1. ЕКОНОМІЧНА ТЕОРІЯ ТА ІСТОРІЯ ЕКОНОМІЧНОЇ ДУМКИ

DOI: https://doi.org/10.32838/2523-4803/71-4-1

UDK 276.12.76

Duginets Ganna
Doctor of Economics, Professor,
Head of the Department of World Economy,
Kyiv National University of Trade and Economics
Busarieva Tetiana
PhD, Associate Professor,
specialist for ensuring the work of the Supervisory Board
of NPC Ukrenergo

Дугінець А.В.
доктор економічних наук, професор,
завідувач кафедри світової економіки,
Київський національний торговельно-економічний університет
Бусарєва Т. Г.
кандидат економічних наук, доцент,
фахівець з забезпечення роботи Наглядової Ради НЕК «Укренерго»

THE ROLE AND PLACE OF THE INFORMATION WAR IN THE MODERN HYBRID WAR

Hybrid warfare is a combination of various techniques from non-military means used to weaken the enemy, destroy statehood, undermine its culture, spiritual values, and economic stability. These hostilities have no declared start, no established front line, no combatants, but there are specific goals that the parties to the undeclared conflict seek to realize. At the same time, information warfare is one of the most important tools of hybrid warfare, moreover, the information component is contained not only in various elements of a hybrid war, but can also play an independent role in international confrontation and act as a separate type of contactless warfare. It poses the greatest threat, since the purpose of this war is to manipulate consciousness and master the minds of people. Information warfare as a phenomenon has existed for many centuries, and its recognition is at the stage of formation, but at the same time, its destructive and destabilizing effect is recognized, various measures are taken to resist both the information threat and the hybrid war as a whole.

Key words: *hybrid war, information war, information, confrontation, values, competition.*

Problem statement. Information warfare is one of the most important tools of hybrid warfare; moreover, the information component is contained not only in various elements of a hybrid war, but can also play an independent role in international confrontation and act as a separate type of contactless combat operations. It poses the greatest threat, since the purpose of this war is to manipulate consciousness and master the peoples' minds. Information war as a phenomenon has existed for many centuries, and its recognition is at the stage of formation, but at the same time, its destructive and destabilizing effect is recognized, and various measures are being taken to resist both the information threat and the hybrid war in general.

Analysis of recent research and publications. Among scientific researches in the field of the importance of the information war in the process of formation of the hybrid war there were developed a number of theoretical, methodological and methodical approaches by foreign and domestic scientists such as B. Milner, I. Nonaka and X. Takeuchi, P. Senge, V. Bukovich, K. Viig, D. O'Leary, D. Snowden, Y. Vovk, M. Martynenko, A. Degtyar and M. Bubliy, A. Nalyvayko, N. Butenko, N. Smolinska and I. Hrybyk, S. Leonov and other scientists. At the same time, it is important to note that at the beginning of the 21st century, the understanding of the role and the place of the information war in the modern hybrid war requests more attention.

Formulation of the aims of the article. The purpose of the article is to analyze the role and play of the information warfare in hybrid warfare, its specific characteristics and the way the information can influence the development of the hybrid war.

Presenting main material. The modern world is experiencing a difficult period of exacerbation of geopolitical contradictions associated with the new redistribution of zones of influence. As a result of these processes in many regions there is a significant increase in instability, which actualizes the problem military security of states. Despite global transformations world system, the potential of military force is still considered one of the effective factors of world politics.

Due to the current geopolitical situation and revolutionary changes in the information technology sphere there is an urgent need to form a modern concept military security, which requires a new look at the ratio of armed and unarmed methods of confrontation. The national security of the state can be measured according to various criteria, the importance of military potential in its maintenance continues to be one of the priority, since the role of military power in world politics has not been decreased, but, as we can observe, it progressively increases. Recent events have convinced that the military aspect of the national security is relevant not only on a theoretical, but also on a practical level.

The nature of wars and armed conflicts in the modern world is undergoing significant changes, including in connection with the emergence and practical application of new methods of armed struggle. So, application of armed means can be both combat and non-combat nature, methods the conduct of hostilities can be both direct and indirect. Hybrid warfare can be interpreted as a model of war that tries to hide its military nature, as well as the participation of state structures in it. That is why the role of the information component in it sharply increases, since real physical contexts are replaced by inadequate informational contexts that hide and cover the real state of affairs more intensively than is the case in a war of the usual order. The unfolding situation, as a rule, has no analogs in history, so it allows for a plurality of interpretations. And this again requires intensified work of the information mechanisms, which are trying to send in the wrong direction, both the consciousness of the enemy and their own population.

Hybrid warfare is already asymmetric in nature. US military analysts use the term "asymmetric warfare" to describe the strategies and tactics of US state and non-state rivals seeking to achieve their strategic goals despite US superiority in conventional military power. Asymmetric methods of warfare, which ultimately boil down to using the strength of one of the opponents against the weak side of the other, have always been an integral part of a successful strategy. Asymmetry naturally includes non-kinetic approaches in the "grey zone" between war and peace. However, the development of information technology allows state and non-state actors to direct their actions against political leaders and the public through the globalized online media and the Internet. In the future, this expands the concept of war and includes cultural, social, legal, psychological and moral aspects, where military force is less suitable for solving the assigned tasks [1].

Today, the "information war" is an umbrella concept that, by definition, covers scattered provisions from many spheres of knowledge and forms a more complex education from them that has an effective explanatory power. Among the most common terms that are used to refer to a variety of practitioner in the aspect of information war, the following can be noted: safety information systems, information superiority, information dominance, critical infrastructure protection, operational security, and many others. Information wars become increasingly sophisticated and effective due to intensive development of the information technology sector. Their negative impact on a wide variety of values – as well as self-awareness – of the affected party may not be felt for a long period, but sometimes it goes unnoticed. Party using information war is able to find an appropriate channel for its actions due to interconnectedness and interdependence of many infrastructures in the modern world.

Information warfare is one of the most extreme threats to national security. The essence of the threat lies in the achievement by any state of excessive superiority in the information field. This superiority makes it possible to influence the behavior of citizens, the political elite, the military, and allows to model public opinion. Information warfare expands the space of warfare; this type of war does not have a front line. It is impossible to unambiguously determine whether informational impact is being carried out at the moment, it is also impossible to detect the conduct of informational operations. Therefore, such an impact is hardly recorded, and the authors of the operations remain unknown. The situation with information wars is complicated by the absence of any international legal and moral norms for waging information war. Participants in an information war can be any actor, from states and state special services to any criminal group, including terrorists [2]. To conduct such a war, technical means are needed, the low cost of which makes information warfare accessible even to ordinary citizens who do not suspect that their intentions are criminal.

For the first time, the term "information war" was used by the American science advisor Thomas Rona in the report "Weapon systems and information war" for the Boeing company in 1976. In particular, the author pointed out that the information infrastructure is becoming a key component of the American economy, but at the same time it is becoming a vulnerable target, both in wartime and in peacetime. The publication of T. Ron's report was the beginning of an active media campaign. The very formulation of the problem aroused the interest of those American specialists who deal with "classified materials". The US Air Force has been actively discussing the subject since 1980. By that time, there was a general idea that information can be both a target and a weapon.

If the goal of a classic war is to inflict damage on the support systems of the enemy state, then the damage caused by information wars is aimed at massive psychological processing of people in order to destabilize the political situation in the country. The main advantage of information

attacks is the ability to achieve a goal without firing a single shot, just imposing different values, different views, reprogramming people's minds in a way that is beneficial to the enemy. And the main audience for such influence is the youth and the ruling elite [3].

Information warfare is a war over ideas and values. It is part of a psychological war, which is aimed at the non-physical destruction of a person, but at the reorientation of his or her consciousness. Considering the essence of information war, it is necessary to point out that this war is aimed at citizens, since information technologies penetrate into everyday life, forcing everyone to be susceptible to imposed ideas, so as to remain indifferent to others. The danger of information attacks lies in the fact that if they are successfully executed, society undermines from the inside, and destroys it in the end result. There are three goals of information war: control of the information space for use for their own purposes; control over information flows for carrying out information attacks on the enemy; improving the efficiency of the armed forces through military information functions.

The main methods of information warfare are methods of information and psychological impact, which can also accompany other elements of a hybrid war. The impact can be carried out by various means (information), where the dissemination of information is the main factor of influence. Thus, the government can prepare the people for a positive assessment of the military policy of its state and form patriotic views through the media, or a probable adversary can introduce ideas and moods that are beneficial to him or her, opposite in direction. A system of trade financial and economic sanctions is applied. This leads to a weakening of the state's economy, a drop in living standards, household difficulties, an increase in the number of epidemiological diseases and, as a result, citizens' dissatisfaction with the existing situation. The pressure can come from political means. Thus, the support of opposition parties and movements by foreign investors is carried out in order to put pressure on the political leadership of the country. The main component of information warfare is the information and psychological warfare. It acts as an instrument of 27 psychological influence on the masses, contains the means and methods of influencing the minds of people. The use of any influence on the psychological state of a person in order to change his or her motivation, especially during the conduct of certain hostilities or preparation for them, refers to such a type of information war as psychological warfare. There are no moral restrictions in psychological warfare; any means of undermining the enemy's morale are allowed, like murder, poisoning of water and food, sabotage, even terror, which makes it similar to a hybrid war, at least in terms of its general tools [4].

Information and psychological operations (actions) of the enemy in cyber space require the use of various Internet resources. Examples of information and psychological operations are the preparation and dissemination of specific information on social networks and other Internet resources aimed at discrediting the Ukrainian authorities, ATO command and military personnel within the campaigns "If not for the generals," "Generals traitors to Ukraine," "Glory to Ukrainian artillery" etc. Disinformation, or unverified, fake information, including the use of special technologies to increase the rating of such messages, is often disseminated in the national cyber space as military patriotic resources. Thus, "hybrid war" is a high-tech conflict. This is a continuation of the policy of the state and/or coalitions, political groups, transnational corporations and non-state actors. The purpose of the conflict is to impose the will of the actors on their opponents through integrated adaptive and asymmetrically synchronized destructive means of influencing them in a multidimensional space and in different spheres of life. Hybrid warfare rationally combines conventional and unconventional components with an emphasis on the use of multiple sources and modes of attack, synergy of results, and a high level of uncertainty for opponents regarding ultimate strategic goals [5].

Information war presents a rapidly developing and all the hard-to-define realm of real interests for defense strategists and policymakers. A source of growing interest in this area can be considered the so-called information revolution, which is based on the accelerated evolution of cyberspace, microcomputers and related technologies. For militaristic purposes, each of the warring parties seeks to use information war, the global information infrastructure and the corresponding advanced technologies. Coalitions involved in mutual information war possess significant resources, including complex control systems and infrastructure, exercising tight control over cash flows, air traffic, electricity, natural resources (primarily gas and oil) and other information-dependent objects. Conceptually, in if the adversary attempts to destroy these systems and infrastructures using information warfare technologies, the information warfare for the wounded side takes on a strategic character.

In hybrid conflicts, the main goals are to seize control over society, influence the mentality of people, manipulate people who are responsible for making important decisions in the state. The enemy is trying to manipulate the basic values, motivational factors, cultural basis and strategic, communication and critical infrastructure of the country. This is achieved by a complex, balanced exercise of influence using soft and hard power. That is why critical elements of systems, in other words, objects of asymmetric actions in hybrid conflicts, are important for key elements of systems (components, subsystems) of the state, political, diplomatic, social, technical, energy, financial, cyber, socio and cyber, information and other systems. The influence on them within the limits of optimal measures and correlations of the parameters of space, time and resources for the party exerting this influence leads to the desired, purposeful, fast, cascading, synergistic and destructive changes (disturbances) for these systems in their relations, structures, processes and results of functioning [6].

Today's international situation is characterized by a new round confrontation of geopolitical subjects associated with the redistribution of zones of influence in the modern world. Moreover, this struggle is carried out in mainly unarmed ways, but in new ways, involving the use of economic sanctions, information technology, terrorist operations, the use of which can destabilize the situation on the territory of the enemy.

The emergence in the modern world of new ways of fighting for power and resources associated with the need to modernize the military security system countries, expanding its capacity to deal with new threats and counteracting them.

In this regard, it is obvious that understanding the nature of modern risks and threats caused by attempts by a number of political actors to implement redistribution of the world, will form a more effective defense of the national security of states.

Conclusion. The policy of the state in relation to advanced technological, information and cyber security systems has become one of the most important components of the national security policy in the military sphere. Modern technologies have changed the ability to influence enemy forces, giving rise to the need to reorganize management and protection against soft and military methods of influence, including training personnel to continuously maintain the combat readiness of forces. The experience of various countries that have already faced new forms of hybrid warfare proves that a high level of national security and defense must be maintained even in the context of the global economic crisis and significantly reduced military spending. Expanding the battlefield beyond kinetic operations and attacks on infrastructure requires the integrated use of both traditional force doctrines and new technological and synergistic planning.

References:

1. Glenn R.W. (2019) Thoughts on "Hybrid" Conflict. *Small Wars Journal.*
2. Hoffman F.G. (2017) Conflict in the 21st century. The rise of hybrid wars. Arlington: Potomac Institute for Policy Studies.
3. Vacca W., Davidson M. (2019) The Regularity of Irregular Warfare. Parameters.
4. Liang Q., Xiangsui W. (2017) Unrestricted Warfare: China's Master Plan to Destroy America. Panama City, Pan American Publishing Company.
5. Miles F. (1999) Asymmetric warfare: an historical perspective. Carlisle Barraks, U.S. Army War Colledge.
6. Kaldor M. (2019) New and old wars: organized violence in a global era. Cambridge.

РОЛЬ ТА МІСЦЕ ІНФОРМАЦІЙНОЇ ВІЙНИ У СУЧАСНІЙ ГІБРИДНІЙ ВІЙНІ

Необхідно зауважити, що серед сучасних наукових підходів до класифікації типів воєн так званого «четвертого покоління» важко зустріти концептуалізацію гібридної війни як окремого типу війни. Це, перш за все, пов'язано з тим, що в науці, особливо української, існують іноді діаметрально різні підходи до визначення поняття гібридної війни. Гібридна війна являє собою сукупність різних прийомів з невійськових засобів, використовуваних для ослаблення противника, руйнування державності, підриву його культури, духовних цінностей, економічної стабільності. У даних бойових дій немає оголошеного початку, немає встановленої лінії фронту, немає комбатантів, але є конкретні цілі, які прагнуть реалізувати боку неоголошеного конфлікту. У той же час інформаційна війна є одним з найважливіших інструментів гібридної війни, більш того, інформаційна складова міститься не тільки в різних елементах війни гібридної, але і може відігравати самостійну роль в міжнародному протистоянні і виступати окремим видом безконтактних бойових дій. Вона являє собою найбільшу загрозу, оскільки метою цієї війни є маніпуляція свідомістю і оволодіння умами людей. Гібридної війні передує досить тривала і комплексна підготовка, а тому їй передують гібридні загрози, які, по суті, є викликами для держави. До таких загроз можна віднести: створення політичних і громадських рухів, які симпатизують майбутньому агресору; налагодження сприятливого інформаційного поля; пропаганду; нав'язування агресором власних історичних, культурних, ідеологічних цінностей тощо (тобто, все те, що покликане за допомогою, так званої, «м'якої сили» схилити населення на сторону агресора). Водночас, треба зазначити, що інформаційна війна як явище існує безліч століть, а її визнання знаходиться на етапі становлення, але при цьому, визнається її руйнує і дестабілізуючий вплив і приймаються різні заходи з метою протистояти як інформаційну загрозу так і гібридної війні в цілому. В цілому, формування єдиної комплексної концепції гібридної війни, концептуалізація поняття гібридної війни в політичному дискурсі і подальше закріплення його в нормативних документах дозволяють вивести наукові дослідження цього явища на якісно новий рівень. Подальші дослідження повинні виявити окремі елементи гібридної війни, особливості проведення операцій, механізми протидії гібридної війні.

Ключові слова: *гібридна війна, інформаційна війна, інформація, протистояння, цінності, конкуренція.*

РОЛЬ И МЕСТО ИНФОРМАЦИОННОЙ ВОЙНЫ В СОВРЕМЕННОЙ ГИБРИДНОЙ ВОЙНЕ

Гибридная война представляет собой совокупность различных приемов с невоенных средств, используемых для ослабления противника, разрушения государственности, подрыва его культуры, духовных ценностей, экономической стабильности. В данных боевых действий нет объявленного начала, нет установленной линии фронта, нет комбатантов, но есть конкретные цели, которые стремятся реализовать стороны необъявленной конфликта. В то же время информационная война является одним из важнейших инструментов гибридной войны, более того, информационная составляющая содержится не только в различных элементах войны гибридной, но и может играть самостоятельную роль в международном противостоянии и выступать отдельным видом бесконтактных боевых действий. Она представляет собой наибольшую угрозу, поскольку целью этой войны является манипуляция сознанием и овладения умами людей. Информационная война как явление существует множество веков, а ее признание находится на этапе становления, но при этом, признается ее разрушает и дестабилизирующее влияние и принимаются различные меры с целью противостоять как информационную угрозу так и гибридной войне в целом.

Ключевые слова: *гибридная война, информационная война, информация, противостояние, ценности, конкуренция*.