UDK 35-355.01
DOI: 10.24144/2078-1431.2021.2(27).82-91

Mykola Hranovskyi,
graduate student of the Department of Political Science and Philosophy
Educational and Scientific Institute "Institute of Public Administration"
Kharkiv National University named after V.N. Karazina

ANALYSIS OF HYBRID OPERATIONS AND MANAGEMENT DECISIONS TO COUNTER SUCH PHENOMENA – ANALYSIS OF FOREIGN EXPERIENCE

У сучасному світі спостерігається тенденція до значного зростання кількості гібридних конфліктів, які стають дедалі більш витонченими і непередбачуваними.

Статтю присвячено теоретичним і практичним аспектам таких явищ, як гібридна війна, гібридний конфлікт або агресія, що впливають на безпеку міжнародного середовища, а також діям органів державної влади щодо протидії таким загрозам, зокрема у країнах ЄС.

Здійснено спробу дати відповідь на запитання: «У чому виражається суть гібридних дій? Як відбувається їх еволюція? Яким є характер сьогоднішньої гібридної агресії?».

Сучасна практика гібридних операцій з боку агресора демонструє кардинальну зміну тактики та засобів, які використовує держава-гравець світового рівня проти супротивника, який є слабким і нездатним захищати цілісність власної території.

Аргументи, викладені у статті, підтверджують необхідність подальшого проведення досліджень гібридних дій, які порушили цілісність державних кордонів багатьох країн, у тому числі й України, та продовжують становити реальну загрозу безпеці в Європі та світі.

Ключові слова: *безпека, гібридна війна, гібридний конфлікт, гібридні дії, гібридні операції, тероризм.*

In today's world there is a tendency to significantly increase the number of hybrid conflicts, which are becoming more sophisticated and unpredictable.

The article focuses on the theoretical and practical aspects of such phenomena as hybrid warfare, hybrid conflict or aggression that affect the security of the international environment, as well as the actions of public authorities to counter such threats, in particular in the EU.

During the analysis of this question, an attempt was made to answer the following questions: "What is the essence of hybrid actions? How is their evolution? What is the nature of today's hybrid aggression? "

The arguments presented in the material confirm the need for further research into hybrid actions that have violated the integrity of the state borders of many countries, including Ukraine, and continue to pose a real threat to security in Europe and the world.

The current practice of hybrid operations by the aggressor demonstrates a radical change in the tactics and means used by the world-class player against an enemy who is weak and unable to defend the integrity of its own territory.

Key words: *security, hybrid war, hybrid conflict, hybrid actions, hybrid operations, terrorism.*

Formulation of the problem. The beginning of the 21st century is characterized by new challenges in the field of international security. It is believed that the end of the Cold War did not eliminate domestic or regional sources of conflict and did not ensure stable peaceful coexistence in the world. According to experts, the international community is facing not so much a direct armed conflict, but one of the types of military operations, which can also be called hybrid. Unfortunately, phenomena such as armed uprisings, guerrilla and civil wars, and other small conflicts will soon become commonplace in the new world order. Therefore, it can be assumed that in the near future different states will be involved, directly or indirectly, in new armed conflicts [18].

Analysis of recent research and publications. The works of foreign scientists and researchers M. Creveld, E. Toffler, R. Glenn, W. Lind, J. Metis, T. McQueen, and U. Nemet, F. Hoffman, J. Berznis, F. Van Kappen, J. Kalh, T. Huber and others. Widespread use of methods and techniques of military-political conflicts of the hybrid type to solve interstate problems at the present stage have also prompted domestic scientists to in-depth analysis. Thus, recently the works of V. Gorbulin, E. Magda, G. Lutsyshyna, Y. Klymchuk, G. Sytnyk, A. Slyusarenko, L. Smol, G. Perepelytsia, B. Parakhonsky, M. Trebina, G. Yavorska and others.

In many armies around the world, the analysis and study of experience gained in both small local conflicts in the past and in multinational operations at the beginning of the XXI century, are already conducted at the strategic level [19].

The main problem is the inability to overcome the stagnation in which modern martial arts found itself due to the growing complexity of conflicts and methods of resolving them [13]. Accurate prediction of the future, especially of armed conflicts, is extremely difficult due to the dynamics of evolving actions and the unpredictability of the reactions of the parties to the conflict. This corresponds to the old saying that "(...) war is full of passions, inaccurate information and errors of assessment, and finally, many things happen in it by accident" [12]. However, based on current trends, it is possible to formulate the thesis that in the modern world the number of places where armed conflicts may occur will increase, the threat to security and interests will increase, including the North Atlantic Alliance and countries seeking to join. These arguments further confirm the need for even more in-depth research on hybrid activities, which, using government or non-government agencies, pose a real threat to security in Europe and the world.

The purpose of this article is to analyze hybrid phenomena and the experience of foreign states to counter hybrid aggression, including through the adoption of appropriate decisions by government agencies, with an unidentified enemy, which indicates that hybrid operational facilities had the ability to use standard tactics and paradigm security, which was based on traditional

military technologies of state defense systems and methods of conducting military operations, was completely undermined [14].

Presentation of the main material of the study. The etymology of the term "hybridization" comes from the Latin word "hybrida" - mixing - a mixture, a combination of two or more different objects or characteristics, properties in one object [2].

At present, the current international environment is facing a new challenge, which is to counter the threat that may arise from a possible hybrid conflict.

Hybridization can be understood as the coexistence of elements of "old" and "new" wars, classic armed conflicts and "postmodern" wars, clashes between national armies and asymmetric conflicts, military supertechnologies and primitive weapons, struggle for territory and resources, and disputes over identity and identity. , the opposition of Eastern civilization to Western civilization [15].

According to T. Huber, author of the concept of war as a complex product, the use of armed forces and scattered irregular forces in combat operations will not be effective without centralized, network-oriented management of military operations and proper recognition of the space of military confrontation [8]. A comprehensive definition of hybrid activity should take into account as much as possible all the experience of this type of operation in recent decades. The simplified statement that hybrid war is "guerrilla warfare + modern technology" is only part of the truth and can only concern non-state actors. Such activities on the part of an entity such as the state are much broader. The range of methods used by the aggressor can range from traditional armed warfare, using non-traditional weapons, cyber weapons and information warfare, to special services that preserve the disintegration of societies, through the activation of the agency of influence [11], and terrorism or support and the use of criminal acts. All activities are subject to the highest political goal of the aggressor state.

Latvian analyst J. Berznis calls the hybrid war the fourth generation war. However, according to some military experts, including Russian, hybrid aggression can be called a "war of the new generation", the rules of which have changed fundamentally. The role of non-military means (economic, cultural) to achieve political and strategic goals has increased. Such measures are much more effective than classical military methods. Thus, to create a permanent front throughout the enemy state, special purpose formations, the potential of the internal opposition, informational influence, as well as ever-changing forms and methods of influence are used. " In the approach to hybrid conflicts, there is no difference between war and peace in the classical sense of the term, as well as between the military and covert activities, which is very different from what war theorists have traditionally focused on. An important element in the "new generation war" is the erasure of differences between levels of action: strategic, operational and tactical, and between offensive and defensive actions. Non-contact, remoteness, influence on the enemy becomes the main means of achieving the goals of combat and operations. A hybrid war can turn a completely stable country into an arena of the most intense armed conflict in a few months or even days! "[16], [13].

In turn, NATO's August 25, 2010 document "Bi-Sc Input To New NATO Capstone Concept for the Military Contribution to Counter Hybrid Threats" provides an assessment of hybrid threats to global security in the 21st century. A NATO study indicates that a future potential adversary will combine different models of war while using a combination of routine, irregular, terrorist and criminal activities, called hybrid warfare or hybrid threat. It was determined that the content of this activity will be a combination of conventional capabilities with tactics of irregular armed forces, as well as terrorist and criminal activities [7]. The essence of criminal activity in this case will be to destabilize the functioning of local government and support the insurgents and all oppositionists by supplying technologically advanced weapons, ammunition and financial resources. Criminal groups, which function as a hierarchical structure in an urban environment, will provide both the basis and support for widely understood hybrid activities, including drug terrorism. It is assumed that the enemy, to gain an advantage, will use all of the above combat models simultaneously, as well as high-tech systems and use them in specific ways to achieve their own goals.

The results of the analysis of the experience of hybrid operations indicate that the future operational environment will be dominated by a hybrid form of action aimed at the most vulnerable points of the armed forces of the states involved in the conflict or the critical infrastructure of the state party. It is to be expected that a potential adversary will use all possible forms and methods of military operations, as well as various tactics. It can be assumed that in case of conflict and intervention, the enemy mixes with the local community and prefers long-term, insurgent and guerrilla actions, including the possible use of improvised explosives and rocket fire. In addition, these activities may include the use of high-tech weapons systems with the simultaneous conduct of classic terrorist activities and cyberspace activities aimed at countering both weapons systems and civilian critical infrastructure systems. This will have a devastating effect on the functioning of the state.

Based on the results of the study, it can be concluded that traditional doctrinal models of military operations have lost their relevance and can not demonstrate their effectiveness in confronting a hybrid opponent.

An example of the full range of methods and forms of hybrid warfare, where a weaker adversary uses them against a stronger one, is the protracted conflict between Israel and Hezbollah. Based on Israel's experience over the past decade, it can be argued that irregular means used by non-state actors are being transformed into hybrid actions used by states. Future challenges will be that the potential opponent will have a much wider range of organizational structures and use more sophisticated strategies and tactics than those faced by the Israeli army in 2006. Hezbollah has clearly demonstrated that non-state actors are able to make a reliable assessment of the strategic capabilities of armies known as the West and successfully confront them with state-of-the-art capabilities. In conclusion, Israel's ongoing conflict with its non-state enemy demonstrates the scale of the Israeli army's and intelligence services' intelligence, military and information efforts to create conditions for neutralizing and eliminating the terrorist organization.

Thanks to Iran's support and its introduction in Lebanon, Hezbollah has become a dangerous threat not only to Israel but also to the Middle East. Hezbollah's victory over the Israeli army in 2006 demonstrated the organization's effectiveness and the level of its threat to neighboring countries in 2006. The question of further development of this organization, of course, is open and can not be ignored [3].

The experience gained from the operations in Iran and Afghanistan, as well as the Ukrainian crisis, shows that states can turn regular units of the armed forces into irregular formations that will be able to adapt new tactics and then support regular units.

Thus, states cannot be perceived through the prism of having only classical armed forces, and non-state actors can only be associated with irregular activities, because in the future hybrid armed forces may be used unpredictably.

A typical example of a powerful state waging a hybrid war with a weaker adversary is the conflict in eastern Ukraine, which can be divided into four stages: political sabotage, separatist social and political position, military intervention and deterrence, demonstrating the potential of non-traditional forces. Characteristic of this conflict is that the above stages often overlap and have different intensities. Despite clear signs of involvement in the regular armed forces, Russia has officially denied involvement in the conflict. NATO experts say the crisis is far beyond Ukraine. Russia believes that the protection of ethnic Russians is not the responsibility of the countries in which they live, and is not subject to their laws, government or constitution, but falls under the Russian Federation [17].

According to K. Walker - former Special Representative of the US State Department for Ukraine (2017-2019), this approach of the Russian government to ethnic Russians, which was previously used, for example, in Estonia in 2007, in Georgia in 2008 through slow but systematic actions aimed at violating sovereignty. It was part of a strategic landscape that was well known in Russia. Sometimes it involves more open and obvious steps, sometimes it is more subtle, it is a struggle with the help of the economy, sometimes it is cyberattacks carried out under the guise of independent activists. "... This set of hybrid warfare tactics has been used by Russia for at least 5-6 years."

There are many preconditions for concluding that the Russian-Ukrainian conflict, unfortunately, is still in its infancy. The time since the beginning of Russia's aggression against Ukraine has allowed both European and NATO analysts to work out scenarios and methods for Russia's hybrid war. The element that initiated it was the activity in the field of information warfare. Analyzing the scenario of Russian aggression in Ukraine, one can question the thesis that Russian aggression began with protests on the Maidan. There are many indications that the Russian attack actually began long before President Viktor Yanukovych left the country. Military participation in the conflict, where Russian paratroopers appeared in the Crimea and Donbas virtually without identification, was preceded by an information offensive. In the years before the conflict, the Russian side began to expand the media in Ukraine. The weapons used

to destabilize the information structure of the Ukrainian media were Russian media companies, with the help of which coordinated information penetration into Ukraine was carried out. The expansion was carried out by purchasing shares in the media from Ukrainian oligarchs. Thus, Ukrainian society began to receive information that highlights the situation in terms of the interests of Russia, not Ukraine. There was manipulation of the media by society. The basis thus created was overlapped by the integration of pro-Russian circles and the intensification of Russian agents of influence.

There are several key methods of attack and the main objectives of the intervention. First, misinformation. The participation of enemy soldiers is masked by the formation of voluntary separatist forces. The concentration of troops of the aggressor country, transferred to Ukraine, took place under the pretext of exercises in the border regions. Although this method can be classified as traditional, it was used in the war with Georgia, it was a novelty in preparation for war in cyberspace. At the beginning of the aggression, hundreds of social media pages and sites appeared on the Internet. It would seem to be "independent and objective information" about events, but in fact interconnected and coordinating active disinformation activities. The purpose of information attacks is to promote negative phenomena in society and the government elite of the country that is the object of aggression. Phenomena such as widespread corruption, strong nationalism, and gaps between the presidential and prime minister's camps have been the main targets of information warfare attacks. The information war against Ukraine is accompanied by similar actions by the aggressor in Europe and the world. An intensive information campaign is underway to increase divisions in the European Union and NATO over the need for and volume of assistance to Ukraine and the legality of sanctions against it. For this purpose, they are used as interpersonal contacts with Western politicians, economic incentives and media influence. The information space represents and emphasizes the Russian version of events, and the common goal seems to be to divide public opinion.

Ukraine is losing the information war. Ukrainian institutions of counteraction are still in the initial phase of their creation. The situation is further complicated by the fact that the security system and international law do not provide for such a sphere of military activity. Neither the UN Charter nor the OSCE founding documents define the concept of information warfare or monitoring methods, nor do they prohibit its conduct. International law is helpless in the face of Russian aggression, as evidenced by the lack of reaction of the OSCE mission to Ukrainian evidence of Russian disinformation activities or even the participation of regular units of the Russian army in the conflict. International observers are also limited in their actions [1].

In addition to the above, the aggressor uses humanitarian convoys as one of the elements of the camouflaged rearmament of separatist forces. There is a correlation between humanitarian convoys and the increase in the intensity of separatist military operations [6].

Through the analysis it can be concluded that the Russian Federation can use the "Ukrainian success" as a template for further use. It is clear that not

only Ukraine is at risk, but also every country inhabited by the Russian minority. The methods used during the hybrid war in Ukraine can be transferred to other regions, including the Baltic countries. It can be assumed that the main and effective action to stop Russia's aggressive tendencies is the unity of Western powers and Ukraine's support for critical military capabilities. The experience of recent conflicts, where elements of hybrid operations are widely used, shows that the potential of non-state actors, especially to influence in the military sphere, is constantly growing.

The power of the aggressor state, combined with elements of hybrid warfare, proves the weakness of international security institutions, and the international agreements that have been proven so far have been called into question. Although theoretically, most experts are of the opinion that the inability to stop aggressive actions against Ukraine at the present stage will lead to a growing threat of destabilization of the entire region of Central and Eastern Europe.

In terms of international experience, the EU's East Strat Com Task Force, an operational task force on strategic communications in the European Union, was launched in the EU almost five years ago to:

- clarification of key aspects of the European Union policy, creation of its positive image and counteraction of misinformation;
- effective communication and promotion of the EU's Eastern Partnership policy;
- general development of the media space in the Eastern Partnership countries and the EU member states, which provides for the promotion of media freedom;
- improving mechanisms that enable the EU to anticipate, assess and respond to disinformation disseminated by external actors [9];
- providing information support to EU delegations in Azerbaijan, Armenia, Belarus, Georgia, Moldova, Ukraine;
- the task force publishes a weekly Review of misinformation on the website https://euvsdisinfo.eu.

And since September 2017, the European Center for Counter-Hybrid Threats (hereinafter - the Center) has been operating in Helsinki (Finland).

The decision to establish the Center was made by representatives of NATO and the EU, and its founders were 12 countries: Finland, Sweden, Norway, USA, France, Germany, Britain, Spain, Poland, Estonia, Latvia and Lithuania. The Centre's initial annual budget was around € 1.5 million.

The purpose of this structure is to counter "new threats to destabilize", conduct research, analyze hybrid threats and methods to combat them, organize joint training for member countries, as well as organize and hold consultations at the strategic level between EU and NATO members, with involving governmental and non-governmental experts in the dialogue.

A practical demonstration of NATO's strategic communications activities was the opening of the NATO Strategic Communications Center of Excellence, which has been granted international status (Latvia, 2014). In particular, the center was established by seven partner countries, including Latvia, Lithuania, Estonia, Germany, Poland, the United Kingdom and Italy.

The main mission of the Center is to support the process of developing NATO's capabilities, enhancing the effectiveness of missions and their functional component by ensuring full and timely expertise of strategic communications. Given that the Center's goal was to improve NATO's strategic communication capabilities through research and analysis, concept development, research, and education and training. The center works as a research institution that carries out scientific-analytical, educational-methodical and information-communicative activities, as well as testing scientific and practical approaches.

The center's activities involve international experts in various fields of strategic communications, including public diplomacy, public relations, military public relations, information and psychological operations, as well as experts in related fields for seminars and conferences organized managed by the center. The development of NATO's Strategic Communications Capabilities is the focus of the Center's Strategic Communications Excellence Center.

On the basis of this center a number of special training courses on strategic communications have been developed, the magazine "Strategic Communications in the Field of Defense" (Defense Strategic Communications) is published; research is carried out; Conferences and seminars are held on the role of propaganda in the modern world, the Russian information war against Ukraine, manipulative techniques, the transformation of social media into weapons, NATO's practice on strategic communications, etc. [10].

Conclusions

Based on the study, it can be concluded that the evolution of hybrid activity, especially over the last decade, has been very dynamic and confirmed the effectiveness of achieving a lasting advantage over the opponent. Modern hybrid operations are conducted with a combination of conventional weapons, guerrilla warfare, terrorism and criminal behavior in order to achieve certain political goals, the main tool of which is the creation of an aggressor state in a state chosen for aggression, internal contradictions and conflicts and their subsequent use to achieve political goals of aggression, which are achieved by ordinary war.

The experience gained from the operations in Iraq and Afghanistan, and especially the armed conflict in Ukraine, shows that it is the states that can transform regular units of the armed forces into irregular formations with classic capabilities and adapt non-traditional methods of operations and then support regular units. The armed conflict also demonstrated not only the weakness of the Ukrainian side, but also the ineffectiveness of the organizations responsible for ensuring international security: NATO, the OSCE and the United Nations.

Further escalation of hybrid activity in Ukraine undoubtedly threatens the countries of the North Atlantic Alliance. The methods used by the aggressor in the hybrid war in Ukraine can be transferred not only to the territory of the former Soviet republics, but also to the Baltic states, Poland and Romania. The crisis situation in Ukraine has completely changed the security situation in the region of Central and Eastern Europe. Prolonged conflict will have the effect of reducing international security, and taking into account the lessons of "hybrid

wars" will clearly help build and strengthen the security and defense sectors of both individual countries and coalitions in the context of "new generation wars."

And the further continuation of the hybrid conflict in the East of our country requires Ukraine to take active action and effective management in the field of preventing and combating hybrid threats. It must be clearly understood that delays in resolving the conflict will inevitably lead to a "frozen" state, which almost automatically, in literary language, "puts a cross" on Ukraine's European and Euro-Atlantic prospects indefinitely.

REFERENCES

1. Analitychnyy dokument: «Hibrydni zahrozy Ukrayini i suspil'na bezpeka. «Dosvid ЕС і Skhidnoho partnerstva», Kyyiv – 2018, Retrieved from https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf
2. Vikipediya. Retrieved from https://uk.wikipedia.org/wiki/Гібрид_(значення)
3. Informatsiyne ahentstvo «Oboronno-promyslovyy kur'yer». Retrieved from http://opk.com.ua/як-заповідав-сун-цзи/
4. «Tuman hibrydnoyi viyny: chomu shkidlyvo myslyty hibrydno», V. Artyukh. Retrieved from https://commons.com.ua/uk/tuman-gibridnoyi-vijni-chomu-shkidlivo-misliti-gibridno/
5. Ukrayins'ka literaturna hazeta «Viyna novoho pokolinnya», 15.10.2018, Retrieved from https://litgazeta.com.ua/articles/vijna-novogo-pokolinnya/
6. Ukrayins'ke natsional'ne informatsiyne ahentstvo «Ukrinform». Retrieved from https://www.ukrinform.ua/rubric-ato/2818620-es-pro-rosijski-gumkonvoi-ludi-strazdaut-vid-rozpocatogo-rosieu-konfliktu.html
7. Bi-sc input to a new nato capstone concept for the Military contribution to countering hybrid threats. Retrieved from https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf
8. «Compound Warfare: That Fatal Knot»T.M. Huber, Retrieved from https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/compound_warfare.pdf
9. EEAS homepage: «Questions and Answers about the East Strat Com Task Force». Retrieved from https://goo.gl/aJS2xk
10. «European Centre of Excellence for Countering Hybrid Threats». Retrieved from https://www.hybridcoe.fi
11. «Kanva vivyadu agenturalnego», A.I. Kuk, Warszawa 1994, s.19. Retrieved from https://szpiegul.pl/blog/o-kanwie-wywiadu-agenturalnego/
12. «Kilka uvag o voynie», Michal Jaskulski. Retrieved from https://core.ac.uk/download/pdf/229244246.pdf
13. Strona internetova Biura Bezpiechenstva Narodovego RP. Retrieved from https://www.bbn.gov.pl/pl/prace-biura/publikacje/inne-wydawnictwa/3545,Biblioteka-BN-Asymetria-i-hybrydowosc-stare-armie-wobec-nowych-konfliktow.html
14. Strona internetova Biura Bezpiechenstva Narodovego RP. Retrieved from https://www.bbn.gov.pl/pl/prace-biura/publikacje/inne-wydawnictwa/3545,Biblioteka-BN-Asymetria-i-hybrydowosc-stare-armie-wobec-nowych-konfliktow.html

15. Strona internetova Biura Bezpiechenstva Narodovego RP. Retrieved from https://www.bbn.gov.pl/pl/prace-biura/publikacje/inne-wydawnictwa/3545,Biblioteka-BN-Asymetria-i-hybrydowosc-stare-armie-wobec-nowych-konfliktow.html
16. The New Generation of Russian Warfare, J. Berzins. Retrieved from https://www.aspen.review/article/2017/the-new-generation-of-russian-warfare/
17. The Russian Military Forum: Russia's Hybrid War Campaign: Implications for Ukraine and Beyond. URL: https://www.csis.org/events/russian-military-forum-russias-hybrid-war-campaign-implications-ukraine-and-beyond
18. «Zagrozhenia militarne a bezpiechenstvo Europy» M. Wrzosek. Retrieved from https://zbrojni.blob.core.windows.net/pzdata/TinyMceFiles/kwartalnik_bellona4_2012.pdf
19. Zeshyty Naukove Akademii Obrony Narodovey nr 2 (99) 2015 ISSN 2299-6753. Retrieved from https://depot.ceon.pl/bitstream/handle/123456789/9904/Banasik,%20Parafianowicz.pdf?sequence=1&isAllowed=y