information sources in order to offer to international public trustworthy information from Russia's perspective. The emergence of Russia Today news channel was one of the results of the intentions mentioned above [10]. In February 2010, the Russian Federation adopted a **Military Doctrine** reminding that one of the features of modern military conflicts is "*the intensification of the role of information warfare*". One of the reforms mentioned in the text is the development of "forces and resources for information warfare", and one of the goals of the information warfare is to "achieve political goals without the utilization of military force and, in the interest of shaping a favoured response from the world community to the use of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force" [11].

Another document that specifies the essence of the global information war is the "**National Security Strategy of the Russian Federation**" published in 2010. In this official document, as well, information is considered to be a weapon or tool in the struggle for political supremacy in the world, and in the context of international conflicts that do not cease: "Global information struggle will intensify, threats will increase to the stability of the industrialised and developing countries, their socio-economic development and democratic institutions" [12]. Also, in this official document, are specified what are both internal and external dangers for Russia. Mainly, NATO's activity is seen as a potential danger, because of the failure of the current global and regional architecture, oriented only towards NATO [13]. The anti-ballistic missile defence system from Poland, Romania, Czech Republic, the breakaway regions of South Ossetia and Abkhazia and "Five-day war„ are just a few of the factors that led to a resetting of relations between Russia and the North Atlantic Alliance, but also to a re-writing of official Russian documents. Like the other documents mentioned above, the **Military Doctrine of the Russian Federation** published in December 2014 emphasizes the importance of information in the context of military conflicts and its presence in Russia's defensive strategy. Unlike the other official documents mentioned above, this doctrine divides the security threats into two groups: "dangers" (*opasnost*) and "threats" (*ugroza*). According to this classification, danger is not a threat, but it can gradually become a threat [14]. In the same vein, the Military Doctrine of Russia published in 2014 is more ideologized than the one published in 2010, because the document specifies the danger of an informational warfare that can affect the young Russian generation and can become vulnerable to external influences: „the activities of information influence on population, especially young citizens of the country, which has to undermine the historical, spiritual and patriotic traditions in defence of the Fatherland" [15].

One of the most recent and more updated official documents, the **Russian Federation's Foreign Policy Concept 2016** regarding information warfare, is specifying that one of the aims is to provide unbiased information to the world community from a Russian perspective on the most important international issues. Also, the promotion of the Russian media and Russian-language media on the international level through new communication technology stands as a task for the Russian government [16].

As a conclusion it can be stated that the quintessence of Russian information warfare theory is based on a proportional combination of media, psychological, economic, political and cultural resources. At the same time, if to make a comparison, in the documents analysed above the term "information security" (*informatsionaya bezopasnosti*) is often mentioned, which suggests its central role in the context of the informational warfare.

Information warfare theory according to Russian experts

Modern military conflicts are no longer the way they once used to be. Everything changes, including the concept of war, that is no longer the same. An important name in Russia's military and academic environment

is that of General Valery Gerasimov. In the work "*The Value of Science is in Foresight*" Gerasimov emphasizes the importance of information in the context of modern conflicts, pointing out that "in the 21st century we are witnessing the erosion of the boundaries between war and peace. The role of non-military means to achieve political and strategic goals has increased and, in many cases, they have overcome weapons in terms of efficiency" [17, p.1-3]. He is also mentioning that modern means of struggle are economic, political, informational or humanitarian. The military means are only additional to those mentioned above, so they are not always given priority, this being the great difference between the conflicts of the twentieth century and those of the 21st century. At the same time, the development of information technologies and their use in all areas, including the military, eventually led to the temporal and spatial "resizing" of modern conflicts. Similar to Gerasimov, Pavel Antonovich is stressing that "in the Russian construct, information warfare is not an activity limited to wartime. It is not even limited to the "initial phase of the conflict" before hostilities begin, which includes information preparations of the battle space" [18].

Among the most eloquent names that have familiarised the Russian public with the term of information warfare are Aleksandr Dugin and Igor Panarin. Both are representatives of the Russian geopolitical school, leaders and experts, ideologists and theorists of the concept of information warfare. The philosopher Aleksandr Dugin, one of the prominent ideologists of the Russian nationalism, an ex-KGB officer, professor of philosophy, political sciences, geopolitics at Lomonosov Moscow State University is the one that has introduced the terms "netwar", "net-centric warfare", (*setevoe voennoe iskustvo*) and "Eurasian Network" in the Russian academic realm. The net-centric warfare can be carried out both in wartime and in peacetime, against friends or allies, as well as against enemies. Several geopolitical factors have triggered the launch of these notions in the Russian academic environment by Moscow ideologues. Dugin, like other Russian theorists, supports the idea that colour revolutions have been successfully directed and implemented by the US applying the principles of a netwar or net-centric war. This involves the extensive use of computers and other computerised machines in full cooperation with the army's working strategies. Moreover, Aleksandr Dugin believes that in this international geopolitical struggle, the US-guided Western states have used impeccably all the information arsenals held by these states. Besides the well-established online information strategies, the political and social influence was also activated by the cultural component of the Western states. For example, Dugin stated that about the Rose Revolution in Georgia (2003), the Orange Revolution in Ukraine (2004), the Tulip Revolution in Kyrgyzstan (2005), the Jasmine Revolution in Tunisia (2010), the Grape Revolution or Twitter revolution from Moldova, were a success for the United States, but have been seen by Russia as a direct threat to the security of former Soviet countries and as an intrusion into the internal affairs of the North African or Arab States. In the same vein, these revolutionary movements were interpreted by the Russian authorities as a new form of war, more subtle, sophisticated and hard to perceive [19].

Igor Panarin is another resonant name of the Russian theory of the informational warfare. Panarin unlike Dugin offers a shorter and clearer definition of this type of war, by saying that: "Information warfare of the 21st century is a way of organising the noosphere and the world information space in your own interests and purposes" [20, p.2].

Georgii Pocheptsov is a professor, specialist in communications technologies, informational warfare, marketing and a reputable Ukrainian journalist. Despite the fact that he is a Ukrainian expert on information warfare topic, it has been decided to mention and analyse his view on this topic in the chapter "Information Warfare in the Concept of Russian Experts". According to Pocheptsov, the informational war is based on two components, on the one hand the computers and on the other one the mass consciousness and the individual consciousness [21, p.56]. Pocheptsov is the author of several important books on informational and psychological wars, that offer the reader a valuable insight into strategic and futuristic information theories.

Sergei P.Rastorguev is one of the most prominent Russian researchers of the information warfare problem, whose works are pretty unknown in the West for the simple reason that most of them have not been translated so far. His most important book is Information Warfare (*Informatsionnaya voina*) in which the author makes a more theoretical and philosophical insight into the study of the informational warfare, launching the idea that people are like computers, may have "viruses" in the information system (referring to the people's thinking process). Rastorguev defines information warfare: "as open and covert targeted informational impact of information systems on each other in order to get certain gains in the material sphere" [22, p.35-37].

The US information warfare theory

The information warfare issue has been always on US agenda, because being informationally dominant has been always the US's aim. The US informational dominance and superiority comprises the continuously developing information technologies sector, mass media, culture and a fast-growing economy. According to the US sources, information warfare theory refers to computer attacks and operational information, so it has a more technological and military character rather than psychological. For example, according to the **US Department of Defence** definition from 1995, information warfare represents a multitude of "actions taken to preserve the integrity of one's own information system from exploitation, corruption, or disruption, while at the same time exploiting, corrupting, or destroying an adversary's information system and (in) the process achieving an information advantage in the application of force" [23, p.20]. American theory of information warfare is part of the concept of "information dominance" and "information superiority", which through its defensive and offensive actions aims at gaining an informational advantage in all fields: political, economic, social, military, cultural etc. In the **US National Security Strategy** of 2015, it is not mentioned only the mere fact of having the informational supremacy in the world, but also the methods -/- strategies that must be applied to obtain and hold that supremacy. These include: lead with purpose, lead with strength, lead by example, lead with capable partners, lead with a long-term perspective strategy. This strategy also mentions the main dangers against which the US will have to fight, and the first "danger" the document refers to is the Russian aggression, after comes the fight against ISIL, Ebola, nuclear weapons, global warming [24].

As we can see, the official documents of both Russia and the US, refer to the main dangers that threaten the security of both countries. Thus, each country mentions the name of the other country as a real danger not only for its own security but also for the international common security. Americans have always associated the psychological information warfare (the humanised part of the information warfare) with psychological operations (PSYOPS) or propaganda. Since these terms have a negative tinge, Americans have refrained from using these terms in their official sources. One reason could be to exclude an association with the Soviet Union and its totalitarian regime, especially during the Cold War, renowned for many other things, but primarily for the propaganda machinery and world renown in this respect. Avoiding the use of such terms as propaganda, manipulation, PSYOP, psychological warfare was possible with the development of information technologies since the 1980s and the emergence of cyberwar, netwar, cyber-attack terms etc. According to the American researcher Nancy Snow, Americans are good specialists in masking what they really do to spread propagandist messages. By using euphemisms such as: "Public Diplomacy", "Atoms of Peace", "Public Information", "Public Communication" or "Strategic Communication", Americans are trying to mask the activity of various state and media structures, fact vehemently criticized by the author [25].

Information warfare in the concepts of American experts

We mentioned above the difference between American and Russian perspectives on information warfare by stressing the more human-related approach of the Russian compared to the American one, more technological or militarist. Accordingly, the definitions both sides are dealing with are different. For example, in the US there are still numerous definitions that researchers are operating with. Some of them are even replacing the term "information warfare" with: information-age warfare, information operations, cyberwar, net war, knowledge warfare or knowledge-based warfare. Yulin G. Whitehead specifies that within the American Department of Defence (DOD) there are no fewer than 27 definitions of information warfare [26, p.4].

In addition to the definitions mentioned in the official **US Department of Defence** documents, many other researchers or field specialists have provided their own interpretations of the concept of information warfare. For example, George Stein in his article "Information Warfare" succinctly states that "information warfare is nothing more than a way to achieve national goals through information" [27, p.31-39]. Winn Schwartau notes that the informational war in the post-modern era has a tremendous power of manifestation and representation. Using the opportunities of classical media and the Internet, it can achieve its real-time goals and live through "breaking news" the media are increasingly operating with [28].

Another author defining the concept of "information warfare" from a less technologically advanced perspective is Richard Szafranski, who, in his studies uses the concept of "neocortical warfare"; on the grounds that, according to the author, the main purpose of the information war is to influence the conscience, the perceptions and will of the opponent. Szafranski is one of the few American authors who has emphasized the

psychological dimension in a conflict, underlining that knowing the set of values and principles with which the opponent's brains operate is more important than the size of his physical and technological systems. In author's opinion, the term "information warfare" is often misinterpreted. Most often and in most sources the term "information warfare" is mentioned in the context of Command-and-Control Warfare (C2W), so to say, direct action or attack on opponent's computerized systems. He emphasizes the idea that the concept of "information warfare" is much wider, including the psychological operations against the opponent [29, p.42].

John Arquilla and David Ronfeldt, American specialists in international relations, in their works on the issue of information warfare, have launched the terms "network warfare" and "cyberwar", proposing their extensive use in scientific work. They mention that the term "information warfare"; is too broad, so, sometimes, it can create confusion and it can be mistaken. Network warfare and cyberwar are types of modern wars, and they are also concepts with a much narrower meaning. For instance, according to these authors, cyber warfare is a conflict of high and medium intensity and network warfare is a conflict of low intensity [30]. These features are very easy to understand, and the existence of confusion in the perception or application process is almost minimal. Both these notions are a logical result of the informational revolution and the informational era which we live in, and with the technological boom, the existence and frequency of such wars is steadily increasing.

In the digital age, the question that the USA is still putting is how to counter Russian informational negative flows, disinformation (*dezinformatsiya*) and manipulation, where lies are much easier to produce and disseminate. The same question is asked by the Russian political technologists, how to counter American disinformation. Both parties (although hardly admitting it) are engaged in an information warfare, where all possible and available resources and channels are used in order to counter or defeat the enemy's informational strategies.

Conclusions

The notable difference between the Russian and American information warfare definitions is that while the Russian doctrine, apart from focusing on the hard component of information, it focuses also on its human component, in other words, it refers to the exercise of the Russian influence on the political, social or economic system of a state, as well as the destabilisation of a society through psychological campaigns, the aim being to take decisions in favour of Russia. The Russian theory is in contradiction with the American theory of cyberattacks or cyberwar, which puts more emphasis on the use of computerised techniques in cybernetic activities. However, unlike the American one, the Russian information war theory with all its components has experienced only a slight relocation or repositioning of manoeuvre and activity space, focusing even more on the human-psychological dimension, that is to say, to influence and manipulate the target audience by means of well-thought-out and effectively applied psychological methods and actions. Unlike the Russian theory of the information warfare: "the Western understanding of information warfare can be defined as tactical information operations carried out during hostilities to deceive adversary and indirectly influence its decision-making and the actions to follow based on this decision-making process,, [31, p.10]. – So, if the Russians apply the intelligence strategies both in peacetime and war continuously, Americans focus more on wartime in the case of certain hostilities. The rise and development of technological devices and software allow Russia to update its old Soviet tactics and the US to improve its informational strategies in order to maintain the "informational superiority". In this "invisible war" (a term being used by more and more academics), having a proactive approach is indispensable for both countries in order to be informationally dominant.

References:

1. RONA, T.P. *Weapon Systems and Information War*. Boeing Aerospace Co., Seattle, WA, 1976.
2. de LANDA, M. *War in the age of intelligent machines*. New York: Swerve Press, 1991.
3. LIBICKI, M.C. *What is information warfare?* Washington, DC: National Defence University, Institute for National Strategic Studies, 1995.
4. SCHWARTAU, W. *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*. 2nd ed. New York: Thunder's Mouth Press, 1996, s.27–42.
5. DENNING, D.E. *Information warfare and security*. Reading, MS: Addison-Wesley, 1999.
6. Sun Tzu. *On the Art of War*, in Lionel Giles trans. and Brig. Gen. T.R. Phillips ed., Roots of Strategy, Mechanicsburg, PA: Stackpole Books, 1985.

7. ALGER, J.I. Introduction. In: *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age.* Ed. W. Schwartau. 2nd ed. New York: Thunder's Mouth Press, 1996, s.8–14.
8. SZAFRANSKI, R. *Neo-cortical warfare: The acme of skill?* Military Review, November 1994, p.41–55.
9. RABINOVITZ, L., JEFFORDS, S. *Seeing through the media: the Persian Gulf War*. New Brunswick, NJ: Rutgers University Press, 1994, p.1-17
10. Information Security Doctrine of the Russian Federation (2000). Retrieved from: https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf
11. The Military Doctrine of the Russian Federation, Retrieved from: http://carnegieendowment.org/files/2010russia_military_doctrine.pdf
12. Strategya Natsionalynoi Bezopasnosti Rosiiskoi Federatsii do 2020 goda, Paragraph 10. Retrieved from: http://kremlin.ru/supplement/424
13. Strategya Natsionalynoi Bezopasnosti Rosiiskoi Federatsii do 2020 goda, Paragraph 8. Retrieved from: http://kremlin.ru/supplement/424
14. Strategya Natsionalynoi Bezopasnosti Rosiiskoi Federatsii do 2020 goda. Retrieved from: http://kremlin.ru/supplement/424
15. Foreign Policy Concept of the Russian Federation (approved by President of the Russian Federation Vladimir Putin on November 30, 2016). Retrieved from: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248
16. Military Doctrine of the Russian Federation, Article 13. Retrieved from: https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf
17. ANTONOVICH, P. Cyberwarfare: Nature and Content, Military Thought, 2011, no.3, vol.20, p.35-43. In: Keir Giles. *Handbook of Russian Information Warfare*. NATO Defence College, 2016, p.4. Retrieved from: https://krypt3ia.fles.wordpress.com/2016/12/fm_9.pdf
18. GERASIMOV, V.V. *Tsennost nauki v predvidenii* [The value of science in forecasting]. Voenno-Promyshlennyi Kurer, Febryary 27, 2013. Retrieved from: https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf
19. "Little Green Men": a primer on Modern Russian Informational Warfare, Ukraine 2013-2014. Published by: The United States Army Special Operations Command Fort Bragg, North Carolina. Retrieved from: http://www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf
20. PANARIN, I. *SMI, propaganda I informationnaie voini*. Moskva: Pokolenye, 2012, p.2.
21. POCHEPTSOV, G.G. *Psihologiceskiye voini*. Moskva: "Refl-buk", 2000, p.56.
22. RASTORGUEV, S.P. *Informatsionnaya voina*. Moscow: Radio i Svyaz, 1999, p.35- 37.
23. WALTZ, E. *Information Warfare: Principles and Operations*. Boston; Artech House, 1998, p.20.
24. National Security Strategy 2015 – National Security Strategy Wash. The White House. February 2015. Retrieved from: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf
25. SNOW, N. *American Propaganda. We need more study, not less*. Retrieved from: https://www.academia.edu/14855646/American_Propaganda_We_Need_More_Study_Not_Less
26. WHITEHEAD, Y.G. *Information as a Weapon: Reality versus Promises*, 1998, p.4.
27. STEIN, G.J. *Information warfare*, Airpower Journal, Spring 1995, p.31-39.
28. SCHWARTAU, W. *Chaos on the Electronic Superhighway: Information Warfare*. New York: Thunder's Mouth Press; Emeryville, CA: Distributed by Publishers Group West, 1994
29. SZAFRANSKI, R. *Neocortical Warfare: The Acme of Skill*. Military review, November 1994, p.42.
30. ARQUILLA, J., RONFELDT D. *The advent of netwar*. The RAND Corporation, 1996. Retrieved from: http://www.rand.org/pubs/monograph_reports/MR789.html
31. ČIŽIK, T. *Information Warfare. New security challenge for Europe*. CENAA Policy Papers. Bratislava, 2017, p.10.

Date about author:
Violeta STRATAN İLBASMIŞ, PhD in Journalism, Turkey, Izmir.
E-mail: violetastratan@gmail.com
ORCID: 0000-0002-0456-7413

Prezentat la 19.11.2021