Information influence of the russian federation on the network environment of Ukraine

Oleksandr Leonov [*A]; Karina Rubel [A]

[*]**Corresponding author:** PhD student, e-mail: 578original@gmail.com, ORCID: 0000-0003-1759-3845
[A] Military-Diplomatic Academy named after Yevgeny Bereznyak, Kyiv, Ukraine

Received: November 22, 2020 | Revised: December 12, 2020 | Accepted: December 31, 2020

DOI: 10.5281/zenodo.4395143

Abstract

The informational influence of the Russian Federation on the network environment of Ukraine and other countries of the world has been analyzed. Emphasis has been placed on the use of non-military means as a powerful tool for destabilization of society and the information component of Ukraine's opposition to the Russian Federation has been considered.

Key words: information, technologies, security, network environment, hybrid war.

Introduction

The armed conflict in Donbass, which has been going on for six years now, is accompanied not only by violence but also fierce information confrontation. Under conditions of confrontation with Russia, the Ukrainian state has become the target of a hybrid war, in which fundamentally different types and methods of warfare are combined and coordinated. Typical components of a hybrid war are the use of classical methods of war involving manpower and military equipment; irregular armed groups (insurgents, terrorists, guerrillas, etc.); means and methods of information and cyber wars (Manuilov Y.M., Prudnikova O.V., 2017).

The rapid development of information technology has led to a surge in the social activity of Internet users, in which more and more conscientious people are becoming involved. Aware of the growing influence of the network environment on public opinion, governments around the world and the structures under their control use a wide range of modern media to widespread certain information: the newest portals, blogs, social networks, messengers etc. All these tools are successfully used by the Russian Federation.

As part of the anti-Ukrainian information campaign, the leadership of the Russian Federation is making efforts to strengthen the ideological, informational, psychological and propaganda influence on the population of Ukraine and the occupied territories. In the international arena, the main goal of Russian propaganda is to convince the European and Ukrainian target audience that the Russian Federation is not a party of the conflict in Donbass, but only a mediator.

The information impact on the network environment is the subject of many recent studies. Y. Derkachenko (Derkachenko Y.A., 2016) considered the issue of manipulative influence through social networks, K. Kotsurba (Kotsurba K.O., 2014) determined the place and role of modern information and communication technologies in the formation and development of civil protest movements, Y. Nesteryak (Nesteryak Y.V., 2013) analyzed the international criteria of information security. However, the problem of informational influence of the Russian Federation on the network environment has not been sufficiently studied.

Material and methods

The purpose of the article is to analyze the consequences of the information impact of the Russian Federation on the network environment, to consider measures to counter the information impact in the advanced countries of the world.

Such scientific methods as observation, analysis, synthesis, generalization were used in the work.

Results and discussion

1. The intensive development of science and technology has reached such the level where new communication technologies can multiply the destructive information impact on large groups of people (Derkachenko Y.A., 2016). In particular, in order to achieve economic, political and other benefits, the Russian Federation is actively using technologies to artificially change human behavior and influence the free expression of human will, as well as a wide range of means: from social media resources to classical methods of influencing public opinion and make decisions. The role of the media (or the organizational structures to which they are subordinated) is mainly to provide or create a kind of information infrastructure for conveying the necessary messages produced by specially trained individuals (so-called agents of influence). An example is the provision of TV airtime for representatives of Ukraine who are loyal to the Russian federation, the creation of Internet sites in other countries, financial or other support for agents for their use of public media resources – Facebook, YouTube, etc (Dubov D.V., Koretska I.O., 2018). As you can see, the network environment is an effective platform for widespreading of advatageous information.

In his research, O. Senchenko gives a transformed concept of network (Senchenko O.M., 2017). The network is a new information space in which the major strategic military operations are deployed, and their media, diplomatic, economic and technical support is provided. A network is any environment,with the help of one the necessary information can be activated, transmitted, received, and conducted. A qualitative, well-established network is the one that reproduces the required intended action in the context of the overall strategy.

According to the Law of Ukraine “The Basic Principles of Cybersecurity”, a network environment that provides opportunities for public relations, formed as a result of the functioning of compatible communication systems using the Internet, is interpreted as cyberspace (On the basic principles).

Cyberspace provides much of the world's population with access to information transforming the human mindset. The openness of the Internet has created new threats to national and international security. The number and power of cyberattacks motivated by the interests of particular states, groups and individuals is growing.

Prerequisites for the emergence of concepts such as cybersecurity and cyber espionage are not only an increase in the number of cases of illegal interference into personal systems, the interception of information by criminal structures and terrorist organizations, but also the systemic, targeted influence of state or quasi-state structures on critical infrastructure, elections or even constitutional order (Diordica I.V., 2017).

As we can see, the Internet has become an important platform for information confrontation. Special units that conduct special psychological operations on social networks and the Internet in general are becoming a key element of cyberspace confrontation (Gorbulin V.).

Evidence of the critically dangerous nature of these technologies was Russia’s actual seizure of the information space of the Crimea, eastern and southern Ukraine during 2013-2014, which created the preconditions for Russia’s occupation of the Crimean peninsula and the organization of armed conflict in Donetsk and Luhansk regions. Today, Russia’s purposeful

activities in cyberspace provoke tensions in other regions of Ukraine, allow to maintain anti-Ukrainian sentiment among the Russian population, discredit Ukraine and justify its policy in the EU (Radkovets Y.I., 2014).

The Russian Federation's interference in Europe's democratic processes has become systemic in nature and has already led to the rise in popularity of far-right and openly pro-Russian political forces in Europe, which is a threat to the unity of the European Union. Thus, in January-October 2019, the "East Stratcom" Strategic Communications Unit recorded about a thousand cases of pro-Kremlin disinformation, which is more than twice the same in 2018. It is assumed that in the future Russia will increase the capacity of its own media to conduct a disinformation campaign against the EU and some neighboring countries, including Ukraine (Derkachenko Y.A., 2016).

Russia's intervention in the 2016 US presidential election should not be forgotten. On the one hand, highly skilled hackers made great efforts to hack Democrats' accounts and mailboxes, and on the other, the entire network of agents worked to spread and cover the stolen data at the right angle. For this purpose, all social networks and media platforms were used, taking into account the interests of voters.

As we can see, in modern conditions of informatization the expansion of spheres of influence is carried out mainly by non-military means. K.O. Kotsyuruba mentions the so-called strategy of indirect action, the essence of which is a comprehensive impact aimed at destabilizing society from within (Kotsurba K.O., 2014). The Internet, the press, television – are all the areas of influence on the consciousness of the population. For example, social networks in the process of their development are not only a means of communication, they are used as a powerful tool to unite people for a specific purpose. It is the information and network technologies that determine the dominant opinion and create certain stereotypes among the population. Thus, the media can manipulate public opinion.

These facts suggest that although the military component of the conflict between Russia and Ukraine objectively remains the main factor in its deployment, the use of the information component is becoming increasingly widespread.

2. The constant influence of the Russian Federation on the consciousness of the population through network resources is the main threat to Ukraine in the context of cybersecurity. About the manipulative influence that Russia is exerting against Ukraine in the online environment, Philip Breedlove, the former Supreme Commander-in-Chief of the United NATO Armed Forces in Europe, said: "This is the most amazing information blitzkrieg we have ever seen in the history of information wars" (Gorbulin V.). Therefore, there is a need to strengthen the information security at the state level.

Nesterjak Y.V. has identified two main approaches to the study of international criteria of information security: technical-technological and humanitarian (Nesteryak Y.V., 2013). The first approach to the international criteria of information security can include protection of information resources from unauthorized access to ensure confidentiality, protection of the integrity of information resources from unauthorized modification or destruction, ensuring the efficiency of systems by means of counteracting threats of denial of service.

Based on the principles of humanitarian approach, information security should be considered as the protection of personal information and information systems, counteracting the negative impact on human consciousness through the media, protection of information resources and people's knowledge of themselves and the world around them, countering propaganda and psychological campaigns, cultural and political subversion. Despite the fact that the information component of the confrontation between Ukraine and Russia is changing both quantitatively and qualitatively, it is necessary to comprehensively strengthen information security by consolidating legislative, organizational and technical means. In addition, the experience of advanced countries in the world in establishing cybersecurity systems

should be taken into account.

Thus, considering the high risks of disinformation and foreign interference in democratic processes in Europe and the United States, Brussels and Washington are planning to strengthen measures to counter Russia's information influence (Derkachenko Y.A., 2016). EU governing bodies envisage focusing on four key areas:

raising the level of awareness of EU citizens about the disinformation campaign conducted by the Russian Federation. For this reason, the website www.euvsdisinfo.eu, created as part of the response to pro-Kremlin disinformation, has been updated. In addition, the EU plans to allocate more than € 4 million to support the media on the freedom of investigative journalism;

reforming the strategic communications unit "East StratCom" and increasing its funding;

developing a legal framework to counter hybrid threats within the EU and at the international level;

increasing support for independent and democratic media in the EU's neighboring countries. At the same time, it is planned to strengthen the editorial responsibility of the media for the disseminating unverified or biased information that undermines citizens' trust in independent media.

The United States is taking similar measures to combat Russian propaganda. The US Congress has decided to increase spending on the Russian Influence Fund by $ 10 million in 2020 to $ 285 million to support EU member states, NATO and Partner countries in countering Russia's information pressure.

Information defense experts from the US Department of Defense are taking steps to strengthen capabilities to counter disinformation and propaganda. The Agency for Advanced Research Projects has announced the development of anti-counterfeit technologies, information technologies that are able to automatically assess the changes made to media files. The possibility of using commercial technologies to combat fraud in the information environment through authentication and verification of data is considered (Derkachenko Y.A., 2016).

Conclusions

Active measures by the Russian Federation to exert destructive information influence on Ukraine and other states through the media are becoming global. Russia's goal is to change the worldview and morals of both individuals and society as a whole, to impose its interests. Social networks, which are one of the most popular resources in cyberspace, are used as a means of influencing most of society.

Analyzing the threats that arise, we can say that the information factor has a significant impact on national security (Tkachuk T.Y., 2018). In the context of information confrontation, the protection of cyberspace is an urgent problem that needs to be addressed immediately. Considering the growing role of the information component in achieving military, economic and political advantages, studying the experience of advanced countries in creating cybersecurity systems, monitoring cyber threats on the Internet and forecasting their impact is one of the key tasks for Ukraine.

Prospects for further research. Analysis of vulnerabilities in the system of information security of the state, identification of methods to counter to information influence of the Russian Federation on the basis of experience in fighting against the Russian propaganda in the leading countries of the world.

References

Derkachenko Y.A. (2016). Social networks as an environment for technologies of manipulative influence. Modern information protection, 1, 51–59. Retrieved from: http://nbuv.gov.ua/UJRN/szi_2016_1_8.

Diordica IV (2017). The concept and content of cyber espionage. Retrieved from: http://goal-int.org/ponyattya-ta-zmist-kibershpigunstva/.

Dubov D.V., Koretska I.O. (2018). "In the

interests of another state ...": problems of identifying and counteracting agents of influence. Retrieved from: http://old2.niss.gov.ua/content/articles/files/Dopovid_Dubov_2018_26_12_18-(2)-44b86.pdf.

Gorbulin V. Hybrid warfare as a key tool of n geostrategy of revenge. Retrieved from: https://dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostra tegiyi-revanshu-_.html (date of application: 15.11.2020).

Kotsurba K.O. (2014). The influence of modern information and communication technologies on the development of civil protest activity. *Problems of International Relations*, 8, 82–95. Retrieved from: http://nbuv.gov.ua/UJRN/Pmv_2014_8_8.

Manuilov Y. M., Prudnikova O. V. (2017). Information and cultural security of Ukraine in the conditions of hybrid war. Bulletin of the National University "Yaroslav the Wise Law Academy of Ukraine", 1 (32), 26-36. Retrieved from: http://nbuv.gov.ua/UJRN/Vnyua_2017_1_5.

Nesteryak Y.V. (2013). International criteria of information security of the state: theoretical and methodological analysis. Bulletin of the National Academy of Public Administration under the President of Ukraine, 3, 40–45. Retrieved from: http://nbuv.gov.ua/UJRN/Vnadu_2013_3_8.

On the basic principles of cybersecurity: the Law of Ukraine from 26.01.2018 № 2469 – VIII Retrieved from: https://zakon.rada.gov.ua/laws/term/ru/39985:64033/sp:max15 (date of application: 26.02.2020).

Radkovets Y. I. (2014). Signs of hybrid warfare technologies in Russia's aggressive actions against Ukraine. Science and Defense, 3, 36–42. Retrieved from: http://nbuv.gov.ua/j-pdf/nauio_2014_3_8.pdf.

Rozumnyi M.M. (Ed.). (2018). Putin's regime: reboot – 2018. Retrieved from: https://niss.gov.ua/sites/default/files/2018-06/New_txt-c7997.pdf.

Senchenko OM (2017). Network tools of new wars. Bulletin of the Book Chamber, 1, 37–41. Retrieved from : http://nbuv.gov.ua/UJRN/vkp_2017_1_13.

Tkachuk T.Y. (2018). Information factor in hybrid warfare. Cybersecurity in the system of national security of Ukraine: priority directions of development, 1, 39–42. Retrieved from http://repository.mdu.in.ua/jspui/bitstream/123456789/658/1/kiberbez peka_2018.pdf.