3. Протидія негативним інформаційним впливам на людину і суспільство в умовах гібридної війни

FEATURES OF THE CONCEPT OF INFORMATION WAR IN THE REALITY OF THE TODAY

Mannapova K.R.
Candidate of Psychological Sciences,
Associate Professor at the Department of Sociology and Psychology
Kharkiv National University of Internal Affairs
Kharkiv, Ukraine

Recently, methods and means of information struggle have been effectively used, which can lead to such tragic consequences as: change of social order and political system; disintegration of the state; loss of the army; the collapse of the country's economic system; loss of national idea and spiritual values; deaths of people and the like. In the information space of Ukraine there is a continuous struggle for resource management, influence and control in the territory of our country. Therefore, developing and improving the basics of information security is one of the most important and especially topical tasks of the state. However, many issues related to information security can only be successfully addressed in close coordination with international organizations.

The scientific understanding of the problems of realization of information security in modern society was facilitated by the work of the following researchers: A. Dulles, M. Castels, V.S. Shapiro, G. Verian, M.V. Baglai, A.V. Krutskikh, I.L. Safronova, O.A. Smirnova, E.B. Belova and others. Among Ukrainian researchers who develop methodological bases for information security, such as: A.G. Shirokova-Murarash, V.I. Gurkovsky, G.M. Sashchuk, G.G. Pocheptsov, V.G. Korolko, O.P. Golobutsky, V.M. Bryzhko, V.S. Tsymbalyuk, B.A. Kormich, E.Y. Kravets, O.V. Oliynyk, L.E. Shimansky and others. The famous researcher Furashev V.M. identifies major constraints on information security.

Thus, G. Pocheptsov believes that the direct precursors of the term «information war» can be considered the following: «psychological war», «political war», «psychological operation», «information operation»; the beginnings of their use in

official documents and scholarly writings date back to the first decades of the twentieth century. And the term was adopted by Americans. They date their own use of the term in 1940. The corresponding English version of the term is political war. The term psychological operations were first used in the document by Captain (then Rear Admiral) E. Zacharias [3, p. 557-558].

It should be noted that the term «information war» was used by one of the first T. Ron in an analytical report for the Boeing Company «Weapon Systems and Information War» in 1976 [4, p. 72]. From that moment on, an understanding begins to emerge that information can be a weapon. There are two leading areas of influence of information weapons: the impact on the enemy's information and systems and the impact on people's consciousness. The first direction is also called cyber warfare. The second direction is the old ways of propaganda and agitation, counter-propaganda and counter-propagation, but they have reached unprecedented heights in the sophistication and mass influence on the minds of people. The most famous definition of information wars is: «this is a type of conflict in which the opposing parties are tasked with protecting their information and information systems, manipulating information of the enemy or distorting it, as well as limiting the opposing party's ability to access and process information» [1, p. 3].

Therefore, when talking about national stability in a hybrid war, one must first investigate the terrorist threats themselves and then talk about security against them, since the primary threat is the information threat. In addition, it should be noted that for an individual there are some information threats, for society - others, for the state - others. Not only are information threats an independent class of threats, but they also serve as a basis (root cause) for the realization of other terrorist threats.

The division of information wars into species is carried out mainly by a number of criteria: it is usually taken into account what the impact is directed to, for what purpose, through which tools. In general, the following types of information wars are distinguished: 1) command and control (confrontation for the purpose of capture or disturbance of command and control mechanisms in the armed forces of the state); 2) intelligence (confrontation with the help of intelligence and counterintelligence

information); 3) financial and economic (information and economic wars for control of trade, mastering information that is necessary for superiority over competitors) 4) electronic, hacker, cyberwar (impact on electronic communications - radio, television and computer networks) 5) psychological (carried out through propaganda and manipulation with the purpose of undermining the public spirit, demoralizing the armed forces, discrediting the culture, disorienting the command of military forces or heads of the legislative and executive power); psychological wars have their subspecies by the nature of the effects used: a) information-psychological (propagate certain ideas, views, ideas, beliefs, create the basis for positive or negative mass psychic reactions); b) psychogenic (accompanied by the effects of physical factors - sound, lighting, temperature, as well as the generation of a state of shock from certain tragic events - deaths, destruction, etc.; consequences - irrational behavior, emotional affect, depression, panic); c) psychotropic (influence is carried out by the transmission of information through unconscious perception; in the case of neurolinguistic programming - by means of special linguistic programs for changing the motivation of people and their behavioral reactions); 6) networking (a set of information influences between social groups in social and professional networks to gain certain advantages in economic, military, political, cultural and public confrontations); a) high-tech networking (modern, high-tech digital communications based on television, radio, Internet, messenger, cellular, satellite and other modern communications and based on gadgets such as fixed computer devices, tablets, smartphones, personal and group devices); b) high-tech networking (modern, high-tech humanitarian technologies for creating, storing, disseminating and retrieving information; these include SMM, SEO, targeting, contextual advertising, media viruses); c) High-Sensor Networking (modern high-tech technologies that allow to regulate and manage social communication processes at the level of social groups and individuals; typical in this aspect are social psychology, applied psychoanalysis and NLP [5, p. 42-43].

Media literacy, one of the best ways to stop the spread of misinformation, is to disseminate information that helps the audience to critically evaluate the information

they see on social media. Explaining how a false story was debunked may increase the awareness of the audience about the risks of misinformation and the problems of finding the truth. Media literacy is related to developing a critical understanding of the nature of media, the techniques they use, and the impact they exert. Media literacy is aimed at understanding how media works and what they mean, what they are made of, and how they create reality. Media literacy is also being explored in Ukraine, although many papers use the concepts of «media literacy» and «media education» as identical. Media literacy is presented as a level of knowledge about the media, related to the ability to use information and communication technology, to express themselves and communicate with the help of media, to consciously perceive and critically interpret information, to separate reality from virtual simulation. Analyzing the use of the terms «media literacy» and «media education» in Ukraine, Ukrainian researcher V. Ivanov notes that in our country there are certain theoretical developments and achievements in the field of media education, but they are not aimed at forming critical thinking, but at mastering the use of media and media opportunities in the learning process [2, p. 52].

In sum, it can be summed up that a democratic society is now forced to balance between two (at least) extremes. On the one hand, there is no democracy without freedom of speech, and on the other, there is the danger of using freedom of speech to manipulate the mass consciousness.

References:

1. Bedritskiy A.V. (2003) Evolyutsiya amerikanskoy kontseptsii informatsionnoy voyny [The evolution of the American concept of information war]. *Analytical reviews of the Russian Institute of Information Technology*, no 3, 26 p.
2. Ivanov V. F. (2012) Mediaosvita ta mediahramotnist′: vyznachennya terminiv [Media education and media literacy: definition of terms]. *Information Society*, no 16, pp 41–52
3. Pocheptsov H. H., Chukut S.A. (2008) *Informatsiyna polityka* [Information policy], Kiev: Knowledge. (in Ukrainian)

4. Thomas P. Rona (1976) Weapon Systems and Information War, Seattle, WA.
5. Zhad′ka V.O. (2018) *Hibrydna viyna i zhurnalistyka. Problemy informatsiynoyi bezpeky* [Hybrid war and journalism. Information Security Issues], Kyiv: M.P. Dragomanov NPU. (in Ukrainian)