DOI: 10.52363/passa-2023.2-5

UDC 351.75

Novikov V. *- PhD Student, Training Research and Production Centre NUCDU, Kharkiv, Ukraine.*

ORCID: 0009-0002-6494-3975

INFORMATION AND HYBRID WARS IN THE CURRENT ENVIRONMENT: PUBLIC-ADMINISTRATIVE ASPECT

The role of information in the processes of national security policy implementation in the context of information and hybrid wars has been considered in the paper. It has been determined that the need to adapt public administration to the conditions of the external environment creates the need to develop effective strategies for managing various aspects of information threats. It has been established that information and hybrid wars are closely related to the policy of ensuring national security. It has been emphasized that information war involves measures directed against management systems, as well as against computer and information networks and systems. It has been proved that the destructive impact on management systems is achieved through the use of information weapons and a system of information operations.

Keywords*: information policy, information security, hybrid war, cyber war, means of information wars, technological progress.*

Problem statement. In the 21st century, information war tools have begun to play a significant role in military and non-military conflicts, and to influence governments and population. The expansion of the information space and the acceleration of information circulation based on new technologies contribute to the accumulation of real and artificially created contradictions in the information sphere.

Of special attention is such a form of conflict situation as information and hybrid war. In modern conditions, this phenomenon affects literally all aspects of social life on a planet-wide scale. It especially affects the states' national security.

Noting the generally positive role in the transition to the information society, which is expressed in the transition to new bases of information processing and transmission in order to improve the efficiency of functioning of many spheres of activity, it is necessary to point out an important circumstance in this regard.

The wave of technological progress has brought significant changes in the methods of resolving military, economic, trade and other conflicts. Direct force methods are increasingly giving way to information ones.

Understanding the negative consequences and destructive power of information war (wars) requires an in-depth study of this phenomenon.

Recent research and publications analysis. Information interactions, contacts, conflicts and different forms of their resolution are the basis of the society development.

The problem of information-hybrid wars has several aspects. In recent years, the terms information war and hybrid wars have emerged in science, implying the creation of new means of confrontation, a new type of weapon – information weapon, which is usually implied when one is talking about the so-called sixth generation wars. Modern scholars interpret information-hybrid war as a social phenomenon generated by society, as an instrument of interstate military confrontation, as a component of the regulating political conflict system, as a tool of state policy.

Various aspects of this issue were studied by foreign scientists, such as: O. Tofler, O. Vasyuta, F. Hofmann and some others. In Ukraine, H. Pocheptsov, V. Horbulin, I. Zharovska, N. Ortynska and some other authors have studied the issue of information wars.

In addition to the synthesis of social, political, economic and cultural elements, hybridity of a war also implies the combination of different tactics, the use of both regular and irregular units, the use of weapons with different purposes, i.e. the combination of elements that originally belong to different forms of wars. Analysing the manifestations of hybridity involves a critical assessment of the use of various technologies of military confrontation at the turn of the century and at the beginning of the twenty-first century.

Analysis of scientific publications on this issue confirms that modern states are involved in the process of information-hybrid wars. Noting the unsurpassed capabilities of information and communication processes in the globalized world, attention should be paid to the growing amount of information that citizens have begun to receive without the control of their national governments.

Paper objective. The purpose of the article is to analyse the phenomenon of information and hybrid wars in the modern world in the public-administrative context.

Paper main body. The definition of a "hybrid war" has been the subject of many academic papers and expert commentaries. The well-known American military analyst Frank Hoffman was one of the first to emphasize the peculiarities of modern wars: "...modern wars are characterized by hybridization, as traditional forms of war are substituted by "cyberwar", organized crime, irregular conflicts, etc.

In 2015, The Military Balance presented a definition of the hybrid war, emphasizing the methods that are used in it, namely: "the use of military and non-military means in an integrated campaign to achieve the effect of surprise, initiative and psychological and physical superiority, the use of diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and sometimes overt military and intelligence activities; and economic pressure" [1].

However, in the author's opinion, the most complete definition is given by the Polish scholar Olga Vasyuta: a hybrid war is "...a war whose main tool is the creation of internal contradictions and conflicts by the aggressor state in order to use them for political aggression, i.e. for goals that are usually achieved through conventional war" [8].

Ukrainian scholars I. Zharovska and N. Ortynska emphasize that the basis of information-hybrid wars is false information. Quite often, under the guise of a great goal – patriotism, protection of indigenous peoples, protection of human rights and freedoms, fight against terrorism, etc. – military aggression, i.e. an undeclared armed conflict, takes place, which causes not only the seizure of territories, but also significant human casualties. The term “information war” became widely used by US military experts after Operation Desert Storm where information weapons proved to be highly effective and gradually gained popularity. In 1992 p. the Pentagon issued the Information Warfare Directive (TS 3600.1) which outlines the main tasks for preparing for this type of wars.

Based on the analysis of the concepts of information wars by the types of armed forces, the US Joint Chiefs of Staff adopted the document “Joint Vision 2010”, in which they developed the concept of the information war. The elements of the information war, according to American experts, include: intelligence gathering, disinformation, psychological operations, physical destruction of the enemy’s information resources (including through electromagnetic influence), attacks (physical and electronic) on its information structure, infection of its computer networks and systems with computer viruses, penetration of information networks, etc., as well as appropriate countermeasures to protect its own information resources [2]. Information wars, also called Sixth Generation Wars, aims to establish control over the minds of citizens of a potential adversary state.

Information wars involve measures aimed at management systems, as well as computer and information networks and systems. The destructive impact on management systems is achieved through the use of information weapons and a system of information operations.

Infologems are used as an information weapon. An infologeme is a false, distorted or incomplete information that depicts real events, filled with ideological myths and political propaganda fabrications [3, p. 284; 4]. They form public opinion, stable stereotypes of individual and social behaviour, values and orientations of the population, and socio-psychological standards of citizens’ behaviour. Like any ideological myths, infologems are active and aggressive. They displace reliable information, while often remaining plausible. They are fertile ground for the tense psychology of the masses, are instantly introduced into information channels and easily flow into various areas of political and spiritual life.

Infologems are the main product of political technologists. The use of infologems is particularly effective during elections, revolutions, civil wars and armed conflicts.

Infologems include rumours, fakes, trolls, repetition of slogans or template phrases, and other methods of arousing planned psychological influence on the behaviour of the population.

Rumours are generally understood as unverified oral information or data whose reliability has not been established but not refuted. Political rumours are used to: 1) compromising allies; 2) checking the acceptability of a proposal to the public; 3) discrediting the opponent; provoking the population to take actions that are beneficial to one of the two political opponents. To prevent and refute rumours, on the one hand, all events should be reported openly and in detail, even if they have a negative aspect, but on the other hand, information should still be filtered and corrected, which creates a dilemma.

In practice, this dilemma is solved by establishing the following forms of rumour control: 1) refutation of rumours by important persons; 2) introduction of censorship; 3) creation of special governmental institutions that study rumours and provide reliable information (rumour columns in newspapers, various sociological centres) [5, p. 42-43].

Fakes are very common infologems. This concept has come into our lives relatively recently, it comes from the English word *fake* – fabricated, false, fictitious. Fake news includes photos manipulated in Photoshop, videos edited in a video editor or filmed at a completely different time and place, fake news that cannot be distinguished from the truth, so-called “newspaper hoax”, social media pages created on behalf of other, usually famous people, and fake accounts.

Some materials have video support which makes fake news look like real news. Later, the truth comes to light, but the information has already been posted online and has done its job. When emotions subside, one false piece of information is replaced by another fake. Hundreds of correspondents work to ensure that the next information bomb reaches the maximum number of people and becomes popular in a matter of minutes. In this regard, another term has emerged – trolling.

Troll, trolling is the posting of provocative messages on the Internet in order to cause conflicts between participants, insults, a “war of edits”, verbiage, etc.

Psychological influence on the enemy, based on communication processes using modern information technologies, involves changing public opinion in a given direction, which is achieved through information operations.

Information operations are planned actions aimed at an enemy, friendly or neutral audience by influencing its consciousness and behaviour through the use of organised information and information technology to achieve a specific goal. They are applied at the macro and micro levels. Macro-level information operations are any agitation and propaganda, intelligence and organisational activities aimed at specific social groups of people and carried out mainly through the media and communication channels.

Micro-level information operations have a targeted and personalised focus and are carried out mainly through interpersonal communication.

Thus, information operations involve causing damage in the political, economic, scientific, technical, social or any other social sphere of the adversary state’s life and, on this basis, exerting beneficial influence to gain advantages in a particular area.

At different times, different forces with different degrees of organisation and relationship to state structures have been involved in information war operations. In particular, it is known that special units of information (psychological) war within the structure of state bodies appeared only during the First World War. Further experience in organising information warfare has shown that the forces involved in the implementation of political and military measures can, in order to exert external influence on state policy, purposefully influence certain organisations and their units. An example is special psychological warfare units.

These units are armed with mobile television and radio centres, printing presses, equipment for conducting oral propaganda programmes for the personnel and population of a foreign state, and relevant technical means: so-called “propaganda” shells, bombs, balloons, etc., which are used to throw propaganda materials into the enemy’s territory and spray them. The availability of such means allows these units to establish targeted work on ideological and psychological influence on the enemy within a short period of time as part of various special or direct military operations. It is worth noting that recently there has been a steadily increasing activity of non-governmental organisations also involved in psychological influence.

Information-hybrid wars are periodically waged in different countries of the world. In order to organise counteraction to information operations, it is necessary to know the factors that contribute to the emergence of threats and dangers in the information sphere of the state, to find out their essence, to be able to assess and determine the reality and level of negative impact on society and the state.

Ukrainian scholars E. Larina and V. Ovchynsky in their report “Electronic Wars of the 21st Century” propose the following way to distinguish between information and cyber warfare: “Information wars are the content of a war aimed at changing mass and individual consciousness, the struggle for consciousness, values, attitudes, and behavioural patterns. Information wars existed long before the Internet. The Internet has brought these wars to a qualitatively different level of intensity, scale and efficiency, and cyber wars are aimed at the destructive effects of information flows in the form of software codes to material objects and their systems” [7].

K. Cheremnykh and M. Voskanyan in their report “Anonymous War” explain the recent increase in mass protests by the influence of information warfare mechanisms [6]. The campaigns are positioned as non-violent, although in some countries, including Ukraine, they are turning into hybrid wars. Hybrid warfare is a type of warfare that combines fundamentally different types and methods of wars, which are used in a coordinated manner to achieve common goals. Hybrid warfare uses classical methods of warfare (with uniformed soldiers, military equipment, etc.), irregular armed groups (insurgents, terrorists, guerrillas, etc.) and such types of warfare as information and cyber wars. Hybrid warfare combines guerrilla and civil wars, as well as insurgency and terrorism. There is no definition of hybrid wars in international legal documents [9, p. 52-53]. Agitators and organisers of campaigns, working with the assistance of some parties and NGOs, are increasing their activity in the combat zone and in the rear.

In countries that have a significant knowledge-intensive sector of the economy and high-tech manufacturing and are characterised by a high level of Internet penetration in everyday life, society is much more vulnerable to the use of information and cyber warfare. One of the leading US public opinion research organisations, the Pew Internet & American Life Project, conducted a survey to find out who is the most likely to threaten the confidentiality of personal and corporate information. The results were as follows: 4% are law enforcement agencies, 5% is government, 11% are other business structures, 28% are advertisers and Internet giants, and 33% are hackers [7]. States are trying to counter information and cyber wars in various ways. Therefore, it would be important and timely to analyse the social and psychological consequences of the impact of information on society, conduct comprehensive research on the problems of countering information wars and information attacks, develop measures to preserve the psychological stability of citizens, and develop measures to reduce the level of aggression and violence in society, including the "blocking" of materials that promote the cult of cruelty.

The processes of globalisation, informatisation and the shift of society's activity to the Internet require states to clearly understand the necessary changes and take active steps to create a legal framework in which society, individuals and the state are interested. In addition to the lack of a legal framework, Internet communities have another drawback – the relative instability of their formation, as even a community with the best ideas risks disappearing very quickly after the key participants lose interest [1].

With the emergence of new technologies, society, individuals and the state face new challenges. Shifting the activity of society to the Internet requires the creation of a legal framework for the Internet environment.

Conclusion. Thus, the information gap can stimulate various information threats, ranging from hacker attacks on private websites to the theft or disclosure of strategically important national information. The need to adapt management to the external environment creates the need to develop effective change management strategies.

In addition to having a positive impact on the democratisation of international political decision-making, modern society may pose a certain threat to democracy, but the risks to democracy are not a reason to slow down the development of global civil society, they are an incentive to treat it carefully. It is established that information and hybrid wars are closely related to the process of globalisation of the world. In modern conditions, special information operations and wars are being deployed against the sovereignty of states. Information and hybrid wars are periodically waged in different countries of the world on the eve of real wars and in the course of their conduct, so the task of the state authorities is to educate the public to protect against information attacks and consolidate society to counteract information influences.

References:

1. The World Hybrid War: Ukrainian Front: a monograph / edited by V.P. Horbulin - Kyiv: NISS, 2017. 496 p. - Access mode: http://ena.lp.edu.ua:8080/bitstream/ntb/27836/1/028_074_076.pdf.

2. Zharovska I., Ortynska N. Information warfare as a modern globalisation phenomenon. Bulletin of Lviv Polytechnic National University. Series: “Legal Sciences”, Vol. 7, No. 2, 2020, pp. 56-61.

3. Pietryk I. Regionalna polityka EU. Warszawa : Wydawnictwo Naukowe PWN SA, 2000. 311 s.

4. Petyk M. Ukraine in modern globalisation processes / M. Petyk // Formation of a market economy in Ukraine. - 2009. - Issue 19. - P. 530-539.

5. Shulga M. Socio-political management / M. A. Shulga - K. : Centre for Educational Literature, 2008. - 248 p.

6. Pocheptsov G. Sense and information wars / G. Pocheptsov // Information society. - 2013. - Issue 18. - P. 21-27. - Access mode: http://nbuv.gov.ua/UJRN/is_2013_18_.

7. Larina E. Digital Wars of the XXI Century [Electronic resource] / E. Larina, V. Ovchinsky - Access mode: dynacon.ru/content/articles/2321/#a1.

8. Wasiuta O. Vademecum Bezpieczeństwa Informacyjnego. Tom 2, s. 533.https://www.researchgate.net/profile/Olga-Wasiuta/publication/346473664_Wojna_hybrydowa/links/5fc40c19299bf104cf93c8d7/Wojna-hybrydowa.pdf [Access mode: 12.04.2021]