Bogusław PACEK
Hennadii PIEVTSOV
Anatolii SYROTENKO

CURRENT ISSUES OF MILITARY SPECIALISTS TRAINING IN THE SECURITY AND DEFENCE SECTOR UNDER CONDITIONS OF HYBRID THREATS

Wydawnictwo Instytutu Bezpieczeństwa i Rozwoju Międzynarodowego SDirect24

CURRENT ISSUES OF MILITARY SPECIALISTS TRAINING IN THE SECURITY AND DEFENCE SECTOR UNDER CONDITIONS OF HYBRID THREATS

Instytut Bezpieczeństwa
i Rozwoju Międzynarodowego

Boguslaw Pacek,
Hennadii Pievtsov, Anatolii Syrotenko

CURRENT ISSUES OF MILITARY SPECIALISTS TRAINING IN THE SECURITY AND DEFENCE SECTOR UNDER CONDITIONS OF HYBRID THREATS

Warsaw 2021

Reviewer
Prof. dr hab. Andrzej Glen

Scientific editors:
Boguslaw Pacek – Jagiellonian University in Krakow, Poland
Hennadii Pievtsov – Ivan Kozhedub Kharkiv National Air Force University, Ukraine
Anatolii Syrotenko – National Defence University of Ukraine named after Ivan Cherniakhovskyi, Ukraine

Language editing and proofreading
Foreign Languages Scientific and Research Centre
of National Defence University of Ukraine
named after Ivan Cherniakhovskyi

Computer typing
Valeriya Kirvas

ISBN 978-83-66676-10-7

Wydawnictwo Instytutu Bezpieczeństwa
i Rozwoju Międzynarodowego
https://instytutbirm.pl

1st Edition

CONTENTS

Training of Personnel for Countering Hybrid Threats in Armed Conflicts

PREFACE

In the current military-political situation, Russian Federation and its armed aggression in the east of our country will remain the main source of threats to the security environment of Ukraine and around it in the coming years, but other military threats are not ruled out. Ensuring the military security and defence of Ukraine, readiness of the defence forces to deter armed aggression is recognized as the main strategic direction of the state policy implementation in the field of national security and defence.

Under such conditions, the development of a military education system is of particular importance. According to the latest statements of the top military and political leaders of Ukraine, such a task is a priority for the military institutions and the Armed Forces of Ukraine. The development of military education is a guarantee of increasing the capabilities and combat readiness of all security and defence sector units, which is essentially a prerequisite for security of the state. This determines the search for effective ways, mechanisms and a systematic approach to the training of specialists in the security and defence sector.

We present to your attention a collective monograph "Current issues of military specialists training in the security and defence sector under conditions of hybrid threats", which was developed as a result of the conference held on November 12, 2020 at the National Defence University of Ukraine with the participation of the Directorate of Defence Policy, Department of Military Education and Science of the Ministry of Defence of Ukraine representatives, as well as representatives of higher military educational institutions of Ukraine and partner countries.

The monograph contains publications of the team of authors in the following relevant areas:

Syndicate I: "Military Scientific Aspects of Counteracting Hybrid Aggression: the Experience of Ukraine":

Syndicate II: "Training of Personnel for Countering Hybrid Threats in Armed Conflicts".

In their materials, the authors note that modern military education must meet the requirements for ensuring the quality of specialists training in the security and defence sector based on the introduction of innovations. Today's conditions are increasingly characterized by challenges such as hybrid threats, which in turn accumulate increasing demands on the specialist, who needs to combine knowledge, skills and ability to adapt to work in ever-changing conditions. Therefore, the monograph focuses on the development of the future specialist's professional competence, which in turn necessitates improving the quality of higher education and making adjustments in the training of military personnel for the security and defence sector.

The most important factors that are determined are the conditions for effective training of future military specialists of different levels for their professional activities, the content of education, pedagogical technologies, the personality of the teacher and the organization of the educational and information environment. The main task that the higher military school and a particular higher military educational institution is to train not just specialists but professionals in their field. Such individuals must have military professional knowledge, high professional competence, high spirituality, moral and ethical beliefs, general culture, innovative nature of thinking, a systematic approach to the analysis of complex production situations. They must be capable of adapting to complex modern market conditions, striving to improve and develop themselves and realize personal potential.

Modernization of the military specialists training system for the security and defence sector is carried out in the context of constant revision of views on national security and defence, principles and directions of state preparation for armed protection of national interests, lack of clear and stable parameters for current and projected reduction of the sector, the tasks of the sector, overall and organizational structure, number and validity of units and subdivisions military accounting specialties, etc. It should be emphasized that due to the use of outdated models of weapons and

military equipment, disregard for modern critical aspects of the development of warfare, informational, automated means, methods, technologies of combat operations, higher military education institutions are training specialists in most specialties with considerable holdback from the modern trends in the use of troops (forces). The transition to new didactic principles in the training of military specialists should include: adjustment of target settings (priority of the general goal over those implemented in higher education institutions in relevant specialties, taking into account national interests and national security; officers must consciously approach all political, military and economic, diplomatic and other government decisions to be designed and implemented in the educational process); optimization of military education integration processes with civilian education in the directions of revision of the higher military education standards normative and variable components ratio, military-professional orientation of military specialists training.

The proposed monograph can provide answers to the questions that must be considered for the training of highly qualified specialists in the security and defence sector, who are able to effectively address the challenges and threats in today's hybrid warfare.

The monograph considers various aspects of both the concepts of training specialists in the security and defence sector and the hybrid aggression, summarizes current views on the development of military education and options for combating hybrid threats in this context, and provides methodological and practical recommendations.

Boguslaw Pacek	**Hennadii Pievtsov**	**Anatolii Syrotenko**
Doctor of Social Sciences	*Doctor of Technical Sciences*	*Doctor of Military Sciences*
Professor	*Professor*	*Senior Research Fellow*

MILITARY SCIENTIFIC ASPECTS OF COUNTERACTING HYBRID AGGRESSION: THE EXPERIENCE OF UKRAINE

Victor Bocharnikov
Doctor of Technical Sciences, Professor
Chief Researcher of the Center for Military Strategic Studies
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-4398-5551

Sergey Sveshnikov
Candidate of Technical Sciences, Senior Researcher
Leading Researcher of the Center for Military Strategic
Studies of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-8924-4535

SYSTEMIC FEATURES OF MILITARY-POLITICAL SITUATION IN UKRAINE DURING 2012-2018

We presented an approach to identifying the main systemic features in the military-political conditions and circumstances in which the current conflict originated and took place on the territory of Ukraine during 2012-2018. We also considered the interests of the current military-political subjects, identified the features of the military-political situation and its transformation, the domestic conditions of Ukraine, as well as the general characteristics that were inherent in the conflict.

Keywords: *systemic features, military conflict, military-political situation, aggression, challenges, threats.*

Introduction

Problem statement. The authors consider the systemic features of military-political conditions and circumstances in which the military conflict in Ukraine originated and took place during 2012-2018. The study is based on the results of several research papers on the analysis of the military-political situation (MPS) in the region around Ukraine. The authors tried to observe the events of the conflict from the view-point of an external observer in order to avoid

errors related to the distortion of reality in the conditions of fierce information and psychological struggle.

Each conflict has its own systemic features. But the current conflict in Ukraine has demonstrated a qualitative leap in the forms and methods of using resources by states to achieve political goals.

Purpose of the report was to try to answer the following questions: whether the nature of the goals of states has changed; on what problems the struggle was concentrated; what resources the parties to the conflict preferred; what features took place in the course of the conflict; how we can classify this conflict and on what grounds.

Main part

Methodological principles that we used during the research. The primary sources of conflicts between states are in the environment of military-political relations, which together constitute a MPS [1]. Military conflict is a special state of a MPS, which characterized by antagonistic, irreconcilable contradictions between the subjects with the use of military force. Therefore, the systemic features of conflicts are determined by the elements of a MPS: subjects, their interests, problems of relations, and so on. First of all, it should be noted that the state of a MPS is determined by the actions of the subjects. These subjects include: external subjects (neighboring states, leading world powers, military-political coalitions, transnational corporations) and internal subjects (parties, political and economic blocs, social groups, etc.).

Subjects are the bearers of interests, and interests are the most profound stimulators of the subjects actions and the evolution of a MPS. Subjects often hide their true interests, especially in the information space. Subjects show and specify their interests in partial problems (problematic questions). All problems are closely linked. With the help of intentions, the subjects show their commitment to a specific solution. The actions of the subjects are a continuation of intentions. The subject directs actions either to save or to change the current state of a problem. A subject must have tangible and

intangible resources (political, economic, etc.) to take action. We consider the resource as a stock, a source. Based on tradition, mentality, own evaluation of contradictions, each subject has an individual propensity and will to use the resource. We characterize the propensity and will to use force as aggressiveness. In an effort to solve problems, the subjects take action and enter into relationships with each other. The set of relations on all problems forms aMPS. An important feature of action is their focus: either on the problem, or on another subject as a bearer of other interests. In the case when a certain subject considers another subject as a source of his problems and seeks to destroy it altogether, a military conflict may arise.

Thus, to consider the systemic features of a military conflict, it is necessary to understand three main positions:

1. The main elements of a MPS are: subjects, their interests and goals, relationship problems, available resources and aggressiveness. Therefore, a specific set of these elements determines the systemic features of a military conflict.

2. Since the main stimulus for the evolution of a MPS is the interests of the subjects, a necessary condition for the emergence of conflict is their antagonism and intransigence, i.e. the impossibility of resolving peacefully.

3. In order to consider a MPS and analyze the causes of military conflict, we should consider relations on all issues (including economic, energy, etc.), but in the context of the use of military force by the subjects of relations against other subjects.

The main results of research. The main actors in the MPS in the region around Ukraine were and are the United States of America (USA) and the Russian Federation (RF), as well as the European Union (EU) [2]. These subjects had the following interests in the region.

The US interest can be considered to prevent the unioning of advanced EU technologies, almost unlimited natural resources of Russia and human resources of China, including by creating a controlled buffer of Eastern European countries (including Ukraine), which would separate Russia and the EU and would disrupt trade

flows between them and between the EU and China [3–4]. Control of such a buffer will allow the United States:

– effectively deter geopolitical competitors;

– control the European consumer market;

– demonstrate the grounds to increase the cost for arms procurement, modernization of military infrastructure;

– to form a positive attitude to tough sanctions that hinder the rapprochement of the EU and Russia;

– to deter the Russian Federation and divert its resources with the help of supporting a hostile for the RF neighboring state.

In this sense, Ukraine's adherence to the pro-Western course is in the long-term interests of the United States, including in terms of strengthening influence in the Black Sea region.

The EU's interests are largely economic. From the viewpoint of European interests, Ukraine is a transit link for Russian energy sources, as well as one of the potential land routes to the East. Ukraine's adherence to the pro-European course [5] in politics and economics is in the long-term interests of the EU, as it provides control over transit infrastructure, a big consumer market and natural resources.

The main long-term interest of the RF [6–7] can be considered to ensure the favorable political and economic course of Ukraine. Ukraine's neutral military-political course suits Russia, as it guarantees the absence of hostile military bases on its territory. The current goals of the Russian Federation in attitude to Ukraine can be considered the weakening of the central government and ensuring the neutral status of Ukraine, greater economic and political autonomy of its regions.

Systemic features of the MPS in the region around Ukraine on the eve of the conflict (early 2012 - late 2013). Ukraine has played a key role in the region as an object of influence of leading states [8]. This shows the composition of the priority problems of international relations: the choice of the integration vector by Ukraine; interference in the domestic affairs of Ukraine; transportation and consumption of Russian energy sources; the problem of foreign military presence.

The composition of these problems is an important systemic feature of the MPS at the beginning of the military conflict in Ukraine. We can also note the following:

– the use of military force against Ukraine in the direction of its internal division was considered as more possible on the eve of the conflict [9];

– all current military-political subjects perpetrated actions that showed signs of military-political challenges. Some actions showed signs of diplomatic (on the part of Western states) and economic (on the part of the RF) threats;

– actions that showed signs of a threat of military force were absent in the open information space.

Systemic features that characterized the domestic conditions of Ukraine and influenced the situation at the end of 2013:

– domestic economic conditions on the eve of the conflict were constantly complicated [10], the top leadership of Ukraine considered the possibility of default [11];

– the global financial and economic crisis of 2008 had a catastrophic effect on Ukraine's export-oriented economy;

– in 2012-2013 the United States and Russia polarized military and political activity in the region around Ukraine. These states have increased pressure for Ukraine to make an integration choice. This exacerbated domestic socio-political instability;

– there was no internal public consensus on the choice of Ukraine's military-political course [12], the priorities of the population in eastern and western Ukraine were diametrically different.

Systemic features of the MPS in the region around Ukraine during the conflict beginning (early 2014 - early elections of the President of Ukraine):

– the United States and the European Union have taken concerted action of a political nature: warnings to the current leadership, support for the political opposition, etc. The EU has been more active. The main question for the EU was Ukraine's signing of an association agreement;

– immediately after the transfer of power to the opposition, the Russian Federation defined the situation as a violent overthrow of the current government. To overcome the political crisis, Russia has proposed creating a free trade zone between the EU and the Customs Union, holding early presidential elections in Ukraine, and making Ukraine a federation. These proposals did not find support, especially from the EU;

– Western states recognized the legitimacy of the new government. They understood the difficult financial situation of Ukraine, but the declared huge amount of assistance in practice was reduced significantly;

– Western states have classified the actions of the Russian Federation in the Crimea as an intervention. The United States and the European Union have announced sanctions, although they have not curtailed cooperation with Russia in important sectors of the economy;

– the Russian's parliament authorized the President of the Russian Federation to use the Armed Forces on the territory of Ukraine;

– Western countries supported Ukraine mainly through political statements, political and economic sanctions against Russia, but refused to provide direct military support, although they intensified military exercises and began to increase their military presence on eastern borders and in the Black Sea;

– Western countries also refused to supply weapons to Ukraine. EU politicians advised Ukraine to react with restraint to the occupation of Crimea;

– Russia's actions were focused on the occupation of Crimea [13]. Russia has recognized the new President of Ukraine and has not contradicted the EU regarding the introduction of a reverse scheme for natural gas supplies to Ukraine.

System features of the transformation of the regional MPS during 2012 – 2018:

– regional military-political relations were focused on the problems of interference in the domestic affairs of Ukraine, territorial

questions, the fight against corruption and the resolution of the conflict in eastern Ukraine;

– we clearly observed the cyclical evolution of the conflict. After the initial period, the conflict drags on, none of the parties can secure their interests, but does not want to get out of the conflict (otherwise it would be tantamount to admitting defeat), the conflict is postponed until one of the opponents weakens or makes a fatal mistake;

– regarding the transformation of the actions nature of influential subjects, there are two periods: before 2014 and after it.

During the first period:

– Russia conducted mainly domestic and, to a lesser extent, international negotiations;

– the United States and the European Union used a policy of maneuvering and waiting, as well as sanctions.

– After 2014:

– Russia has ceased to demand negotiations at the international level, counteracted Ukraine, did not recognize its position, used means of active counteraction, including sanctions;

– the United States and the European Union have maintained a policy of maneuvering and waiting, as well as have demonstrated a neutral position and promoting consideration of questions in negotiations between the parties.

The nature of actions and intentions of military-political subjects [14–15]. Only the Russian Federation carried out actions that can be classified as armed aggression:

– occupation of Crimea;

– sending the Russian Federation to the territory of Ukraine of armed groups of regular and irregular forces;

– support of illegal armed formations (IAF) in the east of Ukraine by means of fire damage by units of the Armed Forces of the Russian Federation;

– blocking the passage of Ukrainian ships to ports on the coast of the Azov Sea.

Also, only the Russian Federation carried out actions that can

be classified as a military threat:

– requirements for changing the constitutional system of Ukraine;

– threats of violation of the territorial integrity of Ukraine;

– direct preparation for the use of military force against Ukraine (building up military groups near the state border of Ukraine, military exercises, etc.);

– deprivation of Ukraine of control over some sections of the state border;

– comprehensive assistance to the IAF in eastern Ukraine.

All influential subjects carried out actions that can be classified as military-political challenges.

Systemic features that were inherent in the conflict as a whole:

– the Ukraine's parliament legitimized the results of the political confrontation between the government and the opposition. States that were on the side of the opposition immediately recognized the legitimacy of the new government;

– during the change of government, national minorities tried to gain more rights in exchange for their support of the new government;

– the Law of Ukraine "On Defense of Ukraine" unambiguously classifies the actions of the Russian Federation in the Crimea as an act of aggression [14];

– in eastern Ukraine, local activists, non-resident citizens of the Russian Federation and representatives of its special services provoked resistance from the population;

– IAF participants received weapons first through the seizure of weapons of the security forces of Ukraine, and later through to the supply of weapons from the Russian Federation;

– Ukraine's security forces were unprepared for action in the situation after the occupation beginning of the Autonomous Republic of Crimea. Until 2014, state bodies did not consider the possibility of applying the Armed Forces of Ukraine within the state;

– the preparation of the RF Armed Forces for the occupation

of Crimea was covert, well-calculated and organized;

– since the beginning of the conflict, all influential states have increased their military presence near the borders of Ukraine, intensified military exercises;

– the evolution of the conflict has clearly demonstrated that a contract army cannot guarantee success in the event of a military conflict on its own territory;

– the UN Security Council, as an international format for resolving conflicts [16], has been transformed into an arena of information and psychological struggle, mainly between the United States and Russia. Attempts to resolve the conflict with the help of peacekeeping forces were unsuccessful;

– the conflict can be called strange. Ukraine declared Russia an aggressor, but refused to sever diplomatic relations with it, completely suspend trade and block border crossings.

General characteristics of armed conflict:

– armed struggle had the following features:

– the main task of the Armed Forces of Ukraine was to take control over the state border with Russia. This task was not completed;

– significant losses of objects in civil infrastructure, livelihoods and the economy;

– the only line of contact was missing;

– due to the proximity of the combat zone to the border with the Russian Federation at the beginning of the conflict, the fighting of the IAF was supported by the fire of the Russian Armed Forces from abroad, without direct combat clashes.

– active use of artillery and limited

– the conflict has the characteristics of a proxy war. Leading states deny their involvement in hostilities, but antagonism between interests is the main cause of military conflict;

– the actions of the parties to the conflict are of a hybrid nature. The parties are engaged in confrontation mainly in the information-psychological and economic spheres. The intensity of action directly in the military sphere is relatively small. Special

actions of the armed forces are important;

– the conflict has signs of a network war. The use of information and psychological influences is aimed at disorienting the population and changing its worldview;

– the conflict has the characteristics of a privatized war, as there are financial interests of corporations, influential politicians or individuals.

Conclusions

Thus, the main systemic features of the military conflict in Ukraine allow us to understand the main driving forces of the conflict, its features in the current military-political situation, to get closer to understanding the measures needed to resolve the conflict. We have analyzed the questions of this report in more detail in monographs, research papers and scientific articles.

References

1. Bocharnikov, V., Sveshnikov, S., Timoshenko, R. and Pavlenko, V. (2019), "*Tekhnolohiia analizu viiskovo-politychnoi obstanovki*" [*Technology of analysis of the military-political situation*], The National Defence University of Ukraine named after Ivan Chernyakhovsky, Kyiv, 384 p.

2. Sveshnikov, S. and Bocharnikov, V. (2018), "*Dovhostrokovyi prohnoz voenno-politychnoi obstanovki v rehioni dovkolo Ukrainy na osnovi analizu heopolitychnoi konkurentsii*" [*Long-term forecast of the military-political situation in the region around Ukraine based on the analysis of geopolitical competition*], The National Defence University of Ukraine named after Ivan Cherniyakhovskyi, Kyiv, 100 p.

3. Hafeznia, M.R., Ahmadi, S. and Hourcad, B. (2013), Explanation of the Structural and Functional Characteristics of Geographical Buffer Spaces, *Geopolitics Quarterly*, Vol. 8, Issue 4 (28), pp. 1-40, available at: https://cutt.ly/0ki8Obi (accessed 22 October 2020).

4. Chay, J. and Ross, T.E. (1986), *Buffer States in World Politics*, Westview Press, Boulder.

5. The Ukraine's government portal (2014), "*Uhoda pro asotsiatsiiu mizh Yevropeiskym Soiuzom ta Ukrainoiu*" [*Association*

Agreement between the European Union and Ukraine], available at: https://cutt.ly/yki8Zn0 (accessed 22 October 2020).

6. Svarin, D. (2016), The construction of 'geopolitical spaces' in Russian foreign policy discourse before and after the Ukraine crisis, *Journal of Eurasian Studies*, Vol. 7, Issue 2, pp. 129-140, available at: https://cutt.ly/fki8Mhe (accessed 22 October 2020).

7. Pabst, A. (2010), President Medvedev's Project of Modernization, *Media website "HUFFPOST"*, available at: https://cutt.ly/pki83Z0 (accessed 22 October 2020).

8. Website of the "eTurboNews" (2013), *EU cannot lose Ukraine*, available at: https://cutt.ly/fki4woD (accessed 22 October 2020).

9. Hoyle, B. (2013), Russia threatens to back Ukraine split, *Website of "Yalta European Strategy"*, available at: https://cutt.ly/Mki4aiK (accessed 22 October 2020).

10. The Statistical Service of Ukraine (2020), "*Ekonomichna statystyka. Zovnishnoekonomichna diialnist*" [*Economic statistics. Foreign economic activity*], available at: https://cutt.ly/Oki4KQD (accessed 22 October 2020).

11. The Ukraine's government portal (2011), "*Premier-ministr Ukrainy Mykola Azarov vziav uchast u prohrami "Ispyt na vladu" na Pershomu natsionalnomu kanali*" [*Prime Minister of Ukraine Mykola Azarov took part in the "Exam for Power" program on the First National Channel*], available at: https://cutt.ly/6ki4MW9 (accessed 22 October 2020).

12. Website of the "The week mirror" (2013), "*Reghyonal Kolesnychenko predlozhyl Rade zakonoproekt ob otkaze Ukrayny ot kursa evroynteghracyy*" [*Regional Kolesnichenko proposed to the Rada a bill on Ukraine's rejection of the course of European integration*], available at: https://cutt.ly/ski7f3G (accessed 22 October 2020).

13. Mereshchuk, V. (2019), "*Yak Rosiia zakhopyla Krym. Khronika podii*" [*How Russia captured Crimea. Chronicle of events*], available at: https://cutt.ly/Tki7x3k (accessed 22 October 2020).

14. The Law of Ukraine (1991), "*Pro oboronu Ukrainy*" [*On Defense of Ukraine*], available at: https://cutt.ly/uj0qedO (accessed 25 January 2021).

15. President of Ukraine (2015), "*Ukaz Viiskovoi doktryny Ukrainy*" [*Decree of the Military doctrine of Ukraine*], available at: https://cutt.ly/zj0qgWI (accessed 25 January 2021).

16. The UN Security Council (2015), *Resolution 2202*, available at: https://cutt.ly/iki7RjD (accessed 22 October 2020).

Volodymyr Bohdanovych
Doctor of Technical Sciences, Professor
Principal Scientific Research Fellow of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-0481-9454

Oleksandr Dublian
PhD (Military Sciences)
Leading Scientific Research Fellow of the Central Research Institute of the Armed Forces of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0001-5129-3913

Oleksandr Peredrii
PhD (Military Sciences)
Head of the Department of Central Research Institute of the Armed Forces of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0003-2877-4959

Valerii Dobrohurskyi
Deputy Commandant of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-5263-6102

COMPREHENSIVE MODEL OF COUNTERACTING HYBRID AGGRESSION PROCESS

The proposed Comprehensive Model of Counteracting Hybrid Aggression Process is a framework for assessing the process of combating hybrid threats. It enables to assess the origin and level of danger from the applied complex of hybrid threats to the key areas of national security. The Model is considered to be a tool for reasoning the structure and management strategy to counteract hybrid threats, as well as to build possible scenarios for the development of the environment, forecasting, use of resources and strategic planning.

The Comprehensive Model of Counteracting Hybrid Aggression

Process is considered to be a formal theory, structuring the system of combating hybrid aggression, its tasks, models of behaviour and decision-making in conditions of variability and uncertainty of the external security environment.

Counteracting the hostile states' hybrid aggression implies a set of measures in the security and defence sector of Ukraine, which is responsible for national security and tasked with neutralizing the destructive impact of identified hybrid threats or their de-escalation to an acceptable level.

The main objectives of Counteracting Hybrid Aggression System are the following: to minimize the expected destructive levels of hybrid threats implementation in the key areas of national security; to preserve the image of the state on the international arena; to preserve best advantage of the State military-political leadership image in the conditions of purposeful hybrid attacks or operations; to prevent violation of socio-political stability within the state; to save resources involved in neutralizing destructive hybrid threats; to descredit the State-aggressor in the international public eye.

Keywords: *hybrid aggression, hybrid threat, combating/counteracting, counteraction system, model, national security, information-psychological impact, special information operation.*

Introduction

Problem statement. The report is devoted to the general problem of ensuring the national security of the state in the conditions of intensive information and psychological confrontation.

Until recently, the protection of their geopolitical interests through wars was carried out by traditional armed means using regular armies. The character of the wars of the XXI century. is that traditional weapons are no longer leading, but the role of such tools as political, diplomatic, economic, informational, ideological, psychological, humanitarian, intelligence, which are often more effective and more destructive [1–2].

Modern wars, called hybrid wars, are characterized not by the means used, but by the goals achieved, comparable to the goals usually pursued in traditional wars, such as destruction, looting, occupation, regime change, immersion in chaos. One of the most

important differences of the hybrid war is that its goal is not so much to seize territories and natural resources, but to control the mood of the citizens of the opposing country by controlling the information space and "brainwashing" in the occupied territories [3–4].

Through the technologies used at the present stage, the above-mentioned goals can be achieved without the use of lethal weapons. Therefore, the organization of counteracting such technologies is an urgent scientific task.

The analysis of recent researches and publications. Special information operations conducted against strategic decision-makers and the image of the state are partially described in [5–6] but the description is only verbal and does not allow to investigate these operations using modern methodological apparatus and modeling.

Purpose of the report is to highlight the main provisions for the *Comprehensive Model of Counteracting Hybrid Aggression.*

Main part

The use of the *Comprehensive Model of Counteracting Hybrid Aggression Process* (CMCHAP) contributes to the assessment of the nature and the level of risk of the hybrid threat (HT). It constitutes the instrument to substantiate the structure and the strategy to manage the processes of the HT resistance and to identify the possible scenarios of the evolution of situation, anticipating, using the resources and the strategic planning.

We are going to understand the CMCHAP as the formalized theory, that can be used as the base for the substantiated structure of the hybrid aggression (HA) resistance, its tasks, the types of the behavior and the decision-making under the variability and uncertainty of the external environment.

The resistance to the HA from the hostile states constitutes for Ukraine the complex of measures being taken by the subjects of the Ukrainian security and defence sector, that deals with the providing of national security as for the neutralization of the destructive impact of the revealed hybrid threats or this impact de-escalation to the allowable level.

The CMCHAP (hereinafter the Model) has to be adequate to this complicated phenomenon and to reflect the multi-dimensional nature of the HA, whose operations are directed to the principal spheres of the target states functioning.

It is reasonable to determine the following tasks of the system of countering hybrid aggression (HA) [7]:

– to minimize the expected destructive levels of the realization of the HT in the governing spheres of the national security (to neutralize the revealed HT at the lowest loss for the state);

– to save as much as possible the image of the state in the international scene;

– to save as much as possible the image of the state military and political leadership (within the country and abroad) under the conditions of the deliberately undertaken attacks or operations;

– not to allow the disrupting of the socio-political stability within the state;

– to keep the relations with the strategic partners and allies, to prevent the harming of their image;

– to minimize the resources used to neutralize the destructive hybrid threats (HT);

– to discredit the state that acts as a source of the HA to the international community.

The CMCHAP has to be informationally compatible with the system of the support of the Main Situation Center decision-making process [5]. The algorithms that are implemented in the Model must be open to the new HT, their assessment and the substantiation of the measures as for the organization of combating in the system of the national security ensuring.

The Model has to ensure the development of several scenarios of the HT exploitation and the modeling of each of them in full. The Model also has to react simultaneously on the several indicators of HA as well as to demonstrate the result of the influence of the indicator chosen by the analyst.

However, we must keep in mind that the developed model of

the revealed HA will have, in certain extent, the conventional nature because it is not able to cover all the aspects of the situation learned. It acts only as an instrument to concentrate the efforts of the analyst on the identification of the principal intrinsic features as the basis for the future substantiation of the most reasonable project of the managerial decision as for the organization of the HA resistance. The proposed structure of the subsystem of the HA resistance of the system of military security ensuring is shown in Fig. 1.

At the first step of the Model the identification of the destructive events, phenomena and threats is carried out.

To reveal the signs of the HA under the restricted resources it is reasonable to connect the appropriate structural subdivision of the resistance subdivision to the state monitoring system in the political, economic, military, informational, cultural and ideological (philosophical, attitudinal) spheres (mandatory spheres).

In the political sphere the special attention is drawn to the attempts to undermine the image of the military and political leadership of the state, to weaken the defence capabilities of the state through the targeted actions and against the military-industrial complex, to accuse the state authority in the excessive military expenditures, to create the contradictions between the producers and customers of military products in the country and abroad. Actually, reducing the prestige of military service, destroying the dynamics of political attitude in society, as well as the protests against the ongoing reforms (reforms), damaging the political image of the state at the international level, etc. are accented.

In the economic sphere, the attempts to impose economic sanctions against the state, undermine the competitive capabilities of the country's products in foreign markets, disorganize the banking system by conducting cyber attacks, creating obstacles in the work of banks, forming protest sentiments by manipulating socio-economic data, are analysed in detail.

In the military sphere, HA measures are aimed at achieving unilateral advantages by misleading the Target State, especially in the collection, processing and use of intelligence, disrupting the

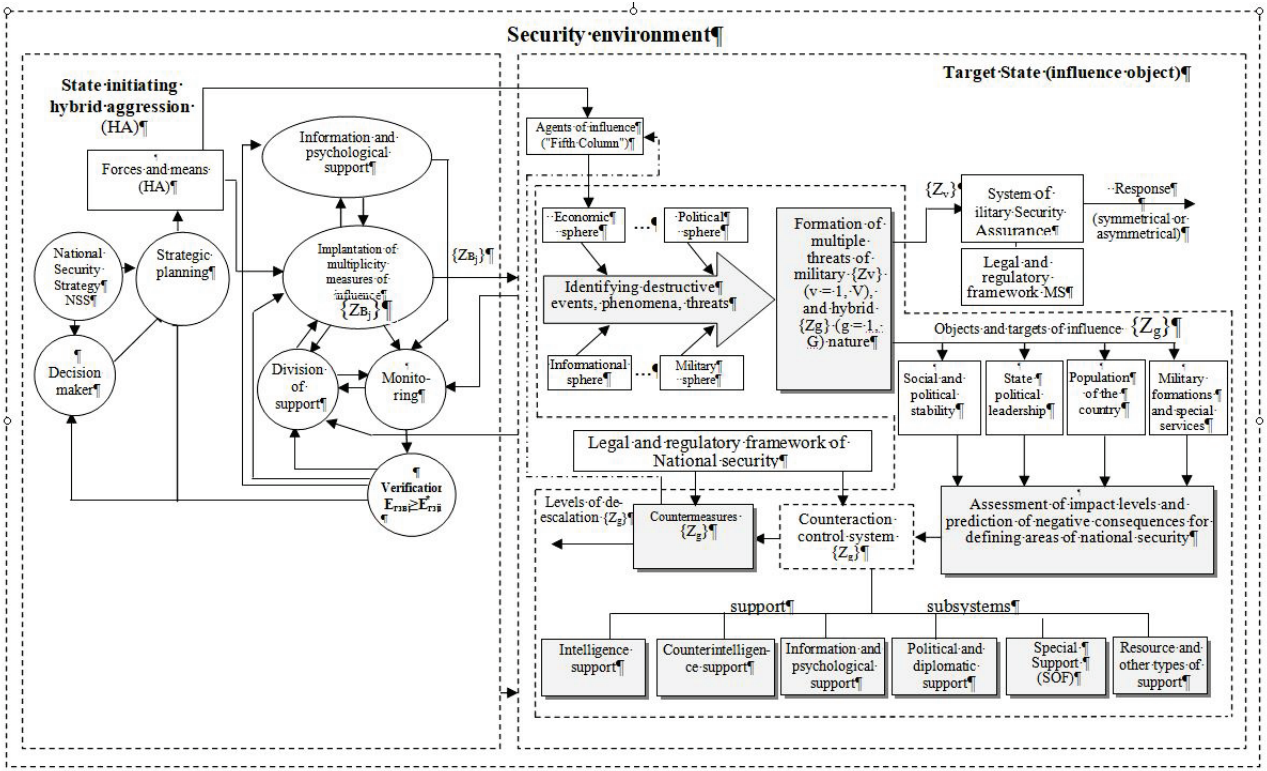

Fig. 1. Version of the complex model structure of the countering hybrid aggression process

stability of the country's critical infrastructure and government and armed forces management systems, including cyber impact on vulnerability.

In the information sphere, HA manifests itself most "powerfully". Information and information-psychological influences are carried out through the information sphere of military security, causing significant damage in other areas (military and military-technical cooperation, foreign economic activity of the Ministry of Defence of Ukraine, during the export of weapons and military equipment, etc.). Part of information threats (IT) at the final stage of their action is transformed into other threats that are inherent in one or another sphere of the state's military security. For example, the powerful informational and psychological influence of the enemy on the personnel of combat units can lead to panic and, as a result, the units leave the battlefield, which ultimately leads to the defeat of our troops in a certain area. In this case, information threats, affecting the military sphere, are transformed into military threats and lead to military losses. Thus, information threats to the state in the military sphere are a "complex" type of threats, they have a specific character of manifestation and, therefore, require a more thorough study, building their models and organizing counteraction.

In the cultural and ideological sphere, a key place is given to the HT, associated with the conduct of information warfare in order to achieve various political goals. Recently, the leading factor is the secondary occupation of enemy territory and the seizure of resources as opposed to the task of establishing strategic, comprehensive control over the consciousness of the Target State population and gaining full power over the future of the conquered state.

In this context, it should be noted the use of the mass media to disseminate false, inaccurate information, Internet trolling against iconic figures in politics, business community and in cultural life. HT are increasingly used in the cultural and ideological sphere to realize their interests in the world, inciting various conflicts, which later become a source of war, armed extremism and international terrorism. In general, the implementation of HT within the

framework of the strategy of information confrontation becomes a key component of the technology of "controlled chaos" in the cultural and ideological sphere [8]. It allows to capture strategic initiative in the course of hybrid attacks, subjugate the population the armed forces of the Target Country to external control influences and thus deprive the Target State of de facto sovereignty without seizing its territory by military force.

The second step of the Model is filtration and formation of sets of military $\{Z_v\}$ and hybrid $\{Z_g\}$ threats. Counteraction to military threats is carried out by known methods of symmetric and asymmetric response [7]. Filtration of hybrid threats is carried out using the expert survey method in two stages. At the first stage, a common set of non-military threats is formed. At the second stage, this set is transformed into four groups:

– the threats aimed at undermining social and political stability $\{Z_{sps}\}$;

– the threats aimed at discrediting the military-political leadership of the state $\{Z_{vpk}\}$;

– the threats against the country's population $\{Z_{nas}\}$;

– the threats directed at the personnel of military formations and special services $\{Z_{os}\}$.

The third step of the Model using the M7 model [9], enables the experts to assess the levels of impact and predict the expected negative consequences for key areas of national security.

In the fourth step, the information is transmitted into the countermeasures management system. The relevant management decisions on counteraction, individual tasks of the subjects involved in counteraction are substantiated, comprehensive support of counteraction measures is organized under the current legal framework of national security. Making management decisions on the implementation of specific countermeasures it is necessary to ensure the sufficient levels of de-escalation of the identified impacts on certain objects of aggression.

Conclusions

The developed Comprehensive Model of Counteracting Hybrid Aggression Process (CMCHAP) is a formalized theory which enables to substantiate the structure of the counteraction system of the detected hybrid aggression (HA) i.e. its tasks, types of behaviour, and decision-making in conditions of the external environment variability and uncertainty.

Counteracting HA of unfriendly states for Ukraine is a set of measures taken by the security and defence sector of Ukraine to ensure national security, to neutralize the destructive influence of identified hybrid threats, or its de-escalation to an acceptable level. Hybrid threats have the most significantly damaging impact on political, economic, military, informational, cultural, and ideological spheres.

The Model of detected HA will always be notional since it cannot cover all aspects of the situation under studied. It is considered as a tool to focus the analyst's efforts on distinguishing the main essential characteristics, and find the most reasonable project management solutions to start counteraction.

References

1. Hracheva, T.V. (2009), "*Nevydymaia Khazaryia. Alhorytmy heopolytyky y stratehyy tainykh voin myrovoi zakulys*" [*Invisible Khazaria. Algorithms of geopolitics and strategies of secret wars of the world behind the scenes*], Zerna, Riazan, 400 p.

2. Bartosh, A.A. (2018), "Trenie i iznos hibrydnoyi viyny" [Friction and wear of hybrid war], *Military Thought*, No. 1, pp. 5-13.

3. Mahda, Y.V. (2016), "Zahrozy hibrydnoi viiny dlia yevropeiskoi intehratsii Ukrainy" [Threats of a hybrid war for the European integration of Ukraine], *Stratehichna panorama*, No. 1, pp. 61-65.

4. Lytvynenko, O.V. (2003), "*Informatsiini vplyvy ta operatsii"* [*Information influences and operations*], NISD, Kyiv, 240 p.

5. Bohdanovych, V.Y., Romanchenko, I.S., Svyda, I.Y. and Syrotenko, A.M. (2019), "*Metodolohiia kompleksnoho vykorystannia viiskovykh i neviyskovykh syl i zasobiv sektora bezpeky i oborony dlia*

protydii suchasnym zahrozam voiennii bezpetsi Ukrainy" [*Methodology of integrated use of military and non-military forces and means of the security and defense sector for countering contemporary threats to Ukraine's military security*], NDU U, Kyiv, 268 p.

6. Bohdanovych, V.Y., Syrotenko, A.M., Vovchanskyi, V.I. and Pryma, A.M. (2019), "Novi "labirynty" bezpekovoho seredovyshcha ta yikh vplyv na zabezpechennia voiennoi bezpeky derzhavy" [New "labyrinths" of the security environment and its impact on ensuring the military security of the state], *Science and Technology of the Air Force of Ukraine*, No. 2(35), pp. 9-15. https://doi.org/10.30748/nitps.2019.35.01.

7. Bohdanovych, V.Yu. and Vysidalko, A.L. (2015), "Metodyka avtomatyzovanoho modeliuvannia ekspertno-analitychnykh stsenariiv vyiavlennia ta usunennia zahroz realizatsii natsionalnykh interesiv" [Methodology of the automated design of the expertly-analytical scenarios of the exposure and removal of the threats of the realization of the national interests], *Science and Technology of the Air Force of Ukraine*, No. 3(20), pp. 21-29.

8. Vlasyuk, O.S. and Yavorska, G.M. (2016), "Stratehichna adaptatsiya NATO do novykh bezpekovykh vyprobuvan: optsiyi dlya Ukrayiny" [Strategic adaptation of NATO to new security tests: options for Ukraine], *Strategic Panorama*, No. 1, pp. 19–25.

9. Saaty T.L. (2008), "*Pryniatye reshenyi pry zavysymostiakh y obratnykh sviaziakh: Analytycheskye sety*" [*Dependency and Feedback Decision Making: Analytical Networks*], LKY, Moscow, 360 p.

Alexandru Herciu
PhD, Professor
Director of Postgraduate Studies School
of Command and Staff College "Carol I[st]"
National Defence University of Romania
Bucharest, Romania
https://orcid.org/0000-0003-1590-7417

RISKS, THREATS AND PECULIARITIES OF CONTEMPORARY HYBRID CONFLICTS

The study of technical documents shows that special attention has been recently paid to the hybrid conflict concept in the new geopolitical and geostrategic context. Thus, several ideas express the word hybridity, emphasizing in this sense, the concepts of multimode, multidimensional, mosaic, proxy or ambiguous war. Starting with 2009, the concept begins to be used more and more by US military theorists, then taken over and put into practice by the Russian Federation in the aggression against Ukraine in 2014. From that moment, the hybrid conflict becomes a certainty and a reality that determines the adoption of appropriate measures, policies and strategies to counteract, at national, regional, or of politico-military alliances level. Although various concepts are used in this field, we appreciate that this type's physiognomy and characteristics are similar, essentially referring to hybrid military operations.

Keywords: *hybrid risks and threats, hybrid conflict, hybrid war.*

Introduction

The dynamic evolution of the war phenomenon from its classical-conventional physiognomy through its physical dimension to a predominantly unconventional and asymetric one, manifested significantly in particular environments (cyberspace, electromagnetic, information, chemical, biological, radiological and nuclear, human psyche) nowadays and in the foreseeable future, is the consequence of the continuous adaptation to the complexity of the challenges that are manifested today towards humanity, challenges expressed and consecrated in the specialized literature by

the terms: hybrid risks and threats.

The novelty in the analysis of the security environment is induced by the transition of conflicts from a conventional, consacrated type (in which the rules are clear, the laws are written, and the weapons are classic and visible) to a hybrid one (for which there is no legal provisions based on which they can be sanctioned and no theoretical fundamentals). Previous experiences that serve as lessons learned are insufficient. Thus, the study and analysis of recent contemporary warfare trends involve launching scenarios and intuitively predicting future events.

Problem statement. The shaping and awareness of a new type of conflict physiognomy have led to intense debates among theorists and military decision-makers. The new paradigm has generated currents of opinion and a modern philosophy regarding the operations process (planning, preparation, execution, and evaluation) in the contemporary operational environment, namely the comprehensive approach. This concept aims to identify, integrate, and engage in a coordinated manner with the most diverse conflict resolution capabilities. These capabilities must be specialized to counteract the multiple risks and threats that intertwine, generating a new, hybrid outcome that manifests itself in all their specific environments.

The analysis of recent research and publications. It is necessary to understand the "hybrid" concept in the security environment analysis in these circumstances. In a broad sense, the term is used to define those concepts that combine different elements without necessarily having a logical link of association. The notion of "hybrid" has its origins in analyzing the evolution of conflicts in the post-Cold War period. In 2007, in a study that addresses this issue for the first time, analyst Frank G. Hoffman pointed out that the contemporary security environment involves the simultaneous use of several types of warfare by opponents who understand that success can come from combining actions that can take different forms, designed to achieve specific goals, at a given time, calling these conflicts "Hybrid Wars" [1].

Thus, the novelty in the way of designing and conducting hybrid wars consists in the ability of actors (state, non-state, or even mixed combinations - composed of both state and non-state actors) to synchronize several power tools in a synergistically, intentionally exploiting vulnerabilities identified in the opponent (which may belong to all sectors: political, military, economic, social, informational or infrastructure), to achieve the desired effects. These actions are designed so that they are as difficult to detect as possible and therefore have a low degree of probability of responses from the opponent. Thus, so far, researchers in the field have concluded that the most appropriate method of counteracting new threats is the proactive approach, involving anticipation, by carefully following all the indicators considered in analyzing the security environment.

The purpose of report. The research effort was focused on identifying instruments to counter threats, and at the level of the armed forces in designing a tailored formation, capable of carrying out military actions in a hybrid environment.

In this broader context, there is an urgent need to nominate suitable tools for forecasting, timely identification, and monitoring of hazards, risks, and threats to prevent their occurrence, through the combined use of military and non-military means, across the spectrum of the environment confrontation in which they manifest.

Therefore, this article aims to facilitate the understanding of the complexity of the current operational environment and the components that determine the hybrid character of military action. This approach is necessary for the context of the emergence and development of new forms of aggression, influence, and coercion as a result of a kaleidoscope of conventional and unconventional components.

Main part

Reflections on the "hybrid conflict" concept. *Conflict.* The term "conflict" has its origin in the Latin word "conflictus", meaning "shock, hit", later taken over by the French language in the form of the word "conflict". The term defines a state of tension (antagonism,

quarrel, discussion) with a certain intensity (violence). Dissension manifests itself in a disagreement or a confrontation due to misunderstandings, clashes of interests, discord, and divergences of ideas or principles. When the state of tension between the actors involved heightens and reaches maximum violence levels, it means armed conflict. This expression expresses a dispute between two or more actors (state or non-state), a clash between two armed forces, possibly different countries. Then the armed conflict acquires an international character of battle or war.

Conflict arises when the parties involved each pursues the attainment of material or subjective, common-desired or different objective, to fulfill which they enter into a situation of competition or incompatibility [2]. That is why the state of conflict requires at least two parties involved, in opposite attitudes and which involves physical or virtual contact.

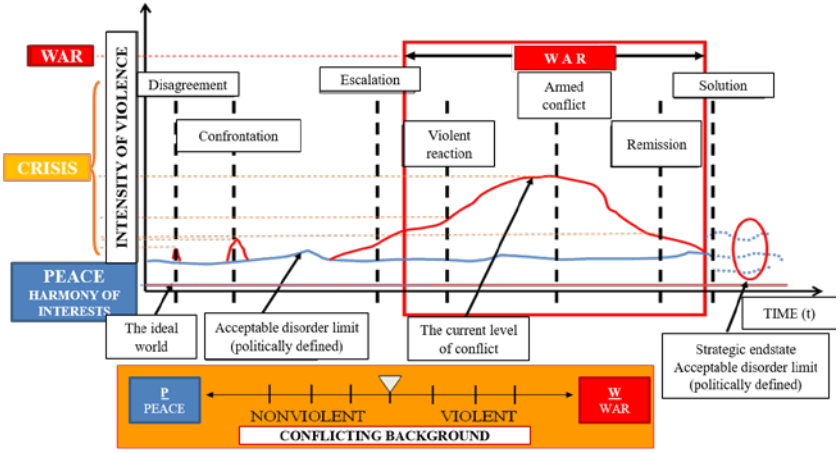

Fig. 1. The states of conflict's manifestation [3, p. 18]

At the social level, the conflict has been defined as "a contextual phenomenon determined by the clash between the interests, concepts, and needs of individuals or groups when they come into contact and have different or seemingly different goals" [4].

Hybrid. The term “hybrid” comes from the Latin “hybrida”, later taken over in French as “hybride” and is used in biology, especially in forestry, to describe a product obtained by crossing two different varieties of living organisms. The term was taken over in other activity fields with a symbolic meaning to define notions (conception, idea, deed) resulting from disparate elements, not organically linked [5].

Used as an adjective, the term “hybrid” characterizes a concept without harmony, resulting from different elements belonging to several categories, other classes, heterogeneous, disparate elements [6]. In the military field, the term has recently been taken over and used to characterize the growing complexity of the war phenomenon, the multitude of actors involved, the obscurity, mixture, and combinations between them. While the existence of an innovative adversary is not a new issue, the “hybrid perspective” approach to recent and ongoing conflicts requires engaged forces to prepare for a broader range of challenges, which recently they were not specific to the military.

Hybrid conflict. In an attempt to describe the dynamics, physiognomy, and evolutionary trends of the conflict, military literature abounds in attempts to define “hybrid conflict” or “hybrid warfare”. From a hybrid perspective, this approach has emerged as a need to explain the multitude of dangers, risks, threats, and actors that manifest themselves today in the operational environment. This situation requires a tailored force, adaptable, and flexible response.

Theories of hybrid conflict. Generally speaking, the phrase “hybrid conflict” is used in the military literature to define a military strategy that encounters elements specific to conventional, unconventional, and asymmetric war:

Col. Jack McCuen (US Army) defines hybrid warfare as the quintessence of asymmetric warfare, waged on three decisive battlefields: (1) among the population in the conflict area, (2) in front of one’s nation, and (3) the international community [3, p.18]. In the same vein, Robert O. Work (US Navy) states that hostile forces would use “hybrid warriors” hidden in civilian populations [3, p.18].

Ltc. Bill Nemeth (United States Marine Corps) defines hybrid warfare as “the contemporary form of guerrilla warfare”, which “uses both modern technology and modern methods of mobilization” [3, p.18].

David Kilcullen, the author of “Accidental Guerrilla Warfare: How to Fight Small Wars Inside a Big One”, asserts in the book launch interview that hybrid war is the best explanation for modern conflict, and emphasizes that it includes a combination of irregular war, civil war, insurgency, and terrorism [7]. The author analyzes today’s conflicts as representing a complex of associated elements: local social networks, global movements, traditional and postmodern cultures, local insurgents seeking autonomy, and a broad pan-Islamic campaign.

Conflicts thus become a “complex hybrid of trends” that dilutes the distinction between “local” and “global” and thus exponentially amplifies and complicates the challenges in the operational environment.

Journalist Frank G. Hoffman defines hybrid warfare as “any enemy that simultaneously and adaptively uses the complex combination of conventional weapons, irregular war, terrorism, and criminal behavior in the fighting space to achieve its political goals” [8].

Nathan Freier (Center for Strategic and International Studies) was one of the key people who initially defined hybrid warfare and involved four types of threats: (1) traditional; (2) irregular; (3) catastrophic terrorism and (4) destructive, which exploits technology to counter military superiority [9].

US military experts believe that both now and in the future, a potential adversary is likely to use hybrid specific tactics to counter military superiority, a complex approach in the form of a combination of conventional and asymmetric (irregular) warfare.

Regarding the implications of the hybrid war on US forces, the Department of Defense officials believe it is necessary to counter threats that they might face. It could involve non-state potential opponents, sponsoring states, systems networks and computer

confederations, satellite attacks, portable surface-to-air missiles, improvised explosive devices, information operations, and mass media manipulation as well as chemical, biological, radiological, and nuclear weapons of mass destruction, and high-yield explosions (CBRNe). In their view, the phrase "hybrid conflict" is used to describe the growing complexity of the present and future conflicts and the nature of threats, which imposes the need for adaptability of forces operating in the current operational environment [10].

Hybrid threats occur where conventional, irregular, and asymmetric threats overlap in time and space. The conflict may involve participants ranging from individuals, groups, or states operating at the local, trans-national, or global levels. Such disputes may include acts of violence within communities, acts of terrorism, cyber-attacks, insurgency, crime, or disorderly conduct [11].

In the approach of American military theorists (based on aquired experiences in Afghanistan and Iraq), Hybrid Threat (HT) [12] expresses the combination of conventional military forces equipped with sophisticated weapons, complex systems and combined tactics with actions of irregular parties such as insurgents or criminal organizations. The combination of traditional and irregular, these forces' ability to migrate and transform in both directions that result in unrestricted violence, directed against weaknesses, makes the hybrid threat extremely effective. To determine the "hybrid" character, these entities (military units, rebel factions, separatists, criminal groups, guerrillas, terrorists, insurgents, partisans) will cooperate in the context of fulfilling their separate interests. Therefore, it is considered that future conflicts cannot be viewed separately on different types of threats or challenges. Most likely, the armies must be able to deal simultaneously with all kinds of threats, to be able to operate successfully against all types of opponents, in complex conflicts, in all possible environments. According to the authors, their synthesis is the essence of hybrid war [13].

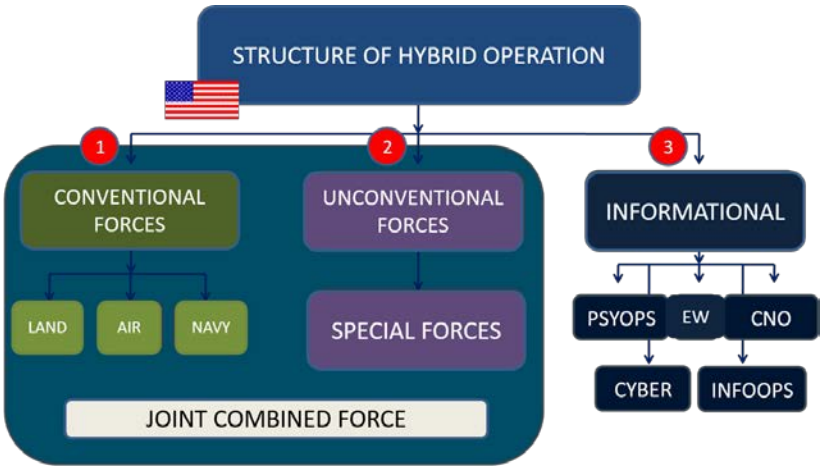

Fig. 2. US Hybrid Approach [3, p. 156]

Regarding the theory and practice of hybrid war, the Russian approach differs from the American one. In the Ukraine conflict, Russia applied a range of actions that resulted in the achievement of its political goals outside of a declared classical war. In February 2013, Valeri Gherasimov, the Chief of General Staff of the Russian Armed Forces that time, wrote in an article published in the Russian defense journal VPK that war and peace are becoming increasingly mixed. Conflict methods have changed and now involve the widespread use of political, economic, information, humanitarian, and other non-military measures. He stated that all this could be supplemented by inciting the local population and using disguised armed forces [14]. In the light of events occured a year later, the Russian military official's statement demonstrates the premeditation and mindful application of the hybrid actions that resulted in the urgent annexation of Crimea and the proclamation of Novorusia's independence. General Gherasimov continued in his speech: "The rules of engagement have changed significantly. The use of non-military methods to achieve political or strategic objectives has, in some cases, proved to be far more effective than the use of force. The widespread use of asymmetric means can help neutralize the military superiority of the enemy. This includes the use of special

forces and internal opposition to create a permanent front within an enemy state, as well as the impact of propaganda tools, forms, and methods that are continually being improved" [15].

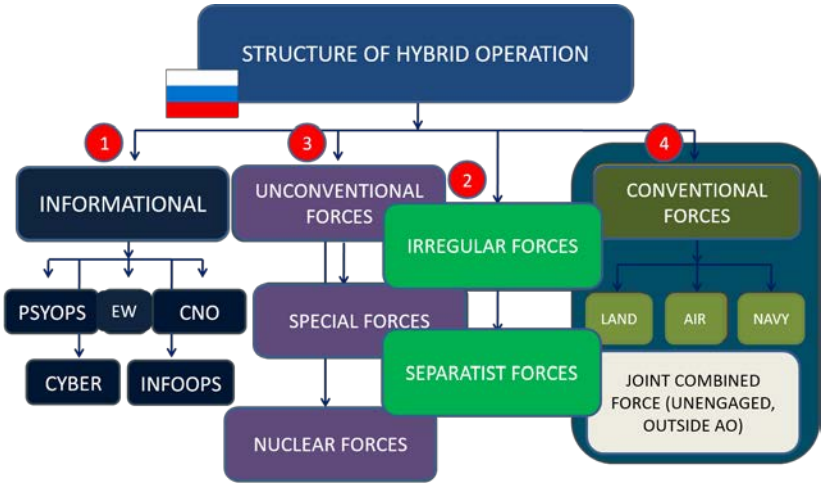

Fig. 3. Russian Federation Approach [3, p. 157]

Typology of risks and threats in hybrid conflicts. From the study of these attempts to explain and define hybrid war or conflict, we consider that this is a fighting strategy that includes both a multitude of different actors: state actors, non-state actors, sponsor states, but also dangers, risks, and multiple threats manifesting themselves in the physical environment, of a conventional nature (conventional military forces, in the legitimate service of the state), unconventional (nuclear forces, special operations forces, chemical, biological, radiological and nuclear weapons of mass destruction-CBRN WMD and toxic industrial materials-TIMs, improvised explosive devices-IED) and asymmetric (guerrillas, insurgent, and separatist groups activated, terrorist and criminal organizations), as well as in the virtual cyber environment (informational). They are engaged in combat in a collaborative and coordinated manner, usually against a superior opponent in military forces and technologically.

When we refer to risks and threats in the context of the contemporary operational environment, defined as a system of systems in which each actor involved seeks to pursue their interests, in a hybrid conflict, we should also address issues from this perspective. The strategy adopted by a potential adversary is complicated, complete, and manifests itself in all the variables of the operational environment. It is a conglomeration of conditions, circumstances, and influences that affect the employment of capabilities and determine the commander's decision [16].

Regarding "hybrid threats", they suggest those threats generated by an opponent capable of performing both classic and asymmetric actions. They are defined by simultaneous and coordinated use by a particular opponent to exploit vulnerabilities, by means located outside the legal framework or bellow the radar of traditional collective defence [17], making them challenging to anticipate.

Once these vulnerabilities have been identified, the adversary will try to achieve its objectives by any means. It will use all the resources at its disposal, at the right place and time. It will intend to create effects on the vulnerable elements that, once affected, will produce the desired changes and, finally, the achievement of the proposed objectives.

Depending on their nature, we can be broken down hybrid risks and threats into:

a) Conventional (traditional capabilities, aggressive and coherent military actions carried out in the physical terrestrial, air, or maritime environment as well as in cosmic space or underwater);

b) Unconventional (Chemical, biological, radiological and nuclear weapons of mass destruction-CBRN WMD; Special Forces; Geophysical/Ecological techniques for modifying environmental parameters for military purposes);

c) Asymmetric (separatism, insurgency, guerrilla, terrorism, and organized crime).

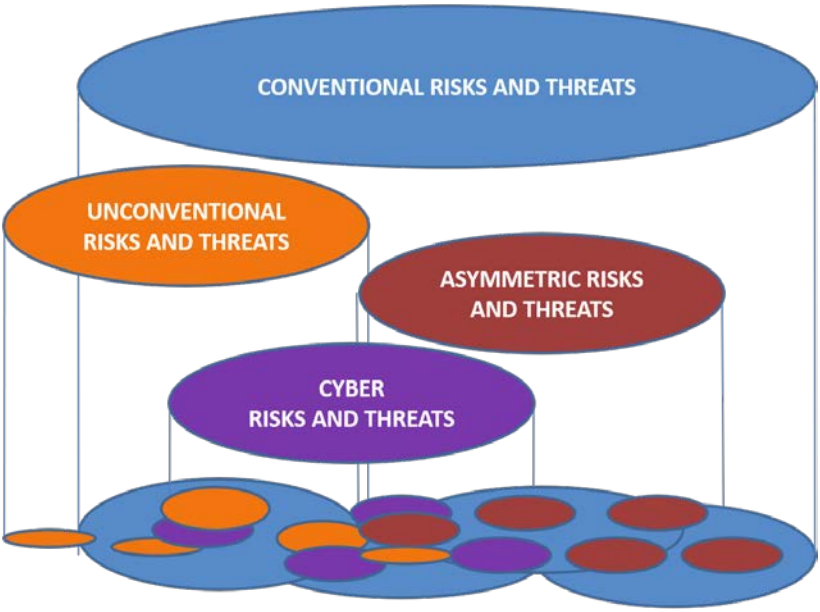

Fig. 4. Hybrid risks and threats [3, p. 61]

The fusion of conventional, unconventional, and asymmetric risks and threats results in a new concept termed “hybrid”, which manifests itself in the contemporary operational environment and suggests complex information, decision-making, and development approaches.

Depending on their environment, hybrid risks and threats can be a combination of:

a) physical environment components (conventional, unconventional, asymmetric);

b) virtual (informational) environment components (Cyber; Information operations-INFO OPS; Psychological operations-PSY OPS, Propaganda).

The overlap of risks and threats in these plans and dimensions generates through overlapping and complementarity, a mosaic of particular complexity expressed in the literature in the combination “Hybrid Threats”.

Fig. 5. Dimensions of operational environment [3, p. 71]

From the analysis of the specific characteristics of the risks and threats that manifest both in the physical space and those in the virtual environment, they can affect national, regional, or global security, leading to planning, preparation, and execution of hybrid military actions.

Conclusions

In conclusion, we appreciate that opponents of hybrid threats will face severe difficulties in identifying and separating the "problems set" specific to each type of threat. They will be forced to apply measures to achieve the economy of forces to cover more lines of operations. The hybrid opponent will continue to shift its efforts and continuously emphasize that any option is inappropriate.

The world's great military powers - such as the United States, the Russian Federation, or an international coalition of states - can momentarily easily impose their determination against a conventional opponent. However, the major challenge today and in

the foreseeable future is how the potential adversary will organize, adapt, and fight, develop unconventional and asymmetric capabilities and strategies, counterbalance, and achieve its strategic objectives.

In hybrid conflicts, the typology of actions displays a shift from the regular, traditional to the unconventional, especially the asymmetric ones. These tend to generalize and manifest throughout the conflict and throughout its spectrum.

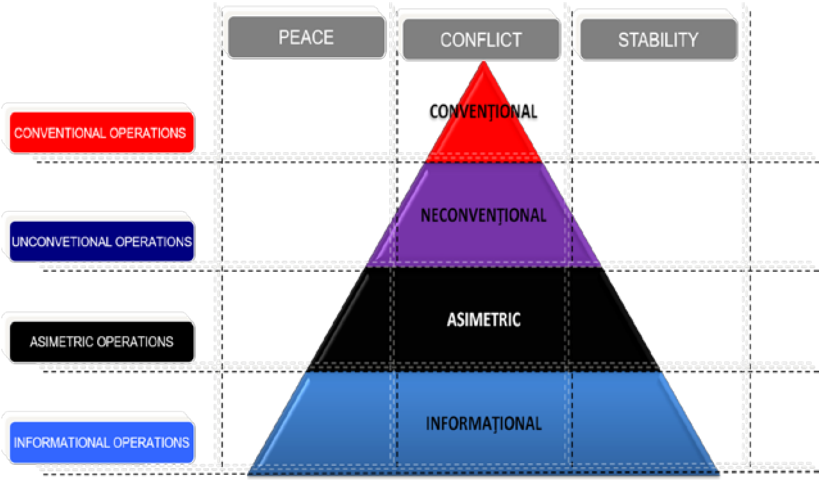

Fig. 6. Incidence of operations that generate the hybrid nature of conflicts [3, p. 76]

We acknowledge that hybrid threats represent the most significant operational risk in the near and medium-term. From this perspective, the armed forces must be prepared to carry out a wide range of missions in a joint and multinational context, in different regions, and in a complex and consequently uncertain operational environment. They will face various hybrid threats and simultaneous combinations of types of activities that will continuously change and adapt.

This reality requires the anticipation, identification, and understanding of the objectives of a wide variety of actors with a role in resolving the conflict from the planning phase of the joint operation to integrate, coordinate and synchronize their effort.

Therefore, to be successful in the fight against a problematic hybrid opponent, in a multinational context, it is essential to use the entire range of tools, from political to military, economic, legislative, and informational to understand, identify, exploit its vulnerabilities and meet the objectives established.

References

1. Hoffman, F.G. (2007), *Conflict in the 21st Century: The rise of Hybrid Wars*, Potomac Institute for Policy Studies, Virginia, SUA, available at: https://cutt.ly/Lk3Yflx (accessed 18 August 2020).
2. Boulding, K.E. (1962), *Conflict and defense: A general theory*, Harper and Row, New York, pp. 5, available at: https://cutt.ly/Uk3T0oJ (accessed 16 October 2013).
3. Herciu, A. (2016), *Conducerea şi întrebuinţarea forţelor întrunite în conflictele hibride*, "Carol Ist" National Defense University Publishing House, Bucharest.
4. Şuştac, Z. and Ignat, C. (2008), *Modalităţi alternative de soluţionare a conflictelor (ADR)*, Editura Universitară, Bucharest, 16 p.
5. Litera Internaţional Publishing House (2002), *Noul dicţionar explicativ al limbii române*, available at: http://dexonline.ro/definitie/hibrid (accessed 6 November 2020).
6. Nacu F. (2002), *Marele dicţionar de neologisme*, Speculum Publishing House.
7. Youtube (2010), The Accidental Guerrilla: Dr David Kilcullen at ANU, June 09, available at https://cutt.ly/ck3ITfN (accessed 10 October 2020).
8. Hoffman, F.G. (2009), *Hybrid vs. compound war*, available at: http://armedforcesjournal.com/hybrid-vs-compound-war/ (accessed at May 16, 2013).
9. Information (2013), available at: http://www.armed forcesjournal.com/2009/10/4198658/ (accessed 16 May 2013).
10. U.S. Government Accountability Office (2010), *Report of Hybrid Warfare*, available at http://www.gao.gov/products/GAO-10-1036R?source=ra (accessed 16 May 2013).
11. NATO Standardization Agency (NSA) (2012), *AJP-2(A) Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, North Atlantic Treaty Organization, Draft, pp. 1-2.

12. Headquarters Department of the Army (2010), *Training Circular No. TC 7-100, Hybrid Threat*, Washington DC.

13. Cruceru, V. (2015), *Războiul hibrid în gândirea militară americană* (*monografie)*, "Carol I-st" National Defense University Publishing House, Bucharest, 28 p.

14. Stan, A. (2014), *Rusia a ridicat războiul la rang de artă*, available at: adev.ro/nb9y9f (accessed 30 March 2015).

15. Gherasimov, V. (2013), "Tsennost nauki v predvidenii" [The value of science in foresight], *Voyenno-Promysblennz Karyer*, No. 8(476), available at: http://www.vpk-news.ru/articles/14632 (accessed 2 April 2014).

16. NATO Standardization Agency (NSA) (2012), *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, pp. 2-O-3.

17. Reisinger, H. and Golts, A. (2014), Russias Hybrid Warfare – Waging War below the Radar of Traditional Collective Defence, *Research Paper*, No. 105, November 2014, pp. 10.

Pavlo Hrytsai
Candidate of Military Sciences, Senior Researcher
Chief of the Department of National Security
and Defence Strategy of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-1181-4523

Serhii Mytchenko
Postgraduate Student of the Department
of National Security and Defence Strategy
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-3711-2033

DEVELOPMENT OF FORMS AND METHODS OF SYNERGY APPLICATION OF NON-MILITARY FORCES AND DEFENSE FORCES IN CRISIS SITUATIONS OF MILITARY NATURE IN CONDITIONS OF CONTERACTION OF HYBRID AGGRESSION

The article considers the need for further development of forms and methods of synergistic [1] use of non-military forces and defense forces in military crisis situations in the context of counteracting hybrid aggression conducted by Russia against Ukraine. The current state of the legal framework for the use of defense forces is considered and the feasibility of developing and implementing new forms and methods of using non-military forces and defense forces in crisis situations of a military nature in terms of combating hybrid aggression is substantiated. The experience of NATO member states in introducing new forms and methods of counteracting hybrid aggression is taken into account. It is emphasized that the timely and high-quality application of the components of the defense forces, their training and application in military crisis situations should be carried out on the basis of certain situations, tasks and requirements for operational (combat, special) capabilities.

Keywords: *synergy, non-military forces, defense forces, counteraction to hybrid aggression, forms and methods, crisis situations.*

Introduction

Problem statement. Shifting the emphasis in military conflicts to the asymmetric use of military force by armed groups not provided by law, the integrated use of military and non-military tools (political, economic, informational and psychological, etc.) fundamentally changes the nature of armed struggle and makes new demands on military security [2]. Purely military tools become ancillary to achieving the military-strategic goals set by the aggressor. Prior to the armed conflict, the aggressor's main efforts were to destabilize the socio-political situation, provoke public dissatisfaction with the current government and incite separatist sentiments in society, and discredit the military-political leadership of the country against which aggressive actions are directed. Together, this creates the basis for the active and covert formation of the so-called resistance movement, the creation of special paramilitary units and their training in methods and techniques of resistance to the current government, including the use of weapons. The result is a violent state response to terrorist acts and provocations, including the use of force, which is presented by the aggressor at the international level as the suppression of democracy or the suppression of the rights and freedoms of citizens of certain regions or national minorities. The combination of different instruments (military and non-military), as a pretext for aggression against another state, determines its "hybrid" nature. The specific sequence of development of modern military conflict necessitates the definition of principles, forms and methods of integration of non-military forces and defense forces of the state to counter armed aggression, which has a "hybrid" nature [3]. Thus, the hybrid war waged by the Russian Federation against Ukraine requires Ukraine to be able to counter emerging threats, and the system of public administration must be able to respond quickly. In view of this, the question arises about the development of new forms and methods of synergistic use of non-military forces and defense forces, and capabilities that need to be developed in the first place.

The analysis of recent researches and publications. The experience of resolving the armed conflict in eastern Ukraine shows that success in counteracting "hybrid" aggression becomes impossible without the integration of military and non-military forces and means of the state [4]. Purposeful, adaptive to the state, which is the object of aggression, the nature of military threats, based on a combination of military and non-military measures, is considered the main sign of their "hybridity" [5]. It is the purposeful nature and high dynamics of the transformation of threats that combine informational, socio-political, ideological, economic and military aspects of the impact on the enemy need careful preliminary study at the state level, with the development of appropriate measures to adequately counter, find new forms and ways confrontation and synergistic influence on the aggressor.

Purpose of the report. On the basis of previous scientific research, requirements of guiding documents to update the search for new forms and ways of synergistic use of non-military forces and defense forces in crisis situations of military nature in counteracting hybrid aggression.

Main part

In modern conditions, the capabilities of the armed forces of the world's leading countries to collect, process and distribute information has increased significantly, which has become an important factor changing the rules of war in favor of widespread use of non-military tools to achieve strategic goals. This tool requires the use of political, economic, informational, humanitarian and other methods that intensify the protest mood of society and are combined with the undeclared use of military forces and means. The aggressor countries no longer rely on the classic invasion, but achieve their goals by a combination of special (subversive) operations, cyber attacks, carefully planned actions, synergistic methods and ways aimed at destabilizing the situation, disorganizing government and military control and supporting illegal armed groups. In such circumstances, the settlement of armed conflict is seen as a process

of orderly interaction of international structures responsible for maintaining international peace and security and components of the security and defense sector, which can be aimed at protecting national interests in order to take all possible actions and measures. or sequentially to solve the problems that led to its solution. In order to counteract the destructive pressure of the aggressor on Ukraine and to enforce the norms of international law and its own obligations, the doctrinal documents of the state [6] provide for “mutually coordinated use of political-diplomatic, informational and forceful instruments of the state”. Given the new, more varied and covert mechanism of armed conflict that the Russian Federation has demonstrated in unleashing armed aggression against Ukraine, the joint and mutually agreed use of military and non-military forces and means is a key condition for resolving it. This requirement is due not only to the desire to avoid duplication of tasks assigned to individual components of the security and defense sector for settlement, and the wasteful use of resources, but also to the fact that in the process of countering "hybrid" aggression changes the role and place of military means. The experience of resolving the armed conflict in eastern Ukraine has shown that success in combating "hybrid" aggression becomes impossible without the integration of military and non-military forces and means of the state that must quickly, effectively and efficiently address aggression and have an effective opportunity to act ahead.

Despite the declared [6] need to integrate the efforts (joint involvement) of the components of the security and defense sector, the organization of the integration process (integration technology) is not defined, which indicates the emergence of both scientific and organizational problems. That is why the definition of the purpose, forms and methods of integration of non-military and military forces and means of the security and defense sector to counter military threats that have signs of "hybridity" is relevant today.

According to military analysts, the ratio of the contribution of military and non-military means to achieve military-political goals in the armed conflict has changed significantly in favor of the latter.

The contribution of military and non-military means also changes during the armed conflict in its stages [7]. This necessitates their prioritization and the development of practical recommendations for integrating the efforts of military and non-military actors in Ukraine's security and defense sector to neutralize military threats that show signs of "hybridity". And this, in turn, forces the state to develop new algorithms, forms and methods of synergistic use of non-military forces and defense forces, both in crisis situations of a military nature and in the initial stages of the hidden origin of conflict in countering hybrid aggression.

The "hybridity" of the military threat is manifested in the hidden, purposeful, destructive and complex influences on the national security system of the state - a set of factors (intentions and actions) of both military and non-military, which are interrelated. That is why it is a question of integrating the efforts of military and non-military forces and means (formation of integrated counteraction potential) to prevent such threats [8]. The implementation of this counteraction is entrusted to the security and defense sector of Ukraine.

Considering possible forms and methods of using non-military and defense forces in different phases of aggravation, both at the beginning of the conflict and in military crisis situations, a synergistic approach should be introduced as more appropriate to combine the results of "hybrid" confrontation and obtain faster and more productive results. A synergistic approach is a cumulative effect, which consists in the fact that when two or more factors interact, their action significantly outweighs the effect of each individual component in the form of their simple sum.

First, the integration of a synergistic approach as a purposeful unification of some actors for joint activities (purely organizational task) will have more effective results.

Secondly, it is a joint activity of some entities with a corresponding common goal.

Thus, the unification of subjects for national security normally already exists in the form of the security and defense

sector, it is considered a synergistic approach to the joint activities of its subjects, which is aimed at neutralizing military threats with signs of "hybridity". Such activities of the security and defense sector actors require the identification of the appropriate forms and methods inherent in the process of counteracting such threats. In the methods of integration are:

– opportunities for forces and means that will be involved in counteraction within the framework of integration efforts;

– qualitative characteristics of personnel, which will be responsible for the development of both a general strategy for countering the threat, and the development and implementation of tasks at the level of the security and defense sector.

– To summarize the above, it is advisable to propose several main ways of synergistic application (integration) of non-military forces and defense forces to counter military threats:

– integration of defense forces and non-military forces and means with priority given to non-force means with the use of force for support;

– integration of defense forces and non-military forces and means with priority given to non-force forces.

It is clear that each of these methods of synergistic application can have many options for the composition of forces and means of the security and defense sector used, and the degree of their participation in countering the threat over time and scale. Further research into the use of non-military and defense forces, especially in military crises that show signs of "hybridity", requires further research.

Regarding the forms of synergistic use of military and non-military means to counter military threats with signs of "hybridity", it is proposed to adopt the military terms "operation" and "company" [3]. At the same time, the essence of the term "operation" is practically indistinguishable from that used in the art of war as "coordinated actions of disparate forces and means united by a single purpose." As for the "campaign", although this term is almost no longer used, but the features of the threats, which have a "hybrid"

nature as the object of study and the complexity of counteracting it give grounds for its use. Thus, threats that have a "hybrid" nature are formed by many factors, the action of which is characterized by: scale; usually significant time limits; focus on various state institutions and entities, the functioning of which affects the state of defense of the state, etc. It is clear that an adequate response to such threats also requires significant time, involvement in counteracting a large number of actors in the security and defense sector (and not only), financial and material resources and is impossible as an operation that has a clear, timed nature.

Conclusions

Thus, in the author's view, the synergistic use of non-military and defense forces, especially in crisis situations of a military nature, will consist of a set of different types and areas of operations (actions and measures), united by a common strategic plan that corresponds to the classical understanding of the term. Given that military threats, especially those that have a "hybrid" nature (signs of "hybridity"), are formed by many different factors, the forms and methods of integration of defense forces and non-military forces and countermeasures can have a large number of options. For the practical implementation of certain forms and methods of integration of defense forces and non-military forces and countermeasures, it is advisable to have the concept of their integrated use taking into account the total synergy effect, as well as to continue research on forms and methods of synergistic use of non-military forces and defense forces during hybrid aggression.

References

1. Wikipedia (2020), *Synergy*, available at: https://cutt.ly/Ej22PFn (accessed 23 January 2021).

2. President of Ukraine (2015), *Decree "On the decision of the National Security and Defense Council of Ukraine on September 2, 2015 "A new edition of the Military Doctrine of Ukraine"*, available at: https://cutt.ly/Zj22m7q (accessed 23 January 2021).

3. Sirotenko, A.M., Bogdanovich, V.Y., Pavlikovsky, A.K. and Dublyan, V.Y. (2020), *Military aspects of countering "hybrid" aggression: the experience of Ukraine*, NUOU, Kyiv, pp. 79-94, available at: https://cutt.ly/cj7Raij (accessed 23 January 2021).

4. Sirotenko, A.M., Bogdanovich, V.Y., Romanchenko, I.S. and Svida, I.Y. (2019), *Methodology of integrated use of military and non-military forces and means of the security and defense sector to counter modern threats to the military security of Ukraine*, NASV, Lviv, 268 p.

5. Gorbulin, V.P. (2017), *World Hybrid War: Ukrainian front*, NISD, 496 p.

6. President of Ukraine (2015*), On the new version of the Military Doctrine of Ukraine*, available at: https://cutt.ly/Zj29sAU (accessed 23 January 2021).

7. Ivashchenko, A.M. (2015), Evolution of views on the strategy of modern hybrid conflict and scenarios for counteracting hybrid threats, *Proceedings of the Central Executive Committee of the NGO*, No. 1(53), pp. 18–23.

8. Bohdanovych, V.Yu., Svyda, I.Yu. and Syrotenko, A.M. (2018), Comrehensive employment of military and non-military forces and means concept for providing the sufficient level of state military security, *Science and Technology of the Air Force of Ukraine*, No. 2(31), pp. 16-29. https://doi.org/10.30748/nitps.2018.31.02.

Oleh Hudyma
Doctor of Philosophy, Senior Researcher
Doctoral Student of the Centre of Military-Strategic Research
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-3494-8583

SITUATIONAL CENTER AS AN ELEMENT OF THE STATE MANAGEMENT SYSTEM IN COUNTERACTING HYBRID THREATS

Hybrid warfare is a combination of traditional and non-traditional methods of warfare, which include the use of special forces, irregular armed groups, information warfare and propaganda, diplomatic measures, cyberattacks, economic pressure and more. Given the multi-vector nature of hybrid wars, it is advisable to take a comprehensive approach to building a system of management and coordination of efforts in all spheres of society and the state.

Taking into account the experience of the world's leading countries in combating hybrid threats and in accordance with the tasks set by the governing documents of the state, it is advisable to build a state management system (coordination) of measures to combat hybrid threats based on a system of situational centers.

Keywords: *situation center, state management system, hybrid threats, security and defense sector, management and coordination.*

Introduction

Problem statement. Modern international conflicts can no longer be assessed in terms of traditional approaches to hostilities, they can be described by one term - hybrid warfare.

Hybrid warfare is a combination of traditional and non-traditional methods of warfare, which include the use of special forces, irregular armed groups, support for internal unrest and separatist movements, information warfare and propaganda, diplomatic measures, cyberattacks, economic pressure and more.

In the conditions of the emerging hybrid threats in the

countries of the world various variant actions on counteraction to it and search of ways of the international collective counteraction to hybrid aggression are worked out.

According to the 2017 memorandum, the European Center for Combating Hybrid Threats was established in Helsinki (Finland) with the participation of the United States, France, Germany, Sweden, Poland, Finland, Latvia, and Lithuania. Which is an interstate, European Center for Combating Hybrid Threats - Cyberattacks, Propaganda and Disinformation [1].

Speaking at the Cyber Defense Conference (Paris, 15 May 2018), NATO Secretary General Jens Stoltenberg noted that today NATO has three key roles in cyberspace to make progress in the Alliance. It is necessary to act as a center for information exchange, training and expertise and to protect our networks [2].

As a result of the meeting of the Heads of State and Government who took part in the meeting of the North Atlantic Council (Brussels 11-12.07.2018), a Declaration was formed stating that “NATO countries have agreed on how to integrate sovereign cyber effects provided voluntarily by Allies, in Alliance operations and missions under strong political control. Reaffirming NATO’s defense mandate, we are committed to seizing the full range of capabilities, including cyber, to deter, protect and counter the full range of cyber threats, including those under the hybrid campaign [3].

The realities of today convincingly prove the fact of waging a "hybrid war" against Ukraine, the main components of which are an information campaign (aimed at splitting Ukrainian society, destabilizing the socio-political situation, discrediting and discrediting the new Ukrainian government in the eyes of the international community) and special operations (sabotage and reconnaissance and the deployment of resistance movements) [4–7].

An extremely dangerous component of the “hybrid” war against Ukraine is aggression in cyberspace.

Given the above, today the urgent task for Ukraine is: to improve the state system of government, which concerns the creation of mechanisms to counter the conduct of “hybrid war” against Ukraine.

The above is confirmed by the fact of the unpredictable occurrence of the Covid-19 pandemic in the world and the inability of even the world's leading countries to predict its occurrence in a timely manner, to work out adequate measures to localize and eliminate it as soon as possible.

The analysis of recent researches and publications. Theoretical foundations of the phenomenon of “hybrid war” have been studied at various times by such world-class experts as F. Hoffman, J. McCwen, R. Wilkie, D. Kilkallen (USA), Martin van Creveld (Israel), Frank van Kappen (Netherlands).) and others.

In domestic science, the study of "hybrid warfare" and its theoretical and methodological foundations are devoted to V. Gorbulin, E. Magda, G. Lutsyshyna, Y. Klymchuk, G. Sytnyk, A. Slyusarenko, L. Smoly, G. Perepelytsia, B. Parahonsky, M. Trebin, G. Yavorska, O. Bazaluk, Y. Punda, Y. Radkovets, V. Telelym, M. Trebin, P. Shevchuk and others.

Research on the formation and implementation of management decisions, the formation and development of public administration decision-making systems were carried out by the following specialists in public administration: O. Amosov, V. Bakumenko, A. Degtyar, N. Nyzhnyk, G. Pocheptsov, V. Rebkalo and others.

V. Sytnyk and R. Marutyan considered the activity of the situation center as one of the tools of strategic state management in the sphere of national security.

The above-mentioned studies do not consider the issues of building a system of management (coordination) of the state’s efforts to counter hybrid threats.

Purpose of the report. Based on the analysis of measures taken by the world’s leading countries to combat hybrid threats and in accordance with the objectives set by the governing documents of the state proposed an approach to improve the quality of countering hybrid threats - building a state management system (coordination) of state efforts to combat hybrid threats.

Main part

According to the Concept of Development of the Security and Defense Sector of Ukraine, approved by the Decree of the President of Ukraine of March 14, 2016 № 92/2016, it is determined that the main form of hybrid war against Ukraine is a combination of diverse and dynamic actions of regular Russian forces interacting with criminal armed groups. and criminal elements, whose activities are coordinated and carried out according to a single plan and plan with the active use of propaganda, sabotage, deliberate harm, sabotage and terror.

In addition, the analytical structures of the European Union have identified such types and areas of threat as terrorism, cybersecurity, organized crime, maritime disputes, space, resource scarcity and covert operations [8].

An extremely dangerous component of the "hybrid war" against Ukraine is aggression in cyberspace. In particular, it is about mass attacks on the websites of authorities and state-owned companies, the war on social networks, which was launched by Russian "troll factories", cyber espionage. On the Russian side, there are numerous hacker groups, such as "Sandworm", "Cyberberkut", "Octopus" (from the territory of the DNR) and others. It is obvious that Russian special services are behind them and direct their activities. (To counter Russian cyberexpansion, Ukrainian volunteers organized a group "Ukrainian Cyber Troops" in 2014. Ukrainian "Cyber Alliance" was also established (an association of FalconsFlame, Trinity, "Rukh8" and "CyberHunt") CERT-UA (Computer Emergency Response Team of Ukraine) at the State Special Communications Service recorded 216 cyberattacks from outside (more than half of them - on government agencies) in 2014. In 2015, the number of attacks increased 1.5 times Over the past three years, pro-Russian hackers have carried out massive attacks on government Internet portals and Internet resources of government agencies, including the websites of the Presidential Administration, the Cabinet of Ministers, and the State Special Communications Service,

and attacked portals of a number of regional state administrations [9].

As of today, the global trend of increasing the number of users of social information network services persists. In addition, research by Western experts notes that over the past ten years, users of social networks began to spend twice as much on social networks [10-12].

Experts have recognized the use of social networks, satellite TV channels and print media in Russia by Russian secret services in 2014-2017 as a threat to the democratic structure of Western society [9].

Russia's aggression on the Internet has caused very serious concern to the intelligence services of a number of countries around the world. US intelligence has accused Russia's top leadership of organizing cyber-sabotage during the US election campaign. The danger of Russian intervention was stated by representatives of the intelligence services of Germany, the Czech Republic and other European countries [9].

In addition, leading US think tanks continued to study Russia's experience of information campaigns during the "hybrid war" against Ukraine and the Kremlin's efforts to undermine democratic institutions in Western countries.

Defense Minister Annegret Kramp-Karrenbauer, speaking at a meeting of the Foreign Affairs and Subcommittee on Defense and Security of the European Parliament (July 14, 2020), stated that one of Germany's priorities during its presidency of the Council of the European Union would be to analyze military and hybrid threats, in particular by Russia [14].

The analysis will be carried out by the EU Intelligence and Situation Center (EU INTCEN), the Member States of the European Union and their intelligence will provide their proposals and data for analysis [13–15].

The main principle of counteracting Russia's information influence is the consolidation of efforts of all NATO countries, as well as the cooperation of the United States with European partners in order to create a "united front of counteraction", which involves

the adoption of joint coordinated decisions.

Given the multi-vector areas of creation of situational centers in Ukraine, which is reflected in a number of guiding documents, namely:

– in accordance with the Decree of the President of Ukraine of 26 May 2020 № 203/2020 "On the Annual National Program under the auspices of the NATO-Ukraine Commission for 2020": creation of a network of situational centers of state bodies in the system of strategic communications; creation of a network of situational monitoring centers, risk analysis to prevent threats to critical infrastructure; building the capacity of situational centers of the security and defense sector of Ukraine, which is achieved by fulfilling the priority task of creating a system of situational centers of the defense sector for operational decision-making in the field of defense;

– according to the Action Plan for Defense Reform for 2019-2020, approved by the Minister of Defense of Ukraine on January 23, 2019: the creation of a system of situational centers for the defense sector based on secure information and telecommunications systems may be a basis for building a national system network (system) of situation centers of the security and defense sector and local authorities under the general direction and coordination of the Main Situation Center of Ukraine in coordination of efforts with NATO and European Union countries.

Conclusions

Thus, based on the analysis of the world's leading actions to combat hybrid threats, it is proposed to create a state management system (coordination) of efforts to combat hybrid threats based on a system (network) of situational centers under the general management and coordination of the Main Situational Center of Ukraine.

In the future, research will focus on the development of: mechanisms for predicting the occurrence of hybrid threats and mechanisms (algorithms to do) to eliminate them within the

functioning of the system (network) of situational centers of the security and defense sector and local authorities; draft Concept of information support and integration of information resources to ensure the functioning of the system (network) of situational centers of the security and defense sector (defense forces) and local authorities.

References

1. The official site of vnk.fi. (2017), *Minister for Foreign Affairs of Finland Mr Timo Soini at the signing of the Memorandum of Understanding establishing the European Centre of Excellence for Countering Hybrid Threat*s, available at: https://cutt.ly/hjNW7at (accessed 15 July 2020).
2. NATO (2018), *Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris*), available at: https://cutt.ly/4jNEerA (accessed 15 July 2020).
3. NATO (2018), *Brussels Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018*, available at: https://cutt.ly/NjNEt5S (accessed 15 July 2020).
4. Barovska, A., Chernenko, T., Dubov, D., Hnatiuk, S. and Isakova, T. (2016), "*Informatsiini vyklyky hibrydnoi viiny: kontent, kanaly, mekhanizmy protydii*" [*Information challenges of hybrid warfare: content, channels, counteraction mechanisms*], available at: https://cutt.ly/tjNEsQ5 (accessed 15 July 2020).
5. Holloway, M. (2017), *How Russia Weaponized Social Media in Crimea*, available at: https://cutt.ly/yjNEhXl (accessed 15 July 2020).
6. Molodetska, K.V. (2016), "Rol sotsialnykh internet-servisiv u protsesi zabezpechennia informatsiinoi bezpeky derzhavy" [The role of social Internet services in the process of ensuring information security of the state], *V International Science conf. Information, communication, society*, 19-21 May 2016, Lviv, pp. 26-27.
7. Perry, B. (2015), *Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations*, available at: https://cutt.ly/NjNEKWd (accessed 15 July 2020).
8. European Parliament (2015), *Understanding hybrid threats. Briefing European parliamentary research service*, available at: www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/ EPRS_ATA (2015)564355_EN.pdf (accessed 15 July 2020).
9. National Security and deFense (2016), "Hibrydna viina Rosii –

vyklyk i zahroza dlia Yevropy" [Russia's hybrid war - a challenge and a threat to Europe], *National Security and Defense*, No. 9-10 (167-168), pp. 2-16, available at: https://cutt.ly/xjNRFRR (accessed 15 July 2020).

10. Slideshare.net (2016), "*Obzor sotsialnykh setey. Leto, 2016*" [*Overview of social networks. Summer, 2016*], available at: https://cutt.ly/tjNR8zR (accessed 15 July 2020).

11. Metelskyi, D. (2020), "*Chomu rosiiski sotsialni merezhi – zbroia?*" [*Why Russian social networks - weapons?*], available at: https://cutt.ly/RjNTtVi (accessed 15 July 2020).

12. Popova, T. (2017), "*Sotsialni merezhi, kiberataky ta hibrydni viiny*" [*Social networks, cyberattacks and hybrid wars*], available at: www.radiosvoboda.org/a/28598299.html (accessed 15 July 2020).

13. The official site of Eurointegration.com.ua (2020), "*YeS z initsiatyvy Nimechchyny proanalizuie zahrozy z boku Rosii*" [*The EU will analyze threats from Russia at the initiative of Germany*], available at: www.eurointegration. com.ua/news/2020/07/15/7112148 (accessed 15 July 2020).

14. Prystaiko, V.V. (2019), "Sytuatsiini tsentry yak kliuchovyi instytutsiinyi mekhanizm derzhavnoho antykryzovoho upravlinnia: zarubizhnyi dosvid" [Situational centers as a key institutional mechanism of state anti-crisis management: foreign experience], *Scientific notes of Tavriya National University named after V.I. Vernadsky. Series: Public Administration*, Vol. 30(69), No. 3, pp. 138-142. https://doi.org/ 10.32838/2663-6468/2019.3/24.

15. Trush, O.O., Hudyma, O.P. and Novik, I.S. (2014), "Informatsiino-analitychni zasoby zabezpechennia derzhavnoho upravlinnia u providnykh krainakh svitu: dosvid dlia Ukrainy" [Information-analytical means of ensuring public administration in the leading countries of the world: experience for Ukraine], *Theory and Practice of Public Administration: Collection. Science. pr.*, No. 3 (46), pp. 287-295.

Vitaliy Katsalap
Candidate of Military Sciences, Associate Professor
Senior Lecturer of the Department of Informational Technologies
and Informational Security Employment of the Force Support
and Informational Technologies Institute of the National Defence
University of Ukraine named after Ivan Chernyakhovskyi
Kyiv, Ukraine.
https://orcid.org/0000-0003-4804-8022

Andrii Pryma
Senior Researcher of the Centre for Military Strategic Studies
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-0776-6864

Mykola Pryma
Researcher of the Centre for Military Strategic Studies
of the National Defence University of Ukraine
Named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-8363-1929

THE ESSENCE OF INFORMATIONAL RESOURCES OF SECURITY SECTOR OF STATE DEFENSE

Analysis of publications on the classification and the nature of "information resources." The relation between the components of the security sector and influence of national security. The necessity of creation of system of comprehensive protection of information resources of military sphere is definited.

Keywords: *information security, information resources, the Security and defense sector of the state.*

Introduction

Problem statement. In the XXI century, the level of development and security of the information environment have

become the most important factors in all areas of national security. Its provision with the use of a well-formulated national information policy greatly contributes to the success of tasks in the political, military, economic, social and other spheres of state activity. At the same time, today no sphere (subject activity) of people can be effectively organized without the corresponding system of information support of this activity. To provide information support for a specific type of human activity, an appropriate information infrastructure is organized (created) [1]. Integral components of the information environment of Ukraine are information resources, information infrastructure and information technologies that are part of the national information potential.

The analysis of recent research and publications. In well-known publications, the number of works on the problem of highlighting the essence, classification, systematization of information resources is limited. The most fundamental is [2].

According to [3], a new post-industrial information society is born, in which knowledge (science) becomes a direct social (production) force. This is achieved through the information, more precisely, the dynamic mechanism of transformation of knowledge into information resources and the latter into material force. "The information society is a society, the structure, technical base and human potential of which are adapted for the optimal transformation of knowledge into information resources and processing it for the purpose of translation from passive forms (books, articles, patents, etc.) into active ones (models, algorithms, programs, projects, etc.) ". But the creation of modern knowledge bases is of special importance for activating the information potential of society. Science (new knowledge) becomes a social force, embodied in the practical experience of the masses, as well as materializing in new technology, technologies, products and services.

Purpose of the report is to substantiate the essence of information resources of the Security and Defense Sector of the state.

Main part

National security of Ukraine has component of military security. As a component of national security, it also has appropriate subsystems (areas): political, economic, military, and so on. In view of this, it is important to establish the interdependencies between the components of the information environment of the security and defense sector of the state and the relevant areas of national security of the state, as shown in Fig. 1.

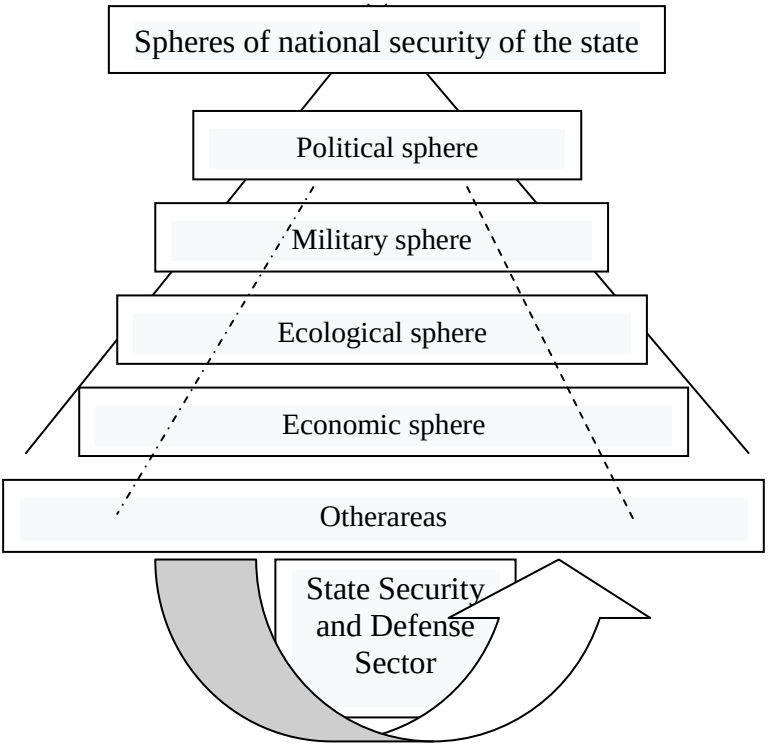

Fig. 1. The relationship of the Security and Defense Sector of the state with the spheres of influence of national security of the state

Protection of information resources is one of the priority tasks of national security of Ukraine, it is an important component of the state information policy.

The current legislation does not establish a full legal

interpretation of the components of information resources. Criteria for assigning information resources to the category of state and non-state are not defined. This situation has created and will continue to create difficulties in the formation of the system of national information resources, the management of this system, as well as in the legal registration of functions related to the possession and use of information resources.

On the basis of information corrective support of material and energy processes in the society the basic streams of the heuristic information which needs processing and use arise. As for the incompleteness of information cycles, which cover only the stages of transmission, data collection, diagnosis, information, they become really clear only when correlated with the full dynamic process (cycle). Information as a message of some information has no independent value. Its value for the recipient is determined by the increase in his knowledge, correlated with a specific purpose, or, in the case of the final information result, the magnitude of the decrease in the entropy of the object under consideration. In the new information society, science acts directly as a productive force. The form of direct participation of knowledge produced by science in the production process is information, and the mechanism of effective interaction of scientific production is the information mechanism. That is, information resources are a necessary and essential intermediate link between knowledge (science) and action (material result), which cannot be left outside the theory of reproduction.

Information resource in its definition has two inseparable components: formal-logical (informational) and semantic (cognitive). The first aspect of this fundamental concept, namely the formal-logical side, is formed as a result of generalization of the practice of computerization and development of engineering knowledge. At the heart of the methods of using the presentation of knowledge, the first aspect of the concept of information resource - is mainly mathematical formalization and logical completeness. On the contrary, the cognitive approach is based on understanding the process of awareness of anything by a person, so the presentation of

knowledge in this case is characterized by expressiveness rather than mathematical sophistication and rigor.

Thus, the information resource can be considered as a "symbiosis" of knowledge and information.

The main feature of information processes is the mandatory interaction of three elements: sources, communication channels, recipients of messages. Shannon was the first to connect the information capacity of the signal to the communication medium. He also made the weight of the message dependent on the characteristics of the source, channel and receiver [5].

The transformation of knowledge into an information resource depends on the possibilities of their coding, distribution and transmission.

The features of the information resource include:

– information resource is practically inexhaustible, in process of development of a society and intensification of process of use of knowledge their stocks - do not decrease, and on the contrary - grow;

– information resource is used, it does not disappear, but is preserved and even increased (due to the constructive transformation of the received messages, taking into account the experience, local conditions);

– it is not independent and in itself has only potential significance and, when combined with other resources, it manifests itself "kinetically" - as a driving force; the efficiency of its use is associated with non-primary (repeated) production of knowledge, information interaction allows to obtain new knowledge at a much lower cost compared to the cost of labor, energy, time for its direct generation;

– information resources is a form of direct inclusion of science, including theoretical research, in the productive forces;

– there is an information resource as a result of not just mental work, but its creative part.

Mankind faces a huge problem in terms of its importance and complexity: to extract the maximum amount of information from the messages accumulated throughout history and turn it into an actively

functioning resource. It is a question of transformation of book descriptions and other scattered knowledge into operating programs and algorithms. This is part of the work on the formation of information resources.

According to the importance of information resources are divided into strategic, operational, tactical [6].

Strategic information resources are resources that provide a permanent process of forming the nation's mentality as the most important factor in the sustainable progressive development of the country. Strategic IP should include transformed into easily accessible to many users, including in electronic form worldviews, cultural, historical, legal and other sections of humanities and fundamental natural sciences. In the military sphere, strategic information resources include military doctrine, laws governing military activities, and fundamental provisions of military security.

Operational information resources are current business, commercial and other reference information that is focused on meeting daily needs in various areas of activity. For the military sphere - this is information of a military nature, which is obtained (obtained) or created during intelligence, information gathering, information work of headquarters and other information activities, as well as information circulating in automated military systems, through communication channels, in information systems. at various levels, including in technical intelligence systems – operational directives, reports, reports.

Tactical information resources include applied scientific, technical, economic, environmental, demographic, and other knowledge that has been transformed into a resource and is needed to address current issues, such as current information or military security issues. In the military sphere, it is a set of basic provisions of operational art and tactics of military branches, it is military-applied knowledge obtained by cadets and students of military educational institutions, statutes, guidelines, etc. It is also mathematical and software for military information systems.

The authors share the opinion of military experts [4] that in

the military sphere, the protection of information resources is the basis of the country's defense capabilities, directly related to information security of the security and defense sector.

It is obvious that the essence of information security of Ukraine in the military sphere, the system-forming core of which is the information infrastructure of the Armed Forces of Ukraine and the Ministry of Defense of Ukraine is not the protection of information resources from various information influences. and defense of the state (protection of national interests of Ukraine from external threats, first of all, protection of state sovereignty, territorial integrity, inviolability of the state border and prevention of interference in internal affairs of Ukraine).

In order to ensure information security in the military sphere, it is necessary to create and actively develop a single information space of Ukraine, its comprehensive protection against unauthorized access to available information resources and external destructive influence.

To achieve an information advantage over the enemy, in accordance with [4], the formation, use and dissemination of information resources of the security and defense sector of the state is provided by:

– subjects of the security and defense sector of the state, effective functioning of the automated control system of the Armed Forces of Ukraine, databases of other subjects of the security and defense sector of the state;

– creation of a base for simulation modeling of armed struggle processes;

– creation of a modern system of communication and data exchange between all levels of military administration;

– evolutionary creation of a set of interconnected monitoring systems;

– improvement of means of remote observation of the enemy;

– introduction of a system of formation and use of special information resources for the purpose of active information pressure on the enemy through measures of operative masking, information

and psychological influence, disturbance of work of its information systems.

Particular attention should be paid to the development of the theory of information operations and its implementation in the practice of further reform of the Armed Forces of Ukraine.

Static information resources of the security and defense sector of the state - logistical, financial, personnel, medical. There is a need to create departmental and interdepartmental electronic libraries, an automated system for managing administrative and economic processes of the Armed Forces of Ukraine, establishing technical conditions and regulations for vertical-horizontal access to static information resources of security and defense sector.

Since computer systems are now directly integrated into the information infrastructures of modern society, the means of protection must take into account modern forms of information presentation (hypertext, multimedia). This means that security systems must provide security at the level of information resources, not individual documents, files or messages.

Conclusions

As a result of the above to solve the problems of information security of the security and defense sector of the state it is proposed:

1. To create a body for coordination of policies and measures to ensure information security in the military sphere (with the function of interaction with certain entities of the security and defense sector of the state). The tasks of such a body will need to be based on a correct understanding of the total information resources in the military sphere, the mechanisms of its production and use, and the conceptual provisions that follow from this.

2. To ensure the interaction in crisis situations of the elements of the operational monitoring system, which are associated with the formation of a dynamic component of information resources.

3. Focus efforts on the protection of information resources by active or passive countermeasures, the possibility of restoring

information resources in case of influence of the opposing party, deepen the study of the properties of information resources of certain classes to improve the efficiency of their operation at all stages of their life cycle.

4. Introduce and constantly improve the system of static information resource of the sector of resource provision of subjects of the security and defense sector of the state.

The above necessitates more thorough research to determine the needs of obtaining and using the necessary information resources of the security and defense sector of the state, namely: creation of elements of the information infrastructure of the military sphere, which produce the necessary information resources; development of means and processes of use of information resources; ensuring the protection of information resources. All this will be possible in the case of creating a system of comprehensive protection of information resources, justification of ways to create and develop which is, in particular, the task of research units of the Ministry of Defense of Ukraine.

References

1. Golubev, Y.N., Golubev, Y.N., Grin, V.R. and Shirmanov, A.V. (2012), Terminological congestion on the paths of military informatization, *Military Thought*, No. 6, pp. 44-53.

2. Ros, A.O. and Pustovit, S.M. (1999), Information resources: essence and classification, *Scientific and Technical Collection*, No. 3.

3. Kanygin, Y.M. and Kalitich, G.I. (1990), *Fundamentals of theoretical informatics*, Publishing house: Scientific Thought, Kyiv, 230 p.

4. Snitsarenko, P. (2009), Sources and essence of information security in the military sphere and problems of its provision, *National security, Ukrainian dimension, stock*, No. 5(24), pp. 23-33.

5. Shannon, K.E. (1963), *Works on the theory of information and cybernetics*, Publishing house: Foreign literature, Moscow, 832 p.

6. Ruban, V.Y., Kalitich, G.I., Shirokov, V.A., Ros, A.A., Maidanyuk, G.Ya. and Gorbatok, N.I. (1994), Informatization and modeling in the development of Ukraine – Informatization of the processes of economic development of Ukraine, *Scientific works of State Research Institute of Informatization and Modeling of Economy of the Ministry of Economy of Ukraine*, pp. 5-28.

Victor Korendovych
PhD (Technical Sciences)
Professor of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-2949-1870

HYBRID WAR OF RUSSIA AGAINST UKRAINE: LESSONS LEARNED FOR THE BLACK SEA REGION

The armed aggression of the Russian Federation against Ukraine has actualized the paradigm of armed conflict and changed the security environment throughout Eastern and Central Europe and the Black Sea region. The Black Sea Region has a special priority among the objectives of Russia's expansion. This region is also very important for Ukraine. The report analyzes the military and political lessons learned of this aggression in the context of their consideration for the military educational process of Ukraine.

Keywords: *hybrid war; casus belli; performance of the armed forces; lessons learned.*

Introduction

Problem statement. The annexation of Crimea by the Russian Federation together with the war in Donbass and a number of other frozen conflicts, surrounding the North Black Sea coast, have created a complex security problem that is difficult to resolve in the short term. This requires the increasing of resilience of the Black Sea region countries as the priority to deter aggressor. The military education performs a special mission in the training of the leader who have to be the core element of this resilience.

The analysis of recent researches and publications. A huge range of publications is devoted to the problems of ensuring defence capability for the countering of hybrid warfare. Among the latest publications about the Russian Hybrid War against Ukraine it is worth to admit publication of James Sherr [1] and Mason Clark [2].

Purpose of the report. The objective of the report is to draw attention to the lessons learned of Russia's hybrid war against Ukraine, both for our country and in a broader context of the Black Sea region.

Main part

Russia's annexation of Crimea changed Ukraine, the Black Sea region as well as it affected a world security. There are many speculators who claim that the annexation of Crimea is the same case as Kosovo one. It does not. The armed conflict in Kosovo was preceded by a long period of negotiations to resolve the existing contradictions. Russia till 2014 brought no official complaint against Ukraine regarding its treatment of Russian "compatriots" or other threats that could be a *casus belli* [1]. The Crimean annexation was carried out without plausible justification and without any effort to resolve the dispute, which did not exist.

Therefore, Russia, not having a chance to use *casus belli* for aggression against Ukraine in 2014, chose a hybrid form of warfare, the methodology of which it tested quite well at the post-Soviet space. Since then, Russia has used all elements of a hybrid warfare and only military aggression it used since 2014.

Russia's strategic goal is not limited by Ukraine, it is aimed at the Black Sea region and beyond. In this region Russia began to implement its policy of collecting "post-Soviet lands", and it belted by the conflicts the entire northern coast of the sea [4], figure 1.

To achieve its strategic goals, Russia adapted its military theory and conducts armed forces as part of a hybrid war (HW), subordinating military activities to other operations. The occupation of Crimea became a classical example of HW. At the same time Russian military retains theoretical space for conventional warfare and does not insist that all conflicts in our time are "hybrid" in nature. They also argue that conventional war in the 21st century is unlikely due to technological change and the strategic balance of power [2].

Fig. 1. Consequences of Russian aggression in the Black Sea region [7]

Conducting HW in Ukraine, Syria and Libya, Russia is preparing for future wars with more powerful opponents. So why it is important for us to understand the goals of the Russian Federation, the forms and ways to achieve them, not just its capabilities.

What lessons learned does Ukraine make and how they are useful for the Black Sea region countries? What warfare against a hybrid war should be?

We will pay attention only to two areas: political and military.

Russia's goal of HW is to destroy Ukraine as an independent state. Ukraine's strategic goal is the restoring its territorial integrity and it is important now to assess real status of the war. The first political lesson-learned could be defined as: the hybrid war is going on … and it is difficult to predict its end, it is a long way for Ukraine to achieve its goal. Russia has only suspended the active phase of military aggression, and the other components of its HW are carrying out their tasks. For the Russian elite, the axiom "Ukraine will never be able to stand by itself" remains the basis of its policy [1].

The second lesson-learned: we need to learn the forms and methods of aggressor's actions, to develop a realistic strategy of symmetrical and asymmetrical actions in response, increase the

efficiency of crisis management. Not only the Defence and Security Sector, but the entire state counters the hybrid war.

Third. Do not allow Russian "moles" to penetrate our society, our political system, defence and security structures. Today, Russia shifting its focus to political, social and economic destruction of Ukraine from inside. These "moles" are inside, they use political, administrative, economic ways to destroy our society.

Fourth. It is impossible to pacify Russia. No country in the Black Sea region (especially a non-NATO ones) can consider itself safe from Russian aggression.

Fifth. The victims of Russian aggression must develop and increase their own resilience in all possible ways in order to prevent and anticipate the crisis.

Sixth. The Russian Federation is being implemented against Ukraine and other states in the region an integral state policy, which security, defence, and economic policy are subordinated to. The same holistic policy has to be directed towards Russia in respond.

Seventh. All foreign economic projects of Russia are means to the goal of global influence on partners and selected victims. There are strong and the same time weak chains of its policy. The Russian endeavor to make harm for Ukraine has speeded up its activity to build the politically motivated gas-pipe routs for Europe bypassing Ukraine. Two strategic gas pipelines Turk Stream and Nord Stream II, figure 2, despite an economic profit for some countries, for Russia are unprofitable and impossible to yield a return in a long-term perspective [3]. Above all, the cost of their continental infrastructure, as Russian experts assess, are five-time more than underwater ones.

Eighth. Awareness of the growing scale of threats in the region. Russia has multiplied and brought the existing challenges and threats behind of the Black Sea region closer to Eastern and Southern Europe. Russia's campaigns in Syria and Libya show that control of the Black Sea is becoming central to a broader strategy and it is another practical step towards dominance in the Eastern Europe, Caucasus, the Eastern Mediterranean and the Middle East. These

days we are witnesses of new development in Nagorno Karabakh and can conclude that not only Azerbaijan is celebrating victory there, but also Russia.

Fig. 2. Russian energy pincer for Europe [10]

Some thoughts about the military lessons learned.

The first lesson - the new military reality requires the new thoughts. As a result of the annexation of Crimea, Russia gained a geostrategic advantage and strengthened its strategic position for further invasions. Russian “near abroad" looks in another way now. The military balance in the region and beyond has changed, and the level of militarization in Crimea, its scale and speed of military transformation are impressive [4; 5; 6].

Second. Russia will never hesitate to carry out armed aggression against neighbouring countries (as it was in 2014), as well as outside the Black Sea region.

Third. Need to learn the experience of counteracting hybrid warfare.

Fourth lesson learned and a task. We must daily conduct tough measures and operations to counter the enemy in Eastern

Ukraine and at the same time to protect national interests in the Black and Azov Seas.

Conclusions

Russia is trying to “force Ukraine into friendship” by military and hybrid means. Unfortunately, Russia discredited the idea of friendship and replaced it by the war. Finding a solution is not only a bilateral problem, but a regional or even global one, and it affects the security of the Black Sea region, the security of Eastern and Central Europe. The Minsk II agreement (February 2015) proves that it is not a road map, but a labyrinth.

Ukraine will not surrender its independence, difficult Ukraine - Russia relations are inevitable. Under such conditions, achieving a just peace between them is a key goal in strengthening security and stability in Europe. The Black Sea region security knot is tight. It will not be resolved itself if Ukraine does not pursue a more effective strategy to deter Russia.

Based on a said above, we can offer some initial recommendations.

First. There is no magic formula that will secure an agreement with Russia on terms that Ukraine and the West can accept. The continued support of the international community and key security organizations for Ukraine, Georgia, and Moldova to develop their national defence capabilities is crucial to create conditions that reduce Russian pressure.

Second. It is necessary to counter the aggressor wherever possible and where its interests are vulnerable.

Thirdly. The unity of the Black Sea Region countries and the world's major security actors in countering Russian aggression is extremely important. Russia is doing its best to break it by relying on the fading memory and often limited attention of democratic societies.

Fourth. Political and economic sanctions against the aggressor prove to be an effective tool of pressure on the aggressor state.

And last but not the least. Ukraine is convinced that it must strengthen its own resilience in order to consolidate the deterrence elements that have already been created during the six-year war against the aggressor within the country.

In order to get resilience what are the priorities for educational institutions?

To counter the enemy, it is necessary to solve three main tasks in the defence:

- strengthening Ukraine's defence capabilities.
- collaborating with our partners, help them and get assistance from them;
- to be interoperable, both within the own defence security sector and with our international partners.

These tasks are performed by our servicemen, representatives of the security sector, the defence industry. They have to get a proper education. That is why the education becomes a priority and it is advisable to identify such preliminary four areas for it.

1. To develop a modality of joint education for defence and security specialists. All of them, in accordance with their positions, have to know the essence of HW, the principles of crisis management, new forms and methods of troops performance in order to implement the strategy to counter the aggressor.

2. Review the content of the educational process in the universities. We are doing a lot, we got a lot of experience, but we are still lagging behind today's requirements.

3. To increase the efficiency of education for our officers cadets and civilians we have:

- to develop theory and practice of hybrid warfare, to implement lessons-learned and exchange them among professionals;
- to raise the professional level of the faculties;
- more effective use of our scientific and military publications, journals;
- to learn the experience of Russian hybrid warfare (from their sources as well);
- to put an attention to the libraries. Do not save on

subscriptions of the foreign journals (also Russian military publications);

- to educate the leaders. The developing of the leadership courses in the National Defence University of Ukraine - is the right way.

4. To educate of interoperability as a basis of effective interaction. The main direction: English language training, education of NATO's procedures and communication. It is a difficult task, but we are not pioneer in solving it.

References

1. Sherr, J. (2020), *Nothing New Under the Sun? Continuity and Change in Russian Policy Towards Ukraine*, International Center for Defence and Security, available at: https://icds.ee/en/nothing-new-under-the-sun-continuity-and-change-in-russian-policy-towards-ukraine (accessed 11 January 2021).

2. Clark M. (2020), *Russian Hybrid Warfare*, Institute for the Study of War, available at: https://cutt.ly/sjc94K5 (accessed 11 January 2021).

3. Klymenko, A., Guchakova, T. and Korbut, O. (2020), *Russia's Economic War Against Ukraine in the Sea of Azov and COVID-19. The Monitoring Results for May 2020*, Crimean Tatar Resource Center, available at: https://cutt.ly/yjc3EIP (accessed 11 January 2021).

4. Hudson Institute Center for American Seapower (2016), *Why The Black Sea Matters*, p. 5, available at: http://newstrategycenter.ro/wp-content/uploads/2016/04/Policy-Paper-NSC-and-Center-for-American-Sea-Power.pdf (accessed 11 January 2021).

5. Klymenko A. (2020), Naval warfare scenarios for 2020, *UA: Ukrainian Analytica*, No. 1(37), pp. 24-28 available at: https://cutt.ly/Djc8WcA (accessed 11 January 2021).

6. Păcuraru C.G. (2020), Ukraine and the Russian Energy Blackmail, Black Sea Security, *Analytical Journal*, No. 1(37), p. 68, available at: https://geostrategy.org.ua/en/black-sea-security/black-sea-security-1-37-2020/zavantazhiti-zhurnal-1-37-2020 (accessed 11 January 2021).

7. Stercul, N. (2020), Security Issues of the Republic of Moldova in the Context of Militarization of the Black Sea Region, Black Sea Security, *Analytical Journal*, No. 1(37), p. 38, available at: https://geostrategy.org.ua/en/black-sea-security/black-sea-security-1-37-2020/zavantazhiti-zhurnal-1-37-2020 (accessed 11 January 2021).

Oleksandr Kovalenko
Graduate Student of Dnipropetrovsk Regional Institute
for Public Administration National Academy for Public
Administration under the President of Ukraine
Dnipro, Ukraine
https://orcid.org/0000-0001-8612-3674

INTERNAL COMMUNICATIONS IN THE ARMED FORCES OF UKRAINE IN COUNTERACTING HYBRID AGGRESSION IN THE ASPECT OF STRATEGIC COMMUNICATIONS

Abstracts of the report describe internal communications in the Armed Forces of Ukraine in combating hybrid aggression in terms of strategic communications. The subject is theoretical and methodological principles, organizational features of internal communications in the Armed Forces of Ukraine in combating hybrid aggression. The object is strategic communications in the Armed Forces of Ukraine. The aim is to investigate the main problems of Internal Communications in the Armed Forces of Ukraine in counteracting hybrid aggression. To analyze and generalize the theoretical foundations of internal communications as an element of strategic communications in the Armed Forces of Ukraine.

The following methods were used to achieve the goal and solve the research tasks:

– theoretical: analysis, synthesis, classification and generalization of domestic and foreign scientific literature - to determine the state of research of the problem of internal communications in the Armed Forces of Ukraine; method of system analysis - to determine the requirements for the level of professional training of specialists in moral and psychological support, the characteristics of the system of advanced training; systematization method - to characterize the concepts and definitions of the system of moral and psychological support; structural-functional, comparative-analytical methods - for systematization of works on the research topic; methods of analysis, synthesis, induction, deduction - to structure developments and proposals for the theory and practice of internal communications as an element of strategic communications;

– empirical: analysis and generalization of experience - to

clarify the features of internal communications in the Armed Forces of Ukraine; comparison - to generalize and systematize the actual material on the content, organizational forms and methods of internal communications as an element of strategic communications.

The research results are a description of the system of internal communications as an element of strategic communications in the Armed Forces of Ukraine; the organizational features of the system of internal communications as an element of strategic communications in the Armed Forces of Ukraine in counteracting hybrid aggression in the aspect of strategic communications are clarified.

Keywords: *internal communications, strategic communications, public administration.*

Introduction

Society develops through communication between people. But man, as a social being, is formed in society. The human need for information is one of the most pressing. In the age of the digital society, the thesis "whoever manages information wins and succeeds" becomes important. The main factor influencing the achievement of success in a combat situation is the possession and management of commanders and personnel operational, reliable, truthful information in the part that concerns them [1]. So the question arises, how to increase the level of internal communications in the Armed Forces of Ukraine for a better understanding of the narratives of the strategic communications of the state? How will this affect the moral and psychological state (fighting spirit) of the staff?

Problem statement. The report attempts to analyze the development of internal communications in the Armed Forces of Ukraine. How were internal communications organized in the Armed Forces of Ukraine during the period of counteraction to Russian aggression in the east of the country. What forms and methods were used? How much has the development of internal communications in the Armed Forces of Ukraine compared to party and political work in the military units of the Soviet Army?

Purpose of the report is to find, improve, supplement or deepen already known approaches to internal communications as an

element of strategic communications in the Armed Forces of Ukraine.

The analysis of recent research and publications. Internal communication is a part of management process, through which information is shared, collected and distributed, as to ensure employee understanding of the organization's goals and objectives [2]. Internal communication plays a key role in keeping the employees informed about the organization's plans, vision and ideas, but also encourages them to participate in the decision-making processes, as well as promotes employee feedback and peer learning. Traditionally, management transmits information to employees in the top-down fashion [2]. In recent decades, the role of internal communication has expanded, so that it now tends to be bottom-ip, i.e. feedback and inputs are collected from employees. It has been noted that internal communication has progressively become more horizontal, i.e. employees tend to communicate and share messages between themselves without any hierarchical consideration [2].

Other researchers note the positive consequences of internal communication, such as more effective changes and decision-making, and higher engagement of employees, all of which leads to more productive work and less risk of failure and losses during the change processes [2].

Some scholars also note the possible negative consequences of internal communication, which leave people feeling insecure about hierarchical structures, poor control of information flow, or insufficient time, devoted to explaining information to participants. All of this makes internal communication an important, yet challenging area to achieve effective change in an enterprise [2].

How do enthusiastic internal communication versus actual organizational practices impact employees' perceptions of their organizational brand in a sector challenged by tough working conditions, negative publicity, and strongly criticized reforms? While previous studies and managerial practice do not uniformly answer this question, we can assume that the demanding conditions that characterize the public sector represent an interesting and unique

contextual setting for examining employees' perceptions [3].

Thus, the issues of internal communications, although studied by scientists, but as an element of strategic communications in the Armed Forces of Ukraine need further study.

Main part

Specialists in internal communications in the military units of the Armed Forces of Ukraine since the beginning of the hybrid war between Ukraine and the Russian Federation can essentially be considered deputy commanders of military units (subdivisions) to work with personnel, and since 2016 - deputy commanders of military units (subdivisions) psychological support. But at the beginning of 2014, there was virtually no significant progress in the methods and forms of work on internal communications compared to the institution of "Comsorg" and deputy commanders for the political part of the Soviet Army. The same functions: informing, working with leaders, supporting military traditions; the same tools: wall and photo newspapers, newsletters, military and ideological training, plaques of honor, ethnographic rooms, etc. In 2014, the system of working with personnel was not fully ready to work in the conditions of hostilities, which had an impact at the initial stage of confrontation with the enemy in eastern Ukraine.

Communication is the exchange of information between people and their associations in the process of interaction, activity and communication. Internal communications - is the management of the exchange of targeted information within the military unit (subdivisions): between individual servicemen, units, commanders and subordinates, and so on [1].

The process of communicating with different target audiences should be continuous, coordinated and carried out at the strategic, operational and tactical levels with the involvement of a large number of actors.

At the strategic level, these are strategic communications that are of interest to many foreign and domestic scientists. Strategic communications are devoted to the study of experts both on the

transformation of the system of international relations under the influence of the communication factor, and on clarifying the mechanisms of international cooperation in a crisis.

The founder of the concept of strategic communications is objectively considered to be the United States, where the first definition of “strategic communications” in the Pentagon documents appeared in the early XXI century, in 2006. In general, strategic communication is the process of supporting a country's foreign policy strategy to coordinate actions, messages, images and other forms of visualization designed to inform, influence the target audience and support foreign policy interests [4].

The relationship between national strategy and strategic communications can only be strategically important when clearly defined national goals, including nested intermediate or ancillary goals, are all the way to the operational and tactical levels [4].

In general, it should be noted that the problem of strategic communications has become scientifically popular only in the last twenty years, although previously actively used mainly in the United States in military, scientific, political and commercial aspects. The effectiveness of this toolkit has provoked its spread to other aspects of public life in many countries: the United States, China, the EU and NATO in general, which use it to effectively implement domestic and foreign policy [5].

Most attention is paid to strategic communications in NATO, where this area has been institutionalized since 2007, is a separate unit was created - the Department of Strategic Communications. Subsequently, NATO singled out the area of strategic communications, which includes research, experience, and the development of communication and information technologies, which has contributed to the creation of the Center for Excellence in Strategic Communications (StratCom). StratCom has put into scientific use the definition of strategic communications used today as the coordinated and appropriate use of NATO's communications and capabilities to support Alliance policies, operations and activities, and to advance NATO's goals. And identifies the main

capabilities / components: public diplomacy, public relations, military public relations, information and psychological operations. The main goal of the subjects of strategic communications is to convince the target audience that NATO is open and transparent in its actions, an effective, cohesive and vital organization, without which global security is impossible [5, 14].

Strategic communications are interpreted as actions aimed at understanding and engaging the target audience to create, strengthen and maintain an enabling environment to achieve government goals, interests and policies by coordinating programs, plans and key messages. Strategic communications are also seen as a process of combining the perception of the audience and stakeholders with the results obtained during the implementation of planning policy [6]. Thus, strategic communications are a public activity that includes public relations, information operations, diplomatic events and other actions of players in the political arena to ensure the support of the foreign policy interests of the state.

Strategic communications are, first of all: a systematic series of long-term and consistently interconnected actions carried out at the strategic, operational and tactical levels of management, which is aimed at achieving strategic goals; concerted actions, messages, insults and other forms of representation or interaction designed to inform, influence or persuade society in order to support national interests; a set of measures aimed at managing target audiences both within the country and abroad, etc.

Military Standard 01.004.007, approved by the order of the Head of the Department of Standardization, Codification and Cataloging of the Ministry of Defence of Ukraine dated December 20, 2017 No. 15 defines strategic communications as “coordinated and proper use of communication capabilities of the state - public diplomacy, public relations, military communications" languages, information and psychological operations, other subjects of information activities in order to implement measures aimed at promoting the goals of the state” [7].

With the Russian Federation launching a hybrid war against

Ukraine, which manifested itself in the annexation of Crimea and the outbreak of hostilities in eastern Ukraine under the guise of the "Donetsk People's Republic" and "Luhansk People's Republic" terrorist groups, the lack of a strategic communications system became acute. At the initial stage of the "hybrid war", all measures to influence the target audience were carried out unsystematically and only as a consequence of countering the influence of hostile media in the information environment, which led to failures in counteracting the negative disinformation of the enemy. Accordingly, there were violations of internal communications in the military units of the Armed Forces of Ukraine. The enemy's propaganda and dissemination of false information through the media and social networks had a significant impact on both the military and the citizens of Ukraine as a whole. The existing system of work with personnel in the Armed Forces of Ukraine at that time was not ready to act effectively during hostilities. In 2014-2015, during the Anti-Terrorist Operation, there were cases when not only individual servicemen, but entire groups and even units sabotaged the implementation of certain tasks.

To improve the state of affairs in the internal communications of the military units of the Armed Forces of Ukraine during the measures of moral and psychological support during the Anti-Terrorist Operation by the order of the General Staff of the Armed Forces of Ukraine dated December 03, 2015 No. 472 was approved the Program for establishing internal communications of the Armed Forces of Ukraine. Highly mobile groups of internal communications were created from among servicemen and employees of the Armed Forces of Ukraine, who underwent appropriate training and coaching. The group, which was tasked with assisting officials in maintaining and restoring the necessary morale (moral and psychological state) to provide information and psychological support, was named "Alpha". Highly mobile internal communications group "Alpha" consisted of an inspector, an ideologist, a military chaplain and a military psychologist. The information obtained during the work of these groups in military

units through the Main Department of Moral and Psychological Support of the Armed Forces of Ukraine was provided personally to the Chief of the General Staff - Commander-in-Chief of the Armed Forces of Ukraine. Subsequently, the activities of highly mobile groups of internal communications were somewhat improved, the order of the General Staff of the Armed Forces of Ukraine dated December 22, 2018 No. 345 “On approval of the Instruction on the organization of highly mobile groups of internal communications in the Armed Forces of Ukraine”, and the order dated December 3, 2015 No. 472 has expired [8].

During the combat use of the Armed Forces of Ukraine in the anti-terrorist operation in Luhansk and Donetsk oblasts, it became clear that such tools as a wall newspaper and military-ideological training were obsolete. For platoon and company bases of brigades stretched along the front, timely proof of truthful information about the actions of the top political leadership of Ukraine and the Armed Forces of Ukraine proved to be problematic. The situation was significantly complicated by the fact that these units were in the zone of stable reception of television channels of “Donetsk People's Republic” and “Luhansk People's Republic” terrorist groups. There was a constant propaganda of the “Russian world”. Since 2016, the channel “Informing ATO soldiers” was created with the help of the Telegram messenger. There were initially connected deputy commanders of military units (subdivisions) for the moral and psychological support of military units, who performed tasks in the anti-terrorist operation. Subsequently, the deputy commanders of the military units for moral and psychological support disseminated information prepared by the Center for Moral and Psychological Support of the Armed Forces of Ukraine in their own groups and channels. Later, military officials were attached to this channel, who, being in the area of anti-terrorist operation tasks, had to conduct commander's briefings, starting with the branch commander. Now this channel continues to successfully disseminate the necessary information, has more than 1,000 users and is called “Informing the soldiers of the Joint Forces operation”.

This is a good example of successful changes in internal communications in the Armed Forces of Ukraine.

The Order of the Ministry of Defence of Ukraine dated November 22, 2017 No. 612 approved the Concept of Strategic Communications of the Ministry of Defence of Ukraine and the Armed Forces of Ukraine. According to this order, internal communication is implemented by the Main Department of Moral and Psychological Support of the General Staff of the Armed Forces of Ukraine. The concept defines the activities for the preparation and implementation of strategic communications, other information activities are part of the activities of commanders (commanders), heads of military authorities at all levels. Commanders (commanders) and staffs of all levels are directly involved in the organization of actions in the information space in peacetime and in special periods, during the preparation and conduct of operations (combat operations). Each of the bodies of military management, depending on its powers, develops and plans measures and actions of subordinate troops (forces), which are united by a single plan of action in the information space [9].

In order to improve the moral and psychological condition of the military units of the Armed Forces of Ukraine, the existing system of work with personnel at that time was revised. In 2016, in the Armed Forces of Ukraine, the bodies for work with personnel were transformed into bodies of moral and psychological support. The purpose and their main functions have acquired a new meaning. The main purpose of moral and psychological support for the training and use of the Armed Forces of Ukraine, as a type of comprehensive support, was determined - the formation, maintenance and restoration of moral and psychological condition of troops (forces) necessary for successful tasks.

The Guidelines on Moral and Psychological Support of Training and Application of the Armed Forces of Ukraine, approved by the order of the General Staff of the Armed Forces of Ukraine on April 27, 2018, have been implemented in the activities of military administration bodies and military units. According to the Guidelines,

internal communication work is a direction of information and propaganda support and is implemented by: establishing a communication process, systematic and targeted propaganda (counter-propaganda), ideological, informational, national-historical, military-social work with personnel; coordination of pastoral care of servicemen; spreading a healthy lifestyle; participation in measures to protect against the negative information and psychological influence of the enemy; systematic analysis of actions taken; providing commanders of military units (subdivisions) and their deputies for moral and psychological support with applied methodological materials necessary for information work with personnel in the conditions of preparation and conduct of operations (combat operations); providing troops (forces) with periodicals, etc. [10].

The direct executors of internal communication work in military units are commanders, staffs, deputy commanders for moral and psychological support at all levels. When carrying out measures of moral and psychological support, officials of military units are guided not only by the above Guidelines for moral and psychological support of training and use of the Armed Forces of Ukraine but also by the order of the General Staff of the Armed Forces of Ukraine from January 4, 2017 No. 4 in the Armed Forces of Ukraine. It was more detailed and revealed the content of such a component of moral and psychological support as information and propaganda support. The definition of internal communication work as a direction of information and propaganda support of military units (subdivisions), military educational institutions, establishments and organizations of the Armed Forces of Ukraine, carried out in the system of information work of military officials, commanders (chiefs) through a set of actions related to the processing and transmission of information to personnel through communication [11]. This order discloses the purpose, types, basic principles which should be followed by officials of military units of the Armed Forces of Ukraine in conducting internal communication work.

On October 12, 2020, the Commander-in-Chief of the Armed Forces of Ukraine approved the Doctrine on Strategic

Communications of the Armed Forces of Ukraine, which provides the following definitions: “Internal audience - military and civilian personnel of the Armed Forces of Ukraine and their families (immediate environment). Internal communications - communicative activities aimed at the internal audience, which has a connection with the Armed Forces of Ukraine” [12].

The doctrine on strategic communications of the Armed Forces of Ukraine was developed by the working group of the Strategic Communications Department of the Office of the Commander-in-Chief of the Armed Forces of Ukraine and is intended for use by officials in military administration. It states: “Internal communications is a mandatory element of the system of strategic communications of the Armed Forces of Ukraine, the main purpose of which is to ensure effective exchange of targeted information within the military structure, organization, unit (subdivision), as well as between individual servicemen, units, commanders and subordinates, etc. Internal communications are the main motivating factor that influences success in a combat situation. Possession of operative, reliable, truthful information by commanders and personnel strengthens the moral and psychological condition of all personnel, promotes trust in the actions of the military leadership” [12].

The main tasks of internal communications in accordance with the Doctrine of Strategic Communications of the Armed Forces of Ukraine include:

- satisfaction of information needs of personnel (in particular through systematic commander's (combat) informing of personnel);
- proving and explaining the goals and objectives of the activity;
- establishing two-way communication between management and personnel (in particular, using the methodology of “After Action Review (AAR)”, the results of internal communications groups, etc.);
- introduction and observance of military traditions;
- ensuring the leadership of servicemen;

- improving the processes of objective information in departments;
- motivation of subordinates [12].

Internal communication work with the doctrine “Moral and psychological support of troops (forces) in joint operations”, approved by the Chief of the General Staff of the Armed Forces of Ukraine on October 27, 2020, is allocated as a separate component of moral support. Other components included: information support; national-patriotic work; culturological work, organization of leisure and recreation [13].

Internal communications are certain networks. The type of internal communication networks directly affects the efficiency, success and leadership of the commander (chief), the military unit (subdivision) as a whole [1].

The success of command, control and leadership depends on whether you have been able to establish effective internal communications in the subordinate military unit. The main rule of internal communications of a military leader is to establish trusting and loyal relations with subordinates (followers, comrades). Communications with personnel should work in all directions - vertically - from bottom to top, from top to bottom and horizontally. But the main result of this process should be the availability of feedback and awareness of people [1].

Conclusions

Without effective internal communication work with personnel in the military unit, it is impossible to achieve high combat capability of the unit. For example, everyone in a unit can be an excellent marksman, operator, driver, cook, and so on, but without combat coherence, without teamwork, without well-established communication, a military unit will be ineffective and the unit will not be considered fully combat-ready. Each platoon or company separately can be quite capable, but without effective internal communication in the regiment or brigade, violations of communication between platoons and companies, the effectiveness

of combat use of the battalion or brigade falls sharply.

Thanks to the experience of using the Armed Forces of Ukraine in repelling Russian aggression in the east, internal communications in the Armed Forces of Ukraine as an element of strategic communications have been further developed. The normative documents gave definitions of this work and its main tasks. The latest communication technologies with the help of social networks and messengers were introduced.

The historical experience of wars and military conflicts shows that wars have always been won by those who could better coordinate and combine the command interaction of hundreds and thousands of armed soldiers in order to win even a much larger army.

References

1. Center for Moral and Psychological Support of the Armed Forces of Ukraine (2020), *Internal communications of the military leader. A guide for officers and sergeants. VP 1-00(31).01*, Publisher Center for Moral and Psychological Support of the Armed Forces of Ukraine, Kyiv, 15 p., available at https://cutt.ly/yjFeQtC (accessed 20 January 2021).

2. Kovaitė, K., Šūmakaris, P. and Stankevičienė, J. (2020), Digital communication channels in Industry 4.0 implementation, *Management*, 25(1), pp. 171-191. https://doi.org/10.30924/mjcmi.25.1.10.

3. Leijerholt, U., Biedenbach, G. and Hultén, P. (2020), Internal brand management in the public sector: the effects of internal communication, organizational practices, and PSM on employees' brand perceptions, *Public Management Review*, pp. 1-24. https://doi.org/10.1080/14719037.2020.1834607.

4. Paul, Ch. (2011), *Strategic Communication: Origins, Concepts, and Current Debates*, ABC-CLIO, Santa Barbara, 240 p.

5. Syvak, T. (2019), International experience of formation of strategic communications, *Actual Problems of Public Administration*, 2(78), pp. 81-86. https://doi.org/10.35432/1993-8330appa2782019179084.

6. NATO (2017), *NATO strategic communication handbook. V1.0*, available at https://cutt.ly/IjFro5n (accessed 20 January 2021).

7. Ministry of Defence of Ukraine (2017), *Military standard 01.004.007, The system of strategic communications of the state in the military sphere. Terms and definitions*, available at: https://cutt.ly/CjA225O (accessed 20 January 2021).

8. General Staff of the Armed Forces of Ukraine (2018), *Order No. 345 "On approval of the Instruction on the organization of highly mobile internal communications groups in the Armed Forces of Ukraine"*, available at: https://dovidnykmpz.info/zagalni/nakaz-heneral-noho-shtabu-zs-ukrainy-v-2/ (accessed 20 January 2021).

9. Ministry of Defence of Ukraine (2017), *Order No. 612 "On approval of the Concept of strategic communications of the Ministry of Defence of Ukraine and the Armed Forces of Ukraine"*, available at: https://cutt.ly/ejA9z28 (accessed 20 January 2021).

10. General Staff of the Armed Forces of Ukraine (2018), *Order No. 173 "On approval of the Guidelines on moral and psychological support for the training and use of the Armed Forces of Ukraine"*.

11. General Staff of the Armed Forces of Ukraine (2017), *Order No.4 "On approval of the Instruction on the organization of information and propaganda support in the Armed Forces of Ukraine"*, available at: https://cutt.ly/9jA9ARP (accessed 20 January 2021).

12. General Staff of the Armed Forces of Ukraine (2020), *Doctrine on strategic communications of the Armed Forces of Ukraine*, approved by the Commander-in-Chief of the Armed Forces of Ukraine on October 12, 2020, VKP 10-00 (49).01., General Staff of the Armed Forces of Ukraine, Kyiv, available at: https://cutt.ly/4jSjDlP (accessed 20 January 2021).

13. General Staff of the Armed Forces of Ukraine (2020), *Doctrine "Moral and psychological support of troops (forces) in joint operations"*, approved by the Chief of the General Staff of the Armed Forces of Ukraine on October 27, 2020, VKP 1.58 (31).01., available at: https://cutt.ly/kjSj40w (accessed 20 January 2021).

14. NATO (2017), *NATO Military Policy on Strategic Communication*, available at: https://cutt.ly/FjFrBg6 (accessed 20 January 2021).

Anatolii Mysyk
Doctor of Military Sciences, Associate Professor
Professor of the Department of National Security and Management
of the National Academy of the State Border Guard Service
of Ukraine named after Bohdan Khmelnytskyi
Khmelnytskyi, Ukraine
https/orcid.org/0000-0003-2378-9887

Oleksandr Andrushko
Doctoral Student of the National Academy of the State Border Guard
Service of Ukraine named after Bohdan Khmelnytskyi
Khmelnytskyi, Ukraine
https/orcid.org/0000-0001-5026-1653

MODEL OF ACTIONS OF UNITS OF THE STATE BORDER GUARD SERVICE OF UKRAINE IN THE SYSTEM OF ANTI- SABOTAGE STRUGGLE IN THE JOINT FORCES OPERATION

The report presents the results of a research that examines the actions of border units in the anti-sabotage struggle system in the Joint Forces Operation. The topic of the report is "Model of actions of units of the State Border Guard Service of Ukraine in the system of anti-sabotage struggle in the Joint Forces Operation." The purpose of the research is to increase the quality of decisions on the use of units and subdivisions of the State Border Guard Service of Ukraine in the Joint Forces Operation (JFO). A comprehensive model of actions of border units has been developed, which includes a model of conducting reconnaissance to detect sabotage and reconnaissance groups (SRG) of the enemy while trying to cross the state border, a model of identifying SRG, a model of choosing methods of action of service elements during search and detention (disposal) of SRG . The model is based on the assessment of the capabilities of units and elements of service. Its use in the work of the SBGS governing bodies will increase the quality of decisions on the actions of units in the system of anti-sabotage struggle.

Keywords: *unit action model, State Border Guard Service of Ukraine, sabotage and reconnaissance group, border units, state border, anti-sabotage struggle.*

Introduction

Problem statement. In modern conditions, together with the classical methods of combat operations, stabilization actions (operations), which form the basis for the implementation of the concept of preventive defense, become especially important. Tasks to ensure the protection and defense of the state border, stop provocations, combat sabotage and reconnaissance groups (DRG) during participation in stabilization operations in accordance with the Concept of Development of the Security and Defense Sector of Ukraine are entrusted to units of the State Border Guard Service of Ukraine. Conditions of struggle against SRG differ in features of actions of the opponent and tasks of the parties, and accordingly by ways of their performance, that is tasks have elements of uncertainty.

Their specificity is the lack of clearly defined methods of implementation. As a special purpose law enforcement unit, SBGS units and subdivisions are used both as security forces and as defense forces. That is additional uncertainty about their role and place in the fight against SRG and about determining their capabilities. Nevertheless, the SBGS governing bodies are obliged to determine the tasks of counteracting the SRG in accordance with the capabilities of subordinate units.

That is, the problematic situation in the practice of deciding on the use of SBGS units in the fight against sabotage and reconnaissance groups is the objective need to reasonably determine the scope of tasks for border units and elements of duty in accordance with their capabilities and incomplete scientific and methodological apparatus for this management task.

The model of actions of border units should provide an assessment of their capabilities and predict the effectiveness of actions in the system of anti-sabotage in the joint forces operation.

The analysis of recent research and publications: The work of many scientists is devoted to the study of the problem of anti-sabotage struggle by units of various departments.

The authors [1] based on the analysis of the actions of

sabotage and reconnaissance forces determine their role in armed conflicts and the main forms and methods of application.

The authors [2–3] developed a model of decision-making on the methods of action of the elements of the service-combat order of the state border guards with known values of their capabilities and the parameters of the situation.

The application of methods of game theory to the choice of methods of action of troops and forces in armed conflicts is proposed by the authors of the articles [4–5].

The author [6] developed a model for determining the ability of border units to fire on entry-exit checkpoints. The technique can be used to assess the ability to perform fire tasks.

The analysis of the existing scientific and methodological apparatus shows that it allows to solve some problems of substantiation of decisions on struggle against SRG, however does not provide an estimation of abilities of border units and service elements on the implementation of tasks in the system of anti-sabotage struggle. This negatively affects the quality of decisions made and can lead to non-fulfillment of tasks and unjustified losses. This confirms the urgency of improving the scientific and methodological apparatus of substantiation of decisions on the use of border units in the system of anti-sabotage struggle.

Purpose of the article is defined as the development of a model of action of units of the State Border Guard Service of Ukraine in the system of anti-sabotage struggle in the operation of the joint forces.

Main part

One of the main trends influencing the military-political situation in the region around Ukraine, the creation and development of conflict situations is the spread of the practice of special operations, which are based on sabotage and reconnaissance operations. The enemy's sabotage and reconnaissance forces will act comprehensively, according to the general plan and plan for the entire depth of the territory of Ukraine. Security and defense forces must oppose this

system of subversive struggle with a systemic anti-sabotage struggle. Interagency groups in military situations will operate comprehensively, combining defense, special and law enforcement measures. This requires the development and application of non-traditional methods of action and their combination.

The SBGS is tasked with participating in the cessation of armed conflict at the state border and in the fight against terrorism; cessation of armed and other provocations at the state border; protection of the state border and sovereign rights of Ukraine in its exclusive (maritime) economic zone.

The content of the anti-sabotage struggle as a separate type of military action has a high degree of uncertainty. First of all, these actions should ensure control of the conflict situation, maintenance of security and stability, creation of conditions for the termination of the conflict and prevention of its resumption. The SBGS has a significant role in such actions.

To study the role, place and tasks of SBGS units and subdivisions in the anti-sabotage struggle system, the peculiarities of the nature and tactics of sabotage and reconnaissance groups, the content of tasks of military formations and law enforcement agencies in possible scenarios of the situation that may arise in stabilization operations, and factors determine the tasks and actions of border units.

In the course of the aggression, the enemy intensifies throwing agents, emissaries of separatist and hostile structures, groups of psychological operations, and organizers of "guerrilla detachments" through the existing checkpoints and positions. Agent networks are being deconserved and new ones are being created, and gangs and detachments are being prepared for active action. The most probable channel of SOF penetration on the land sections of the border is considered to be illegal crossing in hard-to-reach areas and by air.

The experience of hostilities shows that the main objects of reconnaissance and sabotage are: nuclear power plants, airfields, missile and artillery positions, radio and radio reconnaissance posts, regular means of covering the state border, bridges, etc. To ensure success, the enemy will seek to disrupt the regrouping and deployment of troops.

The main objects of SRG activity will be air defense units and subdivisions, EW, airfields and aviation landing sites, control points, communications, important areas, etc. Active counteraction to the penetration of sabotage and reconnaissance formations and groups across the state border into the areas of operational deployment of troops and the fight against them in border areas is the most important task of SBGS formations that have practical experience and preparation for such tasks.

Existing forms of operational and service actions, tasks of SBGS formations are undergoing significant changes. One of the main elements of the SBGS's activities to combat SRG is the use of mobile units and combat reserve units. They are used to step up efforts to protect the state border. SBGS units take part in joint patrols, special operations (counter-sabotage, psychological, search, reconnaissance and combat operations, etc.). A particularly important role of SBGS units and subdivisions is assigned to conducting reconnaissance in order to expose the SRG when attempting to cross the state border. In order to counter the SRG, ground reconnaissance is intensified due to the existing observation towers, hidden posts that provide continuous monitoring of the border and the area to a depth of 15 km. Due to the SBGS units, the number of observation posts is growing by 40-50%, the number of reconnaissance groups is significantly increasing, and the ground radar reconnaissance zone is being strengthened.

The participation of SBGS units and subdivisions in the anti-sabotage struggle is determined by the following components of their capabilities: legally defined functions and tasks; spatial framework for action within controlled border areas (CBA); focus on training to counter small groups of the enemy; a combination of law enforcement and military functions; knowledge of the area and work with the local population, conducting operational and investigative activities; availability of continuous reconnaissance of the state border line and the CRC strip; ability to perform tasks by small separate units and border guards; ability to carry out activities of different directions: regime; stabilization and combat. The developed model is based on the

assessment of the capabilities of SBGS units and elements of official order to perform reconnaissance, identification and participation in the destruction (capture) of SRG, taking into account the conditions and factors that determine the system of anti-sabotage and reconnaissance groups (DRG). The main indicator of the effectiveness of actions during their planning and preparation is the degree of influence of the created (achieved) capabilities (properties) on the ability of units to perform tasks, and the results of actions: change of conditions, methods of action and freedom of action of the enemy or their troops). Evaluation and selection of the required projected result of the actions of border units is carried out using the method of analysis of hierarchies. The quality of decisions is assessed by indicators of suitability and acceptability.

Based on the results of the study of the peculiarities of the use of SBGS units in the anti-sabotage struggle system, the improvement of the scientific and methodological apparatus is based on the model of SRG reconnaissance when trying to cross the state border and move within the controlled border area, the model of SRG identification time of search and detention (neutralization) of SRG.

The SRG reconnaissance model when attempting to cross the state border and move within a controlled border area is based on an assessment of the intelligence capabilities of units and elements of the official order. Methods of operational and tactical calculations are used to assess the ability.

The SRG identification model is based on the procedures of analysis of SRG reconnaissance features and formation of a taxonomic indicator of the ratio of detected objects to SRG.

The model of the choice of modes of action of the elements of the official order includes the model of search, the model of fire confrontation, the model of the choice of the variant of modes of action.

The model of choosing a variant of methods of action is based on the use of the matrix method, the method of analysis of hierarchies and the game method. The model allows you to form and choose ways of action as a set of appropriate tactics that are able to implement elements of the order.

Conclusions

The developed comprehensive model of actions of SBGS units in the anti-sabotage struggle system allows to study the capabilities of border units and elements of official order, substantiate tasks and methods of their implementation, predict the effectiveness of actions and can be used in the decision support system of the head of the state border guard.

References

1. Panchenko, V.Yu. and Radchenko, I.O. (2016), "Analiz dosvidu proty dyversiinykh dii viiskovykh formuvan u viinakh ta zbroinykh konfliktakh" [Analysis of employment of counter sabotage action of units in wars and armed conflicts], *Scientific Works of Kharkiv National Air Force University*, Vol. 1(46), pp. 34-36.

2. Horbatiuk, A.P. (2018), "Model pryiniattia rishennia shchodo sposobiv dii elementiv sluzhbovo-boiovoho poriadku orhaniv okhorony derzhavnoho kordonu v stabilizatsiinykh diiakh" [Model of making decisions concerning methods of operation for service and fighting order elements of the state border guard units in stabilization actions], *Science and Technology of the Air Force of Ukraine*, No. 4(33), pp. 99-106. https://doi.org/10.30748/nitps.2018.33.13.

3. Katerynchuk, I., Mysyk, A. and Horbatiuk, A. (2017), Model of joint actions of military units and law enforcement agencies during the implementation of territorial defense tasks, *Collection of scientific works of the National Academy of the State Border Guard Service of Ukraine*, Vol. 1, pp. 87-106.

4. Nazarenko, V. and Omelchuk, V. (2013), Recommendations for crushing defeat of sabotage and reconnaissance groups of enemy and illegally formed armed units while covering a sector of the state border, *Proceedings of the University*, No. 5(119), pp. 66-70.

5. Seratiuk, V. and Nedilko, O. (2009), Choice of a combat deployment method of an integrated combined arms force, *Proceedings of the University*, No. 1(88), pp. 60-65.

6. Fedorchuk, A. and Oleksiienko, B. (2019), Theoretical and methodological results of the study on the assessment of the ability of the border detachment to perform fire cover tasks at entry-exit checkpoints, *Collection of scientific works of the National Academy of the State Border Guard Service of Ukraine*, No. 2(80), p. 196-210. https://doi.org/10.32453/3.v80i2.199.

Yugenii Pankratov
Candidate of Military Sciences
Deputy Chief of the Department of National Security
and Defence Strategy of National Defence University of Ukraine
named after Ivan Cherniakhovskyi,
Kyiv, Ukraine
https://orcid.org/0000-0001-8050-8813

Vitalii Shevchuk
Candidate of Military Sciences
Chief of the Military Security Research Laboratory of the National
Security and Defence Strategy Department of the National Defence
University of Ukraine named after Ivan Cherniakhovskyi,
Kyiv, Ukraine
https://orcid.org/0000-0002-8532-739X

Andrii Kruzhylko
Postgraduate Student of the Department of National Security
and Defence Strategy of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org 0000-0002-8824-7459

SOME ISSUES OF PLANNING THE DEFENSE OF THE STATE TAKING INTO ACCOUNT SYSTEM FEATURES OF MODERN MILITARY CONFLICTS

Based on the existing approaches to the planning of defense states, taking into account historical experience, studying the course of origin and identification of local wars and armed conflicts of today, the peculiarities of today's conditions for which defense planning is carried out are analyzed. There is an obvious need to revise conceptual approaches to defense planning that take into account the conditions of a hybrid war against Ukraine. The aggression of the Russian Federation against Ukraine showed that our country was not ready to adequately respond to the threats in the military sphere and other modern challenges, which forced the top military and political leadership to reconsider approaches to the formation and implementation of defense

policy in general and the planning process. defense of Ukraine in time.

Thus, understanding the experience of confrontation with the Russian Federation in a hybrid war, clarifying the priorities for further improvement of the process of state defense planning is an urgent task.

Keywords: *defense planning, hybrid war, hybrid threats, military conflict, defense, defense plan.*

Introduction

Problem statement. In modern military conflicts, there is an increasing tendency when the goal of the aggressor states is not the physical destruction of the enemy or the infrastructure of the state, but the complete subordination of the leadership and elite of the country-victim of their will. This is achieved through the use of various technologies and means of influence. They are increasingly based on non-standard or so-called hybrid actions, which include measures of both a military nature and measures without the use of military force. The Russian Federation has long been actively implementing "hybrid methods" in the interests of achieving its military-strategic goals in various regions of the world, such as Ukraine, Moldova, Georgia, Libya, Syria, Venezuela, Belarus and others.

Today, Ukraine's security and defense sector faces the task of rethinking Ukraine's defense planning process. This is the first time that a comprehensive approach to defense planning in Ukraine, covering most areas of the state's life, has been introduced. The starting point of this process was the adoption of the Law of Ukraine "On Amendments to the Law of Ukraine" On Defense of Ukraine "on the organization of national defense", which, inter alia, provides for the development and approval of Ukraine's defense plan [1]. Immediately after the beginning of this process, a number of conceptual problems arose - what should be the content of this process; how it should combine issues of generation and use of forces that public authorities should participate in it. But it is obvious that the formation of new approaches to Ukraine's defense planning is required, which will ensure the ability to successfully resist external aggression against Ukraine.

The analysis of recent researches and publications. The problem of transition to a new format of state defense planning is new, it is still insufficiently studied and needs further study and discussion. Among the latest publications on the topic of state defense planning can be noted articles by R.I. Tymoshenko [2], A.M. Sirotenko [3], in which they analyze the features of modern conditions under which state defense planning should be carried out and set out views on the development of solving this problem.

Purpose of the report. The aim of the article is to study the content of the concept of state defense planning, taking into account the trends of modern armed struggle and the interaction of public authorities.

Main part

The nature of the conflict in which Ukraine is involved differs sharply from the classic armed struggle and war waged within the framework of international humanitarian law. The peculiarity of this conflict is its hybrid nature.

According to experts, the hybrid war that Russia has unleashed and is waging against Ukraine is a long-term factor influencing Ukrainian political, economic, military, informational, social and other spheres of the state's life. As a result of hybrid actions, the Russian Federation has distorted the systems of global and regional security and international law. Almost all international security guarantees for Ukraine, provided by the Budapest Memorandum signed by Russia, were neglected by the latter [4]. Almost all scholars unanimously state that under such conditions in early 2014, Ukraine's national security system was not ready to defend against a new type of aggression conducted by the Russian Federation. The management of Ukraine's security and defense forces, their preparation for concerted joint action, intelligence, counterintelligence, logistics and financial support proved to be weak, excessively bureaucratic and did not meet the requirements of the time. It can also be stated that the influence of international organizations, such as the UN and the OSCE, on the policy and

actions of the Russian Federation as an aggressor country is declining today and is clearly insufficient to stop its aggressive policy towards some countries in the post-Soviet space.

In turn, in response to the Russian Federation's aggression against Georgia in 2008, some Western countries sharply criticized the NATO bloc for not having enough forms of interstate confrontation to deter Russia. It was then that NATO adopted the theory of a "comprehensive approach", which provides for the impact on the enemy with the widespread use of diplomatic, economic, political, military, legal and other non-violent instruments. All these measures are primarily aimed at "rocking" the economy of the aggressor state, inflicting huge economic losses on it, restricting foreign policy activities and forcing it to abandon further aggressive actions, and so on.

Such actions are different from the classic forms of armed struggle and in themselves they are not military. However, their essence lies in the hidden influence aimed at inciting internal contradictions in the enemy state, or the use of the so-called "third force".

In this regard, the information confrontation comes to the fore. With his help there was an opportunity to destroy the foundations of statehood, to solve military-political problems to change the ruling regime in the country. Falsification, substitution of information or its distortion - these are the most effective ways of conducting information confrontation. In his speech at the Academy of Military Sciences of the Russian Federation in February 2016, Chief of the General Staff of the Russian Armed Forces General Gerasimov identified information confrontation and increased information influence as a priority in the activities of the Armed Forces of the Russian Federation [5]. Thus, the massive influence on the minds of Ukrainian citizens through television and the global Internet contributed to the spread of separatist movements and pro-Russian sentiments among the population of Eastern Ukraine and the Autonomous Republic of Crimea, which led to armed conflict between Ukraine and the Russian Federation and temporary

occupation of Donetsk and Luhansk regions and the Autonomous Republic of Crimea.

Classical wars of the twentieth century usually consisted of 80% violence and 20% propaganda. Modern wars, for the most part, consist of 80-90% of propaganda and 10-20% of violence. The effect of informational influence can be comparable to the results of large-scale use of troops and forces. Such an illustrative example is the annexation in the spring of 2014 by the Russian Federation of part of Ukraine, namely the Autonomous Republic of Crimea.

The peculiarity of the conflict in this case is that the leadership and the population of the victim state (in our case - Ukraine), under the influence of information pressure are not immediately aware of what is happening. The emergence of confrontation at the initial stage is not perceived by the masses as a war, as there are no clear signs of external aggression. Moreover, it (confrontation) is presented in propaganda materials as a desire to avoid war.

Uncertain attempts by the political leadership of the victim of hybrid aggression to stabilize the situation in the country often fail. In the absence of external aggression within the state, "peaceful" rallies, demonstrations and anti-government actions of opposition forces suddenly begin. All these signs took place in 2014 at the initial phase of the Russian Federation's aggression against Ukraine. At that time, the government was put in a very difficult situation. There seemed to be no war as such, and how it was necessary to react to the "peaceful" actions of one's own people was sometimes very difficult to determine.

According to the further scenario of the military conflict, there was a covert external invasion, which involved detachments of trained mercenaries and the formation of private military companies, units of the Armed Forces, Special Operations and Intelligence Forces of the Russian Federation, criminal elements and more.

The use of indirect actions and methods of modern warfare allows to achieve the necessary military results, such as demoralization of the enemy, causing him economic, political and territorial damage without the explicit use of their armed forces.

The experience of state defense during the events of the first half of 2014 and the anti-terrorist operation shows that to ensure the armed defense of Ukraine it is advisable to carry out planning that would cover the full range of state measures in all spheres of its life and mobilize all human, material -technical resources and spiritual forces of the state [2].

In their article [3] the authors give the following definition of defense planning and its purpose - is an integral part of the system of state strategic planning in the field of defense, which defines the goals, objectives, directions and complex of political, economic, social, military, scientific, scientific and technical, informational, legal, organizational, other measures and actions of the subjects of state defense to prepare the state for defense, its protection in case of armed aggression or armed conflict. The purpose of defense planning is to combine the efforts and capabilities of the executive branch, other state bodies, state resources to ensure the defense of Ukraine, armed defense of its independence, territorial integrity and other national interests. The main document that reflects the results of defense planning should be the defense plan of Ukraine.

Under such conditions, it is obvious that there is a need to reconsider conceptual approaches to state defense planning, which will take into account the conditions of a hybrid war against Ukraine [6], taking into account the characteristics of modern military conflicts.

Characteristic features and peculiarities of modern military conflicts are:

– comprehensive (according to a single plan and plan) application of political, economic, informational and other measures of military and non-military nature;

– formation and use of protest potential of the population and special operations forces based on military force;

– mass use of high-tech weapons systems, electronic warfare, unmanned aerial vehicles and autonomous naval vehicles, controlled robotic weapons and military equipment;

– influence on the enemy on all depth of its territory simultaneously both in classical geographical dimensions, and in

information, cybernetic and cognitive;

– damage to critical infrastructure as a priority;

– the beginning of hostilities (inflicting missile, missile and air strikes) without visible signs of advance training;

– changing the logic of the organization of the space of hostilities;

– expanding the range of actors in armed conflict - increasing the share of irregular armed groups and private military companies;

– point impact on the centers of gravity of the enemy;

– the design of the operation is formed on the basis of a system approach - the enemy is seen as a system, critical elements are affected and vital relationships are destroyed [7].

However, these characteristics and features of modern military conflicts are not properly taken into account in current legislation. On the one hand, in accordance with the Law of Ukraine "On Defense of Ukraine" [1], Ukraine's defense is based on the readiness and ability of public authorities, all components of the security and defense sector, local government, unified civil defense, national economy to transfer, if necessary, from peace to martial law and repulse of armed aggression, elimination of armed conflict, as well as the readiness of the population and the territory of the state for defense. In this interpretation, defense is considered only in the plane of repelling armed aggression, which is only one component of modern conflict. On the other hand, the main feature of the security environment of today is the confrontation of states in four main areas - political, financial, economic, energy; information, internal security and military confrontation [8].

The core of modern concepts of defense is the idea of involving all citizens and all spheres of public life in the country's defense (Whole governmental approach), namely: political, economic, social, scientific, scientific and technical, informational, legal, etc. Many countries have adopted official concepts of public, total defense. These doctrinal guidelines implement such recognized democracies as: Austria, Norway, Switzerland, Sweden, Finland. As a rule, the concepts of defense are based on the need to educate citizens in readiness to repel aggression, defend the country and defend the values of their society.

Conclusions

Summing up, we can say that the development and implementation of new approaches to state defense planning, taking into account all the factors inherent in modern military conflicts, will allow to unite into one whole (in a system with stable links between the subjects of defense planning state) the activities of all public authorities to ensure military security, preparation for defense and repulse of armed aggression against Ukraine, if any.

Areas of further research should identify ways to improve the process of state defense planning in order to achieve the required level of defense capability of Ukraine in all areas defined by law.

References

1. Law of Ukraine (2019), *On amendments to the Law of Ukraine "On Defense of Ukraine" regarding the organization of state defense: Law of Ukraine No. 133-IX of September 20, 2019*, available at: https://cutt.ly/3j1lnDd (accessed 25 January 2021).

2. Tymoshenko, R.I. and Pubic, M.M. (2018), Problems of Improving the Defense Planning of Ukraine, *Science and Defense*, Vol. 1, pp. 11-17.

3. Sirotenko, A.M., Shchipansky, P.V., Pavlikovsky, A.K. and Lobko, M.M. (2020), Actual Problems of Planning the Defense of Ukraine: a Comprehensive Approach, *Science and Defense*, No. 10 (1), pp. 3-12.

4. Frolov, V.S., Sahaniuk, F.V. and Pushniakov, A.S. (2019), A Glance at the Development of Strategic Capital by the Security Sector and the Defense of Ukraine in the Minds of Hybrid Warfare, *Science and Defense*, No. 2, pp. 27–30. https://doi.org/10.33099/2618-1614-2017-0-2-27-30.

5. StopFake (2015), *Hybrid war as a key tool of the Russian geostrategy of revenge*, available at: https://cutt.ly/Uj1xTqT (accessed 25 January 2021).

6. Misko, V. (2017), "*Svitova hibrydna viina: ukrainskyi front"* [*World Hybrid War: Ukrainian Front*], in Gorbulin, V.P. (ed.), Folio, Kharkiv, 496 p.

7. Duz-Kryatchenko, O.P. and Punda, Y.V. (2017), *Fundamentals of military security of the state*, in Telelim V.M. (ed.), NGOs, Kyiv, 204 p.

8. Frolov, V.S. and Semenenko, V.M. (2019), Formation of perspective model of defense organization of Ukraine, *Science and Defense*, No. 3, pp. 3-9.

Hennadii Pievtsov
Doctor of Technical Sciences, Professor
Deputy Head in Science of Ivan Kozhedub Kharkiv National Air Force University
Kharkiv, Ukraine
https://orcid.org/0000-0002-0426-6768

Olha Usacheva
Candidate of Technical Sciences, Senior Researcher
Head of the Scientific Research Department of Ivan Kozhedub Kharkiv National Air Force University
Kharkiv, Ukraine
https://orcid.org/ 0000-0003-0864-5017

Hryhorii Zubrytskyi
Candidate of Technical Sciences, Associate Professor
Lead Researcher of Ivan Kozhedub Kharkiv National Air Force University
Kharkiv, Ukraine
https://orcid.org/0000-0002-9577-5268

Alla Romaniuk
Research Associate of Ivan Kozhedub Kharkiv National Air Force University
Kharkiv, Ukraine
https://orcid.org/0000-0001-5882-6962

DECISION OF MILITARY COMMAND ON IMPLEMENTATION OF PSYCHOLOGICAL AND INFORMATION OPERATIONS DURING HYBRID WAR

The article focuses on the development of a functional model of the decision support system by the military command during information and psychological operations in hybrid war using the IDEF0 methodology. The proposed process model of the activities of military command regarding the use of automated control methods of information and psychological operations allows making this activity

transparent, manageable, and predictable. It will ensure the successful achievement of planned goals in hybrid war. Such model can serve as the basis for creating the quality control system in accordance with the requirements of existing world standards.

Keywords: *decision support system, functional model, information and psychological operations, hybrid war, military command, IDEF0 standard.*

Introduction

Problem statement. In the modern world, the unique mean for warfare is hybrid war or a colour revolution that differs from other conflicts. Along with the use of military force and various forms of economic forcing the enemy, the capabilities of modern information technologies are widely used. Information systems and technologies for influencing the enemy reached a new qualitative and quantitative level. It gives information weapons spatial scale, threatening relevance and special speed of development.

It requires new approaches to organize the activities of military command, organizing and planning the information and psychological influence on the enemy troops and population [1–2].

At present, information and psychological operations provide joint actions of the Armed Forces of Ukraine with units and subunits of other ministries and departments. In this regard, during implementation of measures by the military command, system of interaction between the information space of the Armed Forces of Ukraine and networks of other law enforcement agencies and networks of public authorities is needed in the context of hybrid war.

The analysis of recent researches and publications. Scientific researches show that for the effective control of troops in hybrid war, it is necessary to reduce the time for information activities of administration to 15-20% and free up time for creative and organizational activities to 80-85%. It's possible to realize it with new information technologies. The problems and shortcomings in the activities of the military command in decision exist not only in the military sphere. This issue is very relevant for most enterprises, both in Ukraine and around the world. Many works are focused on

the problem of improving the activity of at the level of chiefs. The theoretical analysis of the work of various scientific works showed that the problem of this time is considered unsolved [1-5].

The purpose of this article is the research of the functional model of the military command activities involved in the process of organizing the information and psychological influence in the control cycle using a set of automation means.

Main part

For the exchange of information between institutions of various departments and also between different countries, auditors and experts of countries, it is possible to use the IDEF0 methodology as a single language. Using the IDEF0 methodology, a functional model is created. It contains the processes and functions of the system, information flows and resource components. This model have the necessary depth of decomposition, to the description of actions that are performed by individual specialists at specific workplaces, indicating the conditions of implementation and the list of resources used. The use of the mechanism of formalized description of the control of the military command involved in the process of organizing the information and psychological influence will automate their control functions through software and hardware implementation.

A model based on the IDEF0 methodology can be used as information resource to obtain relevant information at all levels of the hierarchy.

The description of control processes has several advantages in the form of functional models as follows:

– model is a kind of a personnel control program (experts, military command), it determines who performs certain functions;

– model determines material flows and workflow and allows to set the rules for the exchange of the results of various processes;

– model is a methodological basis for the construction of applied software systems;

– model can be used as a training simulator system;

– model is convenient mean of analysis, suitable for finding ways to improve the organization and control of processes [6].

The general idea of the process can be described in terms of inputs, outputs, controls and mechanisms for the implementation of functions and tasks, represented by functional diagrams of the IDEF0 standard. The IDEF0 standard is a set of graphic modules. The focus is on the object subordination and logical relationship. The description of the process looks like a black box with inputs, outputs, control and mechanisms. It is detailed to the required level [7].

According to the IDEF0 standard, each function block must have at least one control and output interface.

Each functional block is characterized by the conversion of input (resources necessary for the implementation of the process) to output (result, process products).

Process resource is material, technical, energy, human, information and so on. The process is carried out using a specific mechanism guided by a specific person. Function blocks are connected by lines and arrows, reflecting the connection between them. The technology of using IDEF0 structural analysis involves the development of context (A0) and decomposition (A1, A2) diagrams.

The decomposition principle is used to divide a complex process into its components. The process detail level is determined directly by the developer of the model.

Decomposition allows to structure the system model in the form of hierarchical structure of individual diagrams that makes it less overloaded and easier to understand.

To connect the subsystems with each other the internal arrows are used that exit one action and enter another. There are five types of internal arrows in IDEF0:

– communication on the output-input, when the output of higher action is directed to the input of lower;

– communication control (output-control), when the output of the highest action is directed to the control of the lower;

– feedback on output-input, when the output below the action is directed to the input higher;

– feedback on output-control feedback, when the output below the action is directed to the higher control;

– output-mechanism, when the output of one action is directed to the mechanism of another one.

The existing standard requires the creation and support of appropriate definitions, keywords that should characterize the object captured by this element for each of the elements of IDEF0 diagrams. This set is a glossary and a reflection of its contents. Glossary supplementing the graphic language, providing the diagrams with the necessary additional information and the possibility of qualitative understanding of the processes occurring in the control cycle. Decision process by the military command on the implementation of the informational and psychological operations in hybrid war can be represented by functional schemes of the IDEF0 standard (Fig. 1).

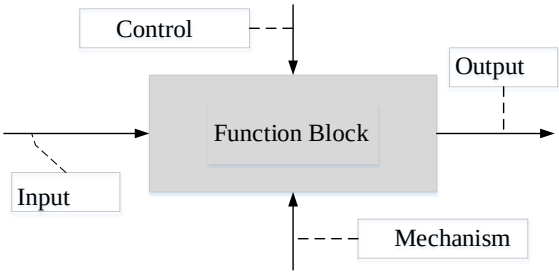

Fig. 1. Function block in the IDEF0 diagram

The name of the high-level process (hyperprocess) shows the general purpose of such work and in accordance with the requirements of the standard [6] can be formulated as “The activities of military command in the application of automated control methods for information and psychological operations”.

The A-0 context diagram of this hyperprocess in the IDEF0 notation is shown in Fig. 2

The inputs of the hyperprocess are the information that came from the analysis of priori data obtained from:

– policy documents;

– print media;

– from entertaining, scientific and analytical periodicals (newspapers, magazines, almanacs), literature (children's, art, scientific, special and encyclopedic), brochures;

– leaflets, posters, “billboards” and so on;

– various informational and journalistic messages (broadcasting);

– television (news, analytical and entertainment programs, cartoons and movies, talk shows, advertising and so on);

– Internet;

– video games and other information sources, with or without influence.

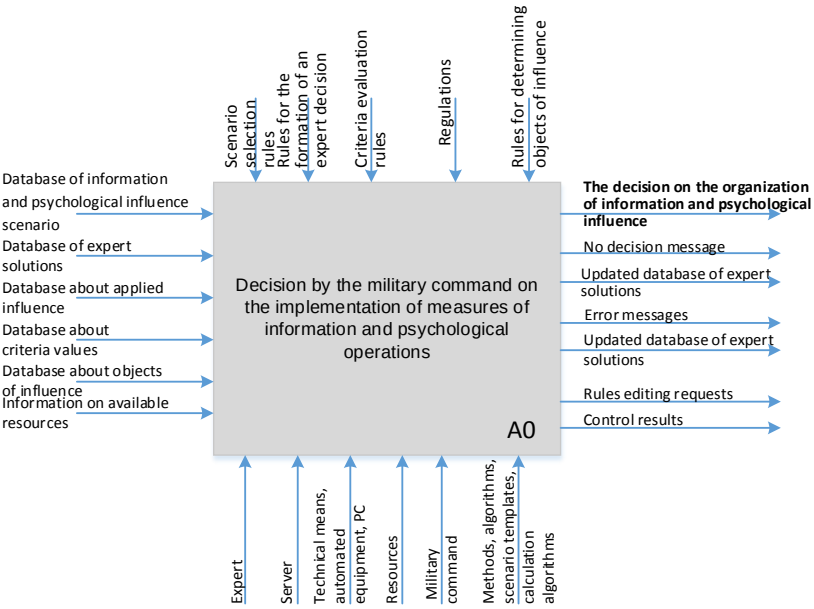

Fig. 2. Context diagram of the hyperprocess of the activities of the military command for the application of automated control methods of information and psychological influence measures

The input information includes data obtained from the experience in solving similar problems that are stored in the system in databases and data on available resources. In this case, the decision process is governed by established rules, regulatory and policy documents.

As a result of activities as a result of this process, we will have a solution in the form of scenario and plan for organizing the information and psychological influence and the results of control.

A certain process is implemented using such mechanisms as: experts, management (military command), personnel, hardware (automated equipment, PC, information display facilities), methods and algorithms necessary for calculations, formalized document templates, resources and servers.

The purpose of this process is to organize and plan the information and psychological influence for the enemy troops and population.

The model is being developed from the point of view of military command.

The decision process by the military command on the implementation of information and psychological operations measures in hybrid war includes three sequential and interrelated stages: organization of headquarters work planning (selection of an expert group, determination of criteria), development and approval of the information and psychological influence scenario, development of an information and psychological influence organization plan. Therefore, the hyperprocess of the activities of the military command in applying the methods of automated control of the informational and psychological influence includes three main macro-processes: organization of information and psychological influence planning (A1), development and approval of information and psychological influence scenario (A2), development of information and psychological influence organization plan (A3).

The content of the selected subprocesses is revealed by the decomposition diagrams of the second level. When constructing them, all “inputs” and “outputs” of the previous diagram are taken into consideration, as well as the internal “inputs” and “outputs” are specified.

The context diagram of the military command activities on the application of methods of the automated control of informational and psychological operations measures gives a general idea of it.

The construction of decomposition diagrams of several lower levels allows to present its component fragments in more detail and to model their interconnections. When constructing them, all the “inputs” and “outputs” of the previous diagram were taken into consideration, as well as the internal “inputs” and “outputs” were refined (Fig. 3).

The subdiagram A0, which shows these processes in the IDEF0 notation, is shown in Fig. 3.

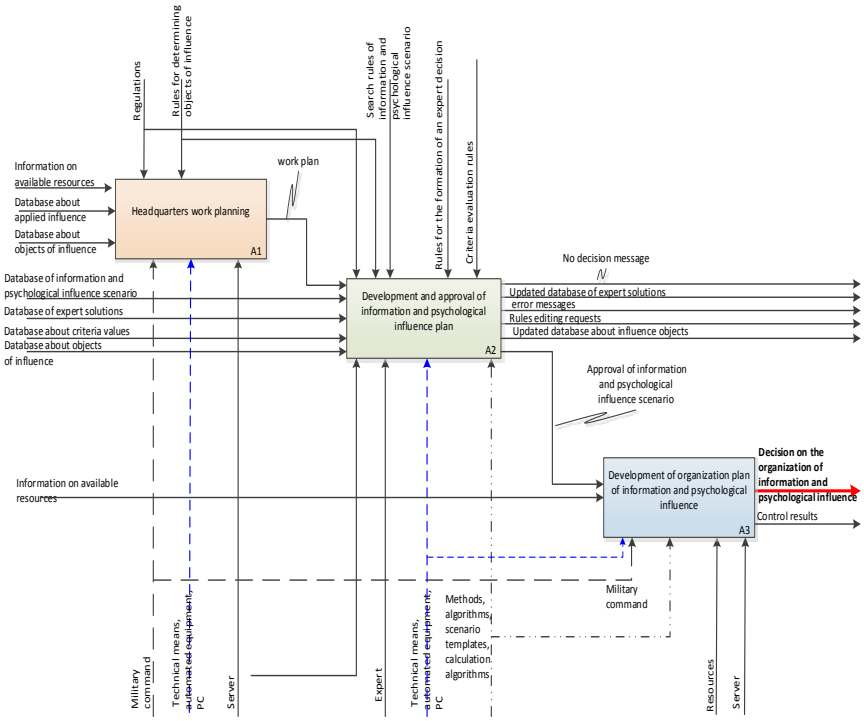

Fig. 3. Diagram of the second level of the functional model of the military command activity on the application of automated control methods of information and psychological operations

The outputs of the process are the contol actions of the military command (plans, instructions, previous orders, information and psychological influence scenario) to achieve the intended goal

through perfect work using methods of automated control of informational and psychological operations.

The result of the A1 process is the provision of the necessary information in the form of planning documentation (time calculation, data for the formation of scenario, resource calculation) of A2 block (stage 2) to ensure activity.

The main result of A2 process is the information and psychological influence scenario. Other results are:

– no decision message;

– updated database of expert solutions;

– error messages;

– rules editing requests;

– updated database about influence objects.

The main A3 result is the military command decision to conduct information and psychological operations and control results.

The control for this process and for others processes is the regulatory documents and rules.

The mechanisms for the implementation of this and other processes are military command officers, experts, technical means, automated equipment, PCs, servers, information display means, formalized document templates, algorithms and methods of information processing.

The proposed functional model of the activities of the military command for the application of automated control methods of information and psychological operations is constructed on the basis of the AS IS model and in the future a transition to the TO - BE model is possible. It is the key to the automation of the "correct", improved processes.

It is known that more than 65% of the time spent on inefficient document control is also present in this scheme, and a large number of duplicate works, especially at the stage of setting tasks for subordinates.

The AS IS model allows to systematize the processes taking place at the moment. On the basis of this, bottlenecks in the organization of interacting processes are found, the need for certain

changes in the existing structure is determined [4].

Accordingly, the less it takes to develop and approve the plan of information and psychological influence, the less is time component of the control cycle.

In addition, now the software environment, used to describe the methodology according to the IDEF0 standard, allow to develop formalized documents. This procedure will reduce planning time by several times, by reducing unnecessary workflow, duplicate work, planning time.

Conclusions

The proposed model of the activities of the military command on the application of the methods of automated control of information and psychological operations measures allows to make this activity transparent controlled and predictable. It will ensure the successful achievement of planned goals in hybrid war.

Such model should serve as the basis for military command control system in accordance with the requirements of existing world standards.

Further outlook is the study of the next step in modeling information processes in the activities of the military command, at the synthesis stage, the creation of a model of control activity of the military command for the application of the methods of automated control of information and psychological operations measures "TO-BE". It will be the basis for information reengineering processes in the future.

References

1. Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), "*Informacijno-psihologichna borotba u vryennij sferi*" [*The information and psychological struggle in the military sphere*], Rozhko S.H., Kharkiv, 276 p.

2. Snezhkova, I.A. (2016), "Otrazhenie gibridnoj vojny v elektronnyh resursah Ukrainy i Rossii" [Reflection of hybrid war in electronic resources of Ukraine and Russia], *Bulletin of Anthropology*, No. 4(36), pp. 175-185.

3. Cheremnyh, S.V., Semenov, I.O. and Ruchkin, B.C. (2006), "*Modelirovanie i analiz sistem. IDEF-tehnologii: Praktikum*" [*Modeling and analysis of systems. IDEF technologies: Workshop*], Finansy i statistika, Moscow, 192 p.

4. Devid, A. Marka and Klement, L. MakGouen (1993), "*Metodologiya strukturnogo analiza i proektiro-vaniya SADT*", [*SADT structural analysis and design methodology*], Moscow, 231 p.

5. State Standard of Russia (2000), "*RD IDEF0 – 2000. Metodologiya funkcionalnogo modelirovaniya IDEF0*" [*RD IDEF0 – 2000. IDEF0 functional modeling methodology*], Moscow, 75 p., available at: https://nsu.ru/smk/files/idef.pdf (accessed 22 January 2018).

6. Parshin, S. and Kozhanov, Yu. (2009), "Sovremennye tendencii v sovershenstvovanii sistemy upravleniya vooruzhennymi silami vedushih zarubezhnyh stran v informacionnuyu epohu" [Current trends in improving the management system of the armed forces of leading foreign countries in the information age], *Foreign Military Review*, No. 6, pp. 3-10.

7. Usachova, O.A., Medvedyev, V.K. and Yakobinchuk, O.V. (2015), International standard IDEF0 in modeling of management processes of commanders of military units (subdivisions) of communication of Radio engineering support of aviation and information systems, *XI scientific conference of Ivan Kozhedub Kharkiv University of the Air Force*, 8–9 April, Kharkiv, Ukraine, pp. 180.

8. Usachova, O.A., Medvedyev, V.K., Usachov, O.M. and Gricenko, P.M. (2013), "Doslidzhennya funkcionalnoyi modeli diyalnosti posadovih osib v cikli upravlinnya z vikoristannyam kompleksa zasobiv avtomatizaciyi" [Research of functional model of activity of officials in cyclic management with use of a complex of means of automation], *Science and Technology of the Air Force of Ukraine*, No. 4(13), pp. 95-99.

9. The official site of DOCS.CNTD (2002), "*Rekomendaciyi R 50.1.028-2001. Informacionnye tehnologii podderzhki zhiznennogo cikla produkcii. Metodologiya funkcionalnogo modelirovaniya*" [*Recommendations P 50.1.028-2001 "Information technologies to support the product life cycle. Methodology of functional modeling*"], available at: http://docs.cntd.ru/document/1200028629 (accessed 22 January 2018).

10. Burkov, V.N. and Kondratev, V.V. (1981), "*Mehanizmy funkcionirovaniya organizacionih sistem*" [*Mechanisms of functioning of organizational systems*], Nauka, Moscow, 384 p.

11. Volkova, O.R. and Volkov, N.V. (2006), Constructing models of random processes with specified properties by the Wiener method for identifying dynamic system, *Measurement Techniques*, No. 8, pp. 803-808.

Sergii Pozigun
PhD (Physical and Mathematical Sciences)
Instructor of the Department of Ground Artillery
of the Hetman Petro Sahaidachnyi National Ground Forces Academy
Lviv, Ukraine
https://orcid.org/0000-0002-1210-8612

Sergiy Holoushko
Senior Instructor of the Department of Engineering
of the Hetman Petro Sahaidachnyi National Ground Forces Academy
Lviv, Ukraine
https://orcid.org/0000-0003-1585-8504

MORAL AND PSYCHOLOGICAL CONDITION OF THE PERSONNEL OF THE ARMED FORCES OF UKRAINE AS AN IMPORTANT FACTOR OF STATE SECURITY

The national security of each country in the world is mostly based on the readiness of its citizens to defend their homeland. Therefore, the analysis of moral and psychological support (MPS) in the Armed Forces of Ukraine is extremely important. One of the main problems of the moral and psychological state of modern Ukrainian servicemen is their considerable "amorphousness" from the world outlook aspect, which forms a significant security risk under conditions of the today hybrid Ukrainian–Russian war. The authors of this report try to formulate modern requirements for MPS of the servicemen and methods of improvement of moral and psychological properties of the latter.

Keywords: *moral and psychological support; world outlook of the personnel; modern requirements for the psychological state in the Armed Forces.*

Introduction

Problem statement. The Armed Forces of Ukraine are at present in a process of active formation of relations with the armies of other leading countries of the world, which obviously affects the world outlook of the personnel. Therefore, proper understanding and

active support of this process are extremely important [1].

The analysis of recent research and publications. Numerous publications have been devoted to a problem of the moral and psychological state of the personnel of the Armed Forces of Ukraine. Among these articles, the following should be highlighted:

– those describing the basis of this problem from the aspect of the public management [2];

– attempts to subject the problem to the scientific analysis [3–4];

– some publications can be considered as actual explorations taking into account, in particular, the experience of Ukrainian–Russian war and other hybrid military conflicts [5–7].

Purpose of the report. The main idea of our report is to formulate the realistic viewpoints on the problem of personal worldview of today Ukrainian officers and to propose some innovations within the field of psychology training.

State security is determined to a considerable extent by the loyalty of the citizens to their state and interest of these people to the development of their country.

With the beginning of the hybrid Ukrainian–Russian war, which is in fact the war of Ukraine for its independence, a significant proportion of the Ukrainian society has been largely concentrated around the Ukrainian national idea. A considerable military experience in this war has been already stored, which is highly important for the formation of an adequate qualitative level of the modern Armed Forces of Ukraine.

Nonetheless, it is not a secret that the nowaday Ukrainian officers are in many cases carriers of old/archaic views and ways of perceiving the external information. This, in our opinion, is related to certain shocking events of disruption of the Soviet society and a necessity for a conscious abandonment of the typically-Soviet way of thinking and the world outlook in favor of the movement towards specifically Ukrainian views on history and social organization, with the emphasis on a concept of the personal freedom. From this aspect, such transformation may be much easier for young officers of the

Armed Forces of Ukraine in this respect. Nonetheless, they, in our opinion, often face the lack of clear guidelines that can reliably form the worldview of a young serviceman.

Among typical negative features of a former Soviet officer, there are in many cases the following:

– attempts to "hide himself in the bushes" in the case of an acute/dangerous situation;

– preference for making of his own career instead of growth due to the professional actions;

– neglecting of the real needs of the subordinate personnel;

– propensity for the "window dressing" and false reporting instead of real practical results and achievements.

Thus, while the Soviet system of moral and psychological upbringing/education of servicemen was, on the first glance, powerful and well-developed, it appeared practically meaningless and powerless when it has met real challenges of contemporary problems.

As it became at present known, the Soviet system was mostly ruined by the action of the following factors:

– total lies in both big and small matters, this, at a certain stage, becomes the inner essence of the man;

– a conscious refusal to fight for his own human dignity due to the obvious futility of the respective efforts;

– as a consequence, a surge in crime (theft in particular), alcoholism, and drug addiction among the personnel.

It is quite obvious that the Armed Forces of Ukraine are a part of our society with all its deficiencies; at the same time, they must ensure the security of the Ukrainian State. Can a person without high-quality moral principles be a true defender of the Homeland? Of course no.

Therefore, both officers of the Armed Forces and the entire society are facing a vital and responsible task of creating such an ideological pattern that would provide support and desire of the personnel to continuously progress from both professional and personal aspects.

There is an idea that a professional serviceman does not have

to be a convinced patriot. The centuries-old experience of our country and other countries, however, demonstrates that, without deep and conscious patriotic feelings, the actions of any officer or soldier are not effective enough. It should be taken into account that military service, even within a peacetime, is associated with constant separation from the family and relatives, a significant restriction of what is allowed or not, and the need for round-the-clock self-control, and these limitations cannot be psychologically overcome without feelings of strong real strong patriotism.

In addition, certain situations under conditions of a military conflict can be strongly life-threatening, and each serviceman in a particular situation should answer to himself whether a real risk is expedient or not and select an algorithm for his adequate actions.

Main part

Let's try to formulate the main mental properties of a professional soldier during a combat:

– ability to concentrate on the actual combat mission by voluntarily subjugating all secondary thoughts;

– ability to navigate in a fast-modified dangerous environment;

– ability to suppress and control the fear of death;

– ability to control his subdivision in a difficult situation and to give adequate expedient commands.

What should be put in the first place in the modern Armed Forces when forming an optimum state of consciousness and psychological stability? In our opinion, this is must be the following:

– to cultivate obligatory deep patriotic feelings in each serviceman. In this process, it is expedient and necessary to study real (not Russia-edited) history of Ukraine, to describe in details successful, as well as unsuccessful (negative experience) actions of the Armed Forces under contemporary conditions and those of Cossacks and troops of the Kyivan Rus'. Different categories of the personnel should obtain the opportunities for both simplified acquaintance with historical information (excursions, movies, concerts, etc.) and in-depth

studying of history (based on the works of famous Ukrainian and world classics of history, philosophy, and martial arts);

– to carefully but insistently remove modern Russian pseudoculture from everyday use by the personnel. Unfortunately, this aspect is, as a rule, ignored;

– to pay much more attention, time, and efforts in training the personnel for professional duties (specialized military and general physical training, competitions, etc.) At present, as we can see, only single subdivisions are trained properly; in many cases, this is in many cases mostly transformed in a show (including special trainings for NATO visitors);

– to introduce a specialized obligatory course of combat psychology; this field should be raised to the appropriate practical level. It should be taken into account that, in combat situations, the personnel is under strong stress-inducing conditions; therefore, the servicemen should be able to adequately enter and leave the state of war-related stress.

In order to formulate adequate requirements for moral and psychological education and support of the servicemen under modern conditions, we should, first, try to briefly classify the features of the existing moral and psychological support (MPS):

– there is too much dependence on the existing former regulations provided by many commanders and their deputies. It should be noted that a term “zampolit” is still widely used in the Armed Forces of Ukraine, although this is a clear relic of the past;

– a majority of modern MPS deputy commanders of the subdivisions do not fully correspond to their positions. Such officers are, of course, able to “talk about life” with the solders, communicate with them in an informal mode (e.g., tell a good anecdote) trying to support the mood of the staff (sometimes successfully). Such officers of the “old hardening,” however, frequently do not meet modern requirements for deputy commanders of the combat units. They are not able to raise patriotic feelings, have a limited knowledge about quite real achievements of Ukraine in the modern world and in the actual hybrid Ukrainian–Russian war;

– lack of clear specification of the responsibilities of MPS officers. Indeed, let us ask a question: Is an MPS officer a "factory of papers" related to investigations of various incidents and to means of visual agitation, or he is a specialist capable of urgent visiting of the firing position and of really supporting and inspiring the combatants?

The main idea of our report is to transfer the support of the moral and psychological state of modern servicemen from a purely bureaucratic category to a field of providing scientifically based high-quality moral state of the servicemen who are teached for best examples of the martial art.

In this case, modern specialists in MPS should, in our opinion, be able to do the following:

– to understand the deep psychological levers of personnel behavior. What motivates a person to be included to military service? Occasional factors (like procuring of more or less satisfactory salary and possibilities for impunity alcohol use) or the opportunity to feel himself as a real defender of his family and country?

– to be able to convey to the people a positive point of vision in problematic situations. Such a skill requires, of course, a certain volume of life experience in MPS officers and the involvement of immediate commanders;

– to be able to resist "aggressive alcoholism" and to maintain a stable working condition in their units for a long time.

It is not a secret that, in military subdivisions, certain "animal" and "prison" instincts are manifested; sometimes there is a clear desire of the personnel to find a "flock leader" among themselves. Such an approach, obviously, sharply simplifies for other members of the "flock" their approach to own behavior: it is not necessary to defend the personal opinion, but only to obey a somebody's will. Such situation, however, induces a great danger of the complete loss of normal control over the subdivision.

Based on the above, we would like to propose certain measures that can help to bring modern moral and psychological support to the required level:

– various trainings with simulations of difficult real combat

conditions should be developed and widely introduced into practice; such trainings will help the personnel to adequately estimate their combat abilities. Thus, the state of mind of the personnel is considered as such a parameter, which can be effectively and permanently trained and developed;

– the informational methodology for mental trainings of psychological relief based on contacts with trained professional psychologists should be created. This is expected to provide some progress in prevention of alcoholism and depressions in the personnel;

– an appropriate informational base for moral and psychological support including manuals, videos, etc. should be formed;

– special trainings for concentration of the willpower should be carried out.

As a result, we can expect that the Armed Forces of Ukraine will get modern highly motivated servicemen, the specialists who will be able to defend and justify their own opinions and to perform their military duty consciously and adequately.

All the above mentioned substantiates the need for a practical and scientific approach in the formation of the moral and psychological support of the personnel. Among other aspects, this makes necessary the involvement of military experts of our country and other states. This process requires integration of:

– practical experience of the activity of subdivisions in the contemporary hybrid Ukrainian-Russian war;

– results of detail analysis of the actions of units in other today hybrid conflicts in the world;

– a professional excursion into the history of competitions of Ukraine and other countries for their independence, which will open the “secrets” of successful hostilities.

Let us analyze the main factors that motivate the servicemen to serve on the basis of a contract with the Armed Forces of Ukraine:

– provision of stable financial supply;

– broad opportunities for the carrier progress;

– sustainable pension provision;

– a possibility for obtaining higher education.

These are the factors that mainly affect the "overall" staff. If we talk about the officers (and especially about the MPS specialists), this category of military men should be individuals with a rigid "state" psychological position, to whom the idea of building of our strong state is not an empty sound.

Let's try to formulate certain criteria for such state of thinking:

– active attention to the development of our country within the medium and long terms;

– the ability to subjugate their own private interests to general interests of the society;

– the ability to inform people about "global" issues in a most popular, but correct manner, i.e., "in simple words."

As we can see, features of the modern state of thinking of Ukrainian officers should be crucially different from those presented in the "Code of the Communism Builder," on which the former zampolits were focused on for years and decades. The absolutely artificial nature of this "Code" did not interfere with its being as a general official obligatory doctrine.

In the modern Ukrainian society, an analogous doctrine for the maintenance of MPS has not been formed and, because of quite understandable considerations, it cannot and should not be formed. Nonetheless, many of contemporary Ukrainian citizens sense a nostalgia for the "old days," despite complete absurdity of these sensations. In our opinion, this is due to the fact that the past Soviet era gave ordinary citizens a feeling of the certain "core," despite the entire artificiality of such a feeling.

Conclusions

One of the important tasks for the modern Ukrainian society is to create a real high-quality state-oriented ideology that would be able to involve the most broad strata of the Ukrainian society having very different views in the active public life.

These are urgent issues for today officers, including the MPS specialists, and these issues should be successfully resolved at both global and "domestic" levels. Thus, transformation of the MPS specialists is an important factor in maintaining the proper combat conditions of all, with no exceptions, units of the Armed Forces of Ukraine. Raising the MPS to a highly successful current level is an extremely important task, as has been shown in our report.

References

1. Rachok, O.S., Mel'nikov, O.V., Gamarnik, A.A. and Pozigun, S.A. (2019), "Moralno-psyhologichnyi stan osobovogo skladu u boyovyih chastynah ZSU ta metody vplyvu na nyogo na suchasnomu etapi" [Moral and psychological condition of personnel in the combat units of the Armed Forces and methods of influencing it at the present stage], *Materials of International Conference "Public Administration in the Field of Civil Defense: Science, Education and Practice", 17-18 of May, Kharkiv*, pp. 149-150.

2. Poltorak, S. (2016), Formation and implementation of the comlex mechanism of public administration of maintenance of military security of Ukraine, *Public Policy and Economic Development*, No. 9-10 (13-14), pp. 102-109. https://doi.org/10.14746/pped.2016.9.9.

3. Kydon, V. (2017), Coverage of the question of moral and psychological state of the soviet troops during the struggle for Kyiv in 1943 in scientific papers, *Istorychni Nauky*, (27), pp. 201-214.

4. Krotiuk, V. (2015), Patriotic education of personnel of the Armed Forces of Ukraine, *Science & Military*, No. 1, pp. 34-37.

5. Homchuk, R. and Boiko, V. (2017), The pedagogical aspects of the psychological training of servicemen in modern conditions, *Research papers collection of the Center of military and strategic studies of the National Defence University of Ukraine named after Ivan Cherniahovskyi*, No. 2 (60), pp. 132-136.

6. Smirnov, S. (2019), Analysis of professional preparation for future officers of the state of Armed Forces of Ukraine in the system of modern military education, *Social and Legal Aspects of the Development of Civil Society Institutions, Part I*, Warsaw, pp. 104-116, available at: https://cutt.ly/aj4xQPE (accessed 27 January 2017).

7. Prykhodko, I., Matsehova, J., Lipatov, I., Tovma, I. and Kostikova, I. (2019), Servicemen's motivation in the National Guard of Ukraine: transformation after the 'Revolution of Dignity', *The Journal of Slavic Military Studies*, No. 3 (32), pp. 347-366. https://doi.org/10.1080/13518046.2019.1645930.

Olha Salnikova
Doctor of Sciences in Public Administration, Senior Researcher
Chief of Educational and Research Centre of Strategic Communications in the Sphere of National Security and Defence of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-7190-6091

Ihor Sivokha
Researcher of Military Strategic Studies Centre of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-5377-2520

Iryna Izhutova
Chief of Training Section of the Educational and Research Centre of Strategic Communications in the Sphere of National Security and Defence of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-2614-7014

USE OF TECHNOLOGIES OF STRATEGIC COMMUNICATIONS AND REFLEXIVE CONTROL IN FIGHTING HYBRID AGGRESSION

In current world the coexistence of propaganda, disinformation, psychological pressure, attacks against information and communication systems is the same challenge as conventional weapons. The effective scenarios of fighting against hybrid threats are based on the use of current technologies of strategic communications, military conflicts' agents control and information processing. The report defines place, aim, scope and features of strategic communications. The integrated use of strategic communications technologies and reflexive control is proposed for development of scenarios of fighting against hybrid threats.

Keywords: *modern hybrid warfare; strategic communications; information technologies; reflexive control.*

Introduction

Problem statement. "Hybrid" aggression of Russian Federation (RF) against Ukraine using various conventional and unconventional tools for pressing Ukraine, forcing it to change strategic choice and current state structure is a serious challenge for national security. Fighting against hybrid threats and revealing hybrid attacks, especially at early stages are more comprehensive. Enhancement of fighting methods, including information and communication ones, use of modern scientific methods form a real problem. Considering controversial opinions of scientists and practitioners concerning use of strategic communications (SC) in fighting against hybrid aggression, it is worth to define SC place, aim, scope, and features, develop recommendations for integrated use of SC technologies and reflexive control in fighting against hybrid aggression [10].

The analysis of recent researches and publications. Modern fighting strategies based on information weapons as one of key deterrence factors are considered in works of one of military theoreticians F. Hoffman [1], Jim Mattis, former US DOD Secretary, M. Kaldor, professor of London School of Economics, works of RAND Corporation and foreign researchers [2]. The SC issue is also discussed in national documents of defense planning and national scientists studies [9–11].

Purpose of the report. To define SC place, aim, scope, and features, develop recommendations for the integrated use of SC technologies and modern theory and control methods in fighting against hybrid aggression.

Main part

The "*strategic communications*" term consists of two words. The "strategic" word means top political level communications, society, and international audience. The "communications" word means national values and capabilities aimed at improving national strategic stance compared to the adversary's stance. The

“communications” word means both the dialog and “top-down” information activities.

The “strategic communications” at modern stage of society development underline the significance of integration of all tools of influence on particular people, target audiences, and country. Meanwhile, the issue of SC influence on decision-making and control processes within “hybrid” warfare is still unresolved.

For the first time the issue of SC development in Ukraine was raised after the beginning of the Russian aggression in 2014 within NATO Wales Summit decisions. The Alliance provided advisory, practical, and technical support, including there was initiated the project of development of national strategic communications centre and situation centers with critical state authorities.

In order to enhance the activities related to SC implementation within “hybrid” aggression the NATO standards are used for development of SC policy, planning, and implementation at all levels.

The “strategic communications” term agreed with NATO terminology is currently officially used in the Ukrainian law after use in Military Doctrine of Ukraine where the SC means “coordinated and appropriate use of the state communicative capabilities such as public diplomacy, public affairs, military relations, information and psychological operations and actions aimed at state aims promotion”.

Particular aspects of SC use in fighting against “hybrid” aggression are considered in national defense planning documents. One of priorities of fighting against “hybrid” aggression is continuous improvement of legislative and normative SC documents. The RF “hybrid” approach makes the information sphere as the key fighting field.

Ukraine faces the newest information cognitive technologies aimed at stirring up national and religious hatred, propaganda of aggressive warfare, coup d’état or infringement of sovereignty and territorial integrity of Ukraine. Special units of RF armed forces deployed in Donetsk and Luhansk oblasts within information and

psychological operations [9].

According to RF officials, the “hybrid” aggression is aimed at establishing external control and total control over state administration when the dominant agent (aggressor, group of states, transnational corporation, syndicate) forms necessary and appropriate conditions for domination over the object (aggression object, social group, society) in order to control fully and totally the sovereignty and territory, other important, but vital signs, except for capitulation of the armed forces [5]. Thus, the Russian view of modern warfare is based on the idea that the main battlespace is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare, in order to achieve superiority in troops and weapons control, morally and psychologically depressing the enemy’s armed forces personnel and civil population [6]. One element of Russian resurgence that captivates Western defense circles is the emergence of new generation warfare [8]. SC play the key role in achieving the “hybrid” aggression aim, which key tool is information, comprehensive armed actions are the support element.

The control system tasks in “hybrid” aggression are in saving and change of aggression object state according to the defined strategy. Usually, this task is realized through the feedback, i.e. information on the aggression object state, external environment influence on it, and results of “hybrid” actions (guiding teams). Accordingly, the control structures involved in the “hybrid” aggression exist due to information flows. If the flow is insufficient for decision-making, the information is non-qualitative and obsolete, the control processes are ineffective. Thus, the control effectiveness during the “hybrid” aggression depends on information quality and the key element is feedback channels between the aggressor and the aggression object which are used for coordination of all involved structures.

The feedback principle means the necessary element such as information exchange, thus, control within “hybrid” aggression means information process with feedback. Otherwise, the feedback

can be considered as potential channel of reflexive control. These channels are strategically important.

The reflexive control based on theoretical developments of V. Lefebvre specifies the effective use of comprehensive tools permitting to influence the adversary's decision-making favorable for other party as a result of formation of certain situations or demonstrations of potential threats [4]. According to V. Lefebvre, the reflexive control means the "process when of one of the parties provides the other party with the decision-making basis" [5]. So, the feedback communications substitute the adversary's motivation factors in order to force him to take unfavorable decisions.

Thus, the applicable aspects of the reflexive control are strategically important, are the effective tool of the "hybrid" aggression and SC, could have advantages compared to conventional tools. Using behavioral stereotypes, psychological aspects, personal data on team members (biographical data, traditions, etc.), the reflexive control enables to increase chances to achieve victory, meanwhile, this tactics includes adversary's detailed and qualitative information, which is received due to appropriate digital capabilities and software. The reflexive control tools include actions aimed at target intellectual forms and methods of the armed aggression except for the traditional terms such as camouflage (at all levels); disinformation, provocations, attention reflection; formation of tense information flow which processing requires resources; cognitive dissonance with decision-making function blocking; adversary's resources exhausting for solving unimportant tasks or fake threats; stimulating contradictions in allies' environment; psychological pressure, etc.

While fighting against the "hybrid" aggression the SC is deemed to be activity which is coordinated at strategic (military political) control level and aimed at controlling the decision-making processes both within country (country group) and outside it to achieve the victory. For this purpose SC fulfill to main functions such as internal – ensure communications with conflict subjects; external – communications with external environment.

The external communications ensures fighting system resilience, the internal communications which is related to military conflict control ensures permanent relation between control agents and objects raising the information importance. The absence of reliable information results in stagnation of control structure which works in inertial manner and ineffectively causing the collapse of the whole system.

Thus, the most important element of the fighting against the "hybrid" aggression is the communications process i.e. direct relation and feedback among all agents [7].

The adversary takes the necessary decision by changing the perception. *Perception* means the active process forming, not fixing the reality. While taking decisions the adversary uses information on conflict region, own troops and other party troops, and their combat capabilities. Based on SC technologies the influence on channels of information reception and messages content are ensured. The adversary uses the up-to-date optimization methods and searches the best solution. However, this solution would not be the best one chosen by us. In order to take own best solution it is necessary to know how the adversary forms the solution based on information which is deemed to be true. The SC ensures functioning of national system of strategic, defense, and operative planning, as well as reduction of effectiveness of the adversary's operative planning system.

When the decision-making process is targeted, it is necessary to ensure security of own strategic and operative function. Information, cultural, structural, and normative deficiencies in decision-making process on national security could threaten the country's security in fighting against the "hybrid" attacks.

Considering this fact, it is possible to define the following three main SC tasks within fighting against "hybrid" aggression: adversary's demoralization, legitimization of own actions in the population eyes, mobilization of target groups, and support of own political elite. In order to solve the SC tasks it is additionally necessary to forecast the adversary's behavior, imitate his decisions

depending on conditions, and choose the most effective information influence, this influence channels.

In order to use effectively SC technologies and reflexive control in fighting against "hybrid" aggression we propose to use the complex of the following activities:

- to focus SC efforts on conflict control;
- to define the responsible authority on SC planning and use;
- to develop plan of SC use where the aim, capabilities evaluation, frameworks, target audiences, information transfer channels, information provision methods, messages structure and orientation, media relations, asymmetric communications, and expected results should be specified;
- to ensure the use of all electronic communications – e-outlets (magazines, newspapers, and information agencies), social media (Facebook, Instagram, Twitter, and etc.), messengers (Telegram, Viber), blogs, and mobile communication;
- to develop dialog among conflict parties by ensuring equal information production and consumption by the conflict parties to develop messages depending on situation and audiences, as well as initiate conflict control;
- to consider the frames of traditional media;
- to implement activities against information interception and processing by the adversary in order to negative change and spread in social media and traditional media;
- to ensure permanent monitoring of new media;
- to develop and implement automated monitoring system of new media, social media, other messages and information accumulation;
- to consider impossibility of total control of information spread through new media;
- to ensure influence on adversary's decision-making and control process through narratives replacement;
- to ensure synchronization and structuring of all output SC information processes, exclude differences in facts assessment criteria;

- to ensure SC influence on service members and other combatants, civilians in the conflict region, and civil-military relations;
- to take the appropriate place in the process of development of national security strategy as mechanism of aim and actions relation;
- to develop national concept of fighting against "hybrid" warfare, its understanding and perception by target audiences; and
- to develop the single universal approach to SC within "hybrid" aggression by business and marketing rules.

The use of SC technologies within information warfare is an important resource of the "hybrid" warfare. The SC effectiveness defines the victory possibility during "hybrid" aggression.

Conclusions

The strategic communications are the integral element of the national security of Ukraine within RF "hybrid" aggression, propaganda, and disinformation about Ukraine in media and social media.

The military political misbalance of forces around Ukraine, ineffectiveness of the international law rules, economic, political, and military problems result in necessity to enhance the state SC system. The SC opportune and effective enhancement is vital in prevention of current challenges and threats to national security of Ukraine, their revealing, and response to them.

References

1. Hoffman, F. (2009), Hybrid Warfare and Challenges, *Joint Force Quarterly*, No. 52, pp. 34-39.

2. National Military Strategy of the United States of America (2015), available at: https://cutt.ly/3j1sEoJ (accessed 22 January 2021).

3. Lefebvre, V. (1982), *Algebra of Conscience: A Comparative Analysis of Western and Soviet Ethical Systems*, Reidel Publishing, Dordrecht, 220 p.

4. Lefebvre, V. (2010), *Lectures on the Reflexive Games Theory*

Paperback – September 2, Leaf & Oaks Publishers, 220 p.

5. Gorka, D.S. (2016), How America Will Be Attacked: Irregular Warfare, the Islamic State, Russia, and China, *Military Review*, 96(5), p. 30.

6. Bērziņš, J. (2014), Russia's new generation warfare in Ukraine: Implications for Latvian Defense Policy, *Policy Paper*, 2, pp. 2-14.

7. Kokoshin, A. (2018), *The Problems of the Applied Theory of War*, Publisher the Higher School of Economics, Moscow, 227 p.

8. Sinclair, N. (2016), Old Generation Warfare: The Evolution – Not Revolution – of the Russian Way of Warfare, *Military Review*, May-June, pp. 8-16.

9. Ivashchenko, A. (2015), Evolution of views on strategy of modern hybrid conflict and scenarios of countering hybrid threats, *Scientific Works of Center for Strategic Studies*, 1(53). pp. 18-23.

10. Salnikova, O., Mishchenko, V., Schidlyukh, V. and Antonenko, S. (2017), Use of Strategic Communications Technologies in the Governance System of Armed Forces of Ukraine, *Modern Information Technologies in Security and Defence*, 3 (30), pp. 61-66.

11. Sivokha, I. and Vorovich, B. (2015), XXI Century Wars and Hybrid War Technologies, *Scientific Works of Center for Strategic Studies*, 1 (53). pp. 24-30.

Viacheslav Semenenko
PhD (Technical Sciences), Senior Researcher
Deputy Head of the Centre for Military Strategic Studies
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-5774-0868

Andrii Ivashchenko
PhD (Technical Sciences), Associate Professor
Leading Researcher of the Centre for Military Strategic
Studies of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-8131-5463

Serhii Antonenko
Senior Inspector of the Main Inspectorate
of the Ministry of Defence of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0002-0729-8431

INTERNAL COMMUNICATIONS AS A WAY TO COUNTER HYBRID AGGRESSION IN BATTLEFIELD

A High Mobility Internal Communications Groups Project has been implemented with support of US and Ukrainian partners as part of implementation of the strategic communications concept in the UAF to introduce new technologies of internal communications in Joint Forces units. An analysis of the results of the work of highly mobile internal communications groups in the headquarters and units of the Allied Forces in the course of combat missions. It is proved that the organization of work of highly mobile groups of internal communications is one of effective measures of counteraction to hybrid aggression of the Russian Federation. Recommendations for the use of the communications technologies in the management processes in the headquarters and units of the Allied Forces in the course of combat missions.

Keyword: *internal communications, strategic communications, hybrid aggression, JFO.*

Introduction

Problem statement. Internal communications are an important component of the strategic communications system. Internal communications help personnel understand the military-political and operational-tactical situation and feel involved in the implementation of the overall operation plan. There is information exchange both from commanders to subordinate personnel and in the opposite direction within the framework of internal communications. According to the JFO experience, the lack of reliable information creates vacuum filled by the enemy. The information exchange process includes accumulation, structuring and processing of data used for informed decision-making. Insufficient effectiveness of internal communications leads to risks of ineffective decisions as well as misunderstanding between tactical and operational levels which can have serious consequences for strategic communications and success of the overall operation. That is why internal communications are very important during planning and conducting of any military operation, and their associated problems always remain relevant.

The analysis of recent researches and publications. According to NATO standards [1], internal communications are one of the crucial components of the strategic communications system. Internal communication is a line of information and propaganda support of military units (elements), military educational institutions, establishments and organizations of the Armed Forces of Ukraine performed within the system of information work by officials of military administration bodies and commanders (chiefs) through a set of actions related to processing and transmitting information to personnel through conversations [2].

A High Mobility Internal Communications Groups Project has been implemented with support of US and Ukrainian partners as part of implementation of the strategic communications concept in the UAF [3] to introduce new technologies of internal communications in Joint Forces units [4]. The project involved logistical and expert assistance from the US partners, NGO “Spirit of

America" and Ukrainian NGO "Initsiatyva Ye +" [5].

Purpose of the report is to determine the effectiveness of internal communications in the headquarters and units of the Allied Forces in the context of hybrid aggression.

Main part

High mobility internal communication groups (hereinafter – the Groups) are freelance groups of experts in moral and psychological support, social and legal protection, representatives of religious (public) organizations and creative community who are assigned to assist commanders of military units in establishing communication processes, providing prompt psychological help to the personnel, and carrying out socio-legal and cultural work. The Groups aim to establish internal communications in UAF military units (elements) as a component of effective C2 activities and leadership of commanders (chiefs) of all levels to achieve the appropriate level of motivation and loyalty of personnel and facilitate the military units (elements) to perform their assigned tasks. The Groups performed tasks in UAF operational and tactical groupings with a rotation period of 15–45 days.

Within the project, the Groups were divided according to the following lines: "Alpha" – ideological and moral support of military personnel, "Charlie" – prompt psychological assistance (support) to the personnel, "Delta" – socio-legal work, and "Omega" – administration and coordination of project processes.

The "Alpha" group consisted of the following specialists trained on special trainings: an inspector (a military communicator who underwent special training), a psychologist, a priest, and an information specialist (ideologist).

The Group aimed to establish communications within military units, especially between units and brigade headquarters. The "Alpha" Group had the following key tasks [6]:

- to assist commanders of the military units in establishing a system of internal communications with personnel;
- to introduce new internal communications technologies in

practice of combat activities;

- to organize feedback;
- to help the commanders promptly solve issues of daily and combat activities of the JF units.

Being provided with modern off-road vehicles, the Group significantly increased coverage of the personnel and units. Priority attention was given to the personnel of platoon and company bases of the first line of defense. In addition to helping the Group to achieve its planned objectives, such an approach helped increase personnel morale.

The Group have studied how internal communications influence the level of authority and leadership of commanders. Methods of "Action analysis", "Commander's information", "Situational leadership", assessment of moral and psychological condition of the personnel and determining influence of the relevant commander's activities on this condition were used in the research.

The research examined the following issues: internal communications process, internal communications characteristics, internal communications information, its classification, media, internal communications organization models, internal communications means, their advantages and disadvantages, internal communications tools, internal communications feedback, ways to solve problems and implement new technologies of internal communications [7].

According to the NATO standards, several organization models of internal communications can be used [8].

According to the first model, internal communications mobile groups (special headquarters elements) shall be established. This option is used in strategic and operational level headquarters. Such location of internal communications specialists guarantees effective supervision over strategic communications at the strategic level.

The second model envisages establishment of a position of the Deputy Chief of Staff for Internal Communications and relevant subdivisions responsible for organizing internal communications,

analyzing information from the media, liaising with the media to disseminate necessary narratives and messages, directing and coordinating information and psychological operations, civil-military cooperation operations, and influencing important VIPs.

The third model envisages a position of the JF Deputy Commander for Internal Communications responsible for organizing all internal communications during the entire period of operations.

In each model, a person in charge of internal communications has direct access to the JF commander.

As far as internal communications are crucial in countering aggressive information influences, it is advisable to significantly strengthen the role of strategic communications elements in the C2 system. Thus, it is sufficient to use the first model at the strategic level (in the General Staff of the Armed Forces of Ukraine) to create an appropriate military-political level narrative and ensure that the internal communications strategy is reflected in operation planning. At the operational level (Headquarters Joint Operations, operations commands), it is advisable to choose the second model with establishment of a deputy chief of staff position who would arrange internal communications, information operations, psychological operations and civil-military cooperation. As far as concentration, coordination and synchronization of all efforts is crucial to create favorable conditions for JF tasks (or subsequent operations) and persuade target audiences, introduction of a special deputy commander position in a troops (forces) headquarters in the area of the operation will allow to achieve even greater centralization of communication management. Therefore, the third model shall be used.

A system or organizational tools as well as personal commander's efficiency tools shall be used to form internal communications. However, the most effective and frequently used internal communications tools are: meetings (32%), information messages (26%), informal communications (17%), a corporate website or a Facebook page (14%), and printed publications (11%). Such a tool as "open door policy" should also be highlighted. This concept is taken from the practice of the armed forces of NATO

member countries and means that any serviceman can address commanders of various levels with any question. From internal communications perspective, it relates to building an additional feedback channel independent of the C2 hierarchy. This is extremely important for making decisions about the use of units.

Internal communications feedback is organized and formed through informal events, open door policy and evaluation reports. It is difficult to manage the feedback process, especially its informal part. Therefore, it is possible to provide only general advices that can help achieve more effective communications in case they are adjusted to a particular unit, or rather to servicemen of this unit.

While arranging feedback, it is necessary to take into account servicemen's character traits, their interests, hobbies and aspirations. The "open door" policy helps partially solve the internal communications information reliability issue: the serviceman can report his proposals, difficulties and dissatisfaction himself bypassing the intermediate C2 levels. Servicemen evaluation reports are an effective mechanism of internal communications. It gathers information about each serviceman's character and other factors that influence his behavior, hence, a communication process he is involved.

Let us consider ways to solve problems and implement new effective internal communications technologies. The Group examined internal communications in JF headquarters and units, opinions of their chiefs and commanders and made some conclusions about how to solve problems and implement new effective internal communications technologies. The Group has defined the following key practices to consider:

- to constantly struggle for your actions to be perceived as legitimate, worthy of trust and support, to ensure necessary influence, to act actively, proactively and quickly;
- to understand the operational environment where actions take place, the audience and the content of senior command's directives, to support actions with internal communications tools;
- to assign personnel responsible for assisting the commander in developing a communication strategy and synchronizing with

strategic communications activities to achieve synergy;

- to use opportunities of training in internal communications, informing and influencing not only on those who are directly involved in communications, information operations, and organizes contacts with influential players in the operation area, but also on those who use forces and means against the enemy;
- to continuously review and analyze operational environment and important audiences to keep internal communications correct and effective [9].

Servicemen of some units do not understand the extent of their influence on the course of the operation under the conditions of the interaction-related formed difficulties. From the perspective of tools, such problems can be solved through the following measures: clear prescription of responsibilities, ensuring openness and transparency of internal relations, management control, eliminating information duplication at the organizational level, training in internal communications, and assistance in building the internal communications system.

This refers more to measures for implementation of internal communications standards adopted in the armed forces of NATO member countries. These measures are carried out within internal communications system which, on one hand, depend on personal effectiveness of a commander, and, on the other hand, is a system management tool.

The work of the Group in the UAF headquarters and units performing tasks in the JFO area allowed to:

- promptly identify problematic issues in JF units and take appropriate measures;
- stabilize moral and psychological condition of the personnel;
- collect (together with the JF Headquarters Experience Generalization Department) practical information about various issues of the use of troops (forces);
- organize prompt informing the leadership of the Armed Forces of Ukraine about the situation in the JFO area (informing the

military leadership about potential risks that may adversely affect the accomplishment of combat tasks).

In the course of the Group's work, the command staff of brigades and each unit analyzed actions taken, commander's (combat, targeted) informing, priority of incentives, and situational leadership. The above mentioned methods were methodologically supported with recommendations on how to increase their effectiveness. A number of consultations on social and legal issues were provided to servicemen of combat units. The personnel, the level of authority and leadership of brigade commanders and their deputies were assessed.

Conclusions

Thus, the tasks accomplished by the high mobility groups allowed creating an effective system of internal communications between commanders and personnel, to maintain and restore moral and psychological condition of units and their psychological readiness to perform combat tasks. Arrangement of constant feedback from the headquarters and units, obtaining objective information by the UAF leadership, identification and prompt resolution of problematic issues that adversely affect the moral and psychological condition of personnel were the most effective part of the accomplished work.

References

1. Verbytska, A.M., Savchenko, V.A., Dziuba, T.M. and Katsalap, V.O. (2017), The Strategic Communications System of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, *Science and Defense*, No. 1, pp. 34-39.

2. General Staff of the Armed Forces of Ukraine (2017), *The Order No. 4 "On Approval of the Instruction on Arranging Information and Propaganda Support in the Armed Forces of Ukraine", dated 04 January, 2017*.

3. Ministry of Defense of Ukraine (2017), *The Order No. 612 "The Concept of Strategic Communications of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine", dated 22 November, 2017.*

4. General Staff of the Armed Forces of Ukraine (2015), *The Order No. 472 "On Organization of High Mobility Groups for Internal Communications in the Military Units (Elements) of the Armed Forces of Ukraine", dated 3 December, 2015*.

5. NATO (2015), *NATO Strategic Communications Handbook: Draft for Use Ver. 9.1.21–31*, Norfolk, VA: Supreme Allied Command Transformation HQ, 86 p.

6. General Staff of the Armed Forces of Ukraine (2018), *The Order No. 345 "Instruction on Organizing the Workflow of Internal Communications High Mobility Groups in the Armed Forces of Ukraine", dated 22 October, 2018.*

7. Semenenko, V. and Ivashchenko, A. (2020), Organizing Internal Communications in the Headquarters and Units of the Armed Forces of Ukraine in Carrying out Tasks in the Area of Operation of the Joint Forces, *Collection of the Scientific Papers of the Centre for Military and Strategic Studies*, No. 1 (68). https://doi.org/10.33099/2304-2745/202.

8. Hrebenyuk, M. (2017), *Fundamentals of Strategic Communications According to NATO Standards*, NDUU, Kyiv, 180 p.

9. Semenenko, V. and Shidlyukh, V. (2019), Organizing Internal Communications in the Joint Forces, *Philosophical, Sociological, Psychological and Pedagogical Issues of Preparing a Person for Performing Tasks in Special Conditions": Proceedings of the scientific-practical conference*, pp. 249-250.

Maryna Semenkova
Instructor of Foreign Languages Education and Research Centre
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-4143-5671

THE POPULATION MOVEMENTS IN THE HYBRID WAR CONCEPTS

The article examines the issue of use the population movements as the instrument of the hybrid influence. The author studied some of the well-known concepts of contemporary conflicts and identified the peculiarities and the main characteristics of the population movements for the policy actor to be interested in using them. The author points out that the current level of technological development increases the opportunity for the adversary to control and direct population movements and, therefore, to use them as a destructive instrument in the hybrid war context. The article substantiates the necessity to constantly monitor the population movements in order to identify if they are going to be used by the policy actor as a hybrid influence instrument and, accordingly, the necessity to address the issue while preparing the security and defence sector specialists.

Keywords: *hybrid war concepts, instrument of hybrid influence, population movements, directed migration processes, coflictogenity.*

Introduction

Problem statement. The graduate transition from the understanding of war purely as a violent military conflict caused the emergence of the modern wars concepts as well as the scientific search for the modern wars means and instruments. The combination of military and non-military means and the blurred line between the war and peace substantiated the use of the word “hybrid” related to this sort of conflicts. As the instruments of the hybrid warfare we can regard the phenomena, processes and the algorithm of actions that are used to change the characteristics of the object and the course of actions. Considering the state as the object of hybrid influence we

can treat, for example, its political destabilization, the deteriorating economic situation, the loss of social coherence as the changes in its characteristics that makes the balance of power the beneficial one for the foreign policy actor.

The analysis of recent researches and publications. Though there are numerous case-studies of the use of population movements and, particularly, the migration processes we can mention only a few that study the issue of using them as a policy instrument [1–3]. We can also state the lack of studies that examine the following aspects: the preconditions for the external influence on the international processes of the population movements; how the political actor's directing of the migration processes with the aim of their further use as a destructive policy instrument can be identified and prevented [4; p. 143].

Purpose of the report is to identify the principal characteristics of the population movements that turn them into the attractive hybrid warfare instrument.

Main part

Having studied some of the most well-known concepts of the contemporary foreign policy confrontation we identified the principal methods and instruments for the hybrid influence, than we identified the population-related ones:

The use of political refugees for propaganda purposes in the concept of Political Warfare by G. Kennan [5];

Riddance to the active segment of population in the concept of Mutiny-War by E. Messner [6];

The psychological and informational pressure on the population; causing the tension and turmoil among the population in the Forth-Generation Warfare [7];

The political control over the excluded or displaced population; the intimidation and the violence towards the population; the expulsion of the population with the inappropriate identity in the concept of the New Wars by M. Kaldor [8];

The preparation of the population to the participation in the unrests, protests, etc. in the Hybrid War concept by V. Gorbulin [9];

In the context of the above-mentioned concepts the population movement seems to be reasonable for the policy actor if: 1) local population defies the external influence; 2) newly immigrated population can be turned into the source of conflictogenity. The important feature of the population movements like the directed migration cannot bear the conflict potential at the first glance; however they can be used to achieve the necessary strategic results, to gain the foreign policy advantage in order to achieve the hybrid war objectives.

As a whole we can define two main characteristics of the population movements that explain the policy actor's interest in their use as a hybrid warfare instrument:

1) Their effectiveness that means that the actor by using the population movements can change the status of the target country and made it to change its policy according to the geopolitical interests of the actor;

2) To be used as the hybrid warfare instruments the population movements must be controlled and directed by the policy actor. Given the peculiarities of the hybrid influence such as its non-obvious nature, the foreign policy actor has to control and direct the population movements in a hidden way or to pretend having the noble motivation.

The international migration processes as the example of the population movements can be used as the hybrid war instruments both due to their effectiveness and their ability to be controlled and directed.

Their effectiveness was demonstrated by the political, demographic, economic, social consequences of international migration for the states over the centuries. In contemporary world the migration has obtained the unprecedented scale, there isn't any country excluded from the process of the global population movement.

In the context of the hybrid warfare we can consider the possibility of use the population movements first of all with the aim to worsen the conditions of functioning and development of the target country, to weaken its political and socio-economic situation and, subsequently, to take control of the country. For instance it can

be achieved by concentrating in the certain country or region the number of people who, being controlled by the actor will be able to contribute to the achievement of the actor's destructive goals.

However, the second condition for the international migration to be used as the hybrid influence instrument has emerged fairly recently, along with the rapid development of the information technologies and the access of the general public to Internet all over the world together with the technologies of the mass consciousness manipulation. The interested foreign policy actors have obtained the opportunity to encourage people to migrate, influence on their choice as for the direction of migration and on the behaviour of both migrants and locals. Besides it can be possible for the actor to influence on the number of migrants and the migrants with certain age, occupations and/or ethnic, religious identity, etc. For example one of the essential effects of directed migration in the hybrid war context can be the increasing the conflictogenity level of society, the formation of the protest potential and, respectively, further destabilization of the country from the inside.

Conclusions

Given the growing opportunities of directing the international migration processes as well as the population movements as a whole we must expect the raising possibility of their use as the hybrid warfare instrument. It forces us to take that fact into account when studying the national defence and security policy issues, inter alia the population movements must be constantly monitored with a view to their possible destructive effect on the state and the possibility of them to be directed by the adversary actor in its aggressive foreign policy objectives. It is also necessary to work out the set of measures to prevent such destructive use of the population movements. Accordingly, this new role and peculiarities of the popular movements must be properly addressed while preparing the security and defence sector specialists.

References

1. Greenhill, K.M. (2016), Migration as a Weapon in Theory and in Practice, *Military review*, 96(6), p. 23-36.

2. Veselska L.A. (2017), "Masova vymushea migratsiia yak instrument vedennia gibrydnoi viiny" [Mass forced migration as a tool for hybrid warfare Manager], *Bulletin of Donetsk State University of Management*, pp. 108-117.

3. Malynovska, O.A. and Kolomoiets, O.O. (2017), "Migratsiinyi aspect gibrydnoi viiny Rosii proty Ukrajiny" [Migration aspect of Russia's hybrid war against Ukraine], *Demography and the Social Economy*, 2(30), pp. 78-88.

4. Semenkova, M.A. (2020), "Mizhnarodni nigratsiji protsessy yak instrument gibrydnogo vplyvu: stan vyvchennia problemy" [International migration processes as a tool of hybrid influence: the state of study of the problem], *Actual Problems of Politics*, Vol. 65, pp. 139-146. https://doi.org/10.32837/app.v0i65.318.

5. Kennan, G. (1948), *The inauguration of organized political warfare*, available at: https://cutt.ly/EjBEwgf (accessed at 23.01.2021).

6. Messner, E.E. (2005), "*Khotchesh mira, pobedi miatezhevojnu!"* [*If You Want Peace, Defeat the Rebellion!*], available at: https://cutt.ly/wjBE0Ka (accessed at 23.01.2021).

7. Lind, W., Nightengale, K., Schmitt, J., Sutton, J. and Wilson, G. (1989), The changing face of war: into the forth generation, *Marine Corps Gazette*, October, pp. 22-26.

8. Kaldor, M. (2012), *New and old wars: organized violence in a global era*, Polity Press, Cambridge, 268 p.

9. Gorbulin, V.P. (2015), "*Ukrayina i Rosija: devjatyi val chy kytajska stina*" [*Ukraine and Russia: the ninth wave or the Chinese wall*], NISD, Kyiv, 132 p.

Pavlo Shchypanskyi
Candidate of Military Sciences (PhD in Military), Professor
Deputy University Commandant for Science of the National Defence
University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-0854-733X

Mykhailo Hrebeniuk
Candidate of Historical Sciences (PhD in History)
Education & Research Centres Chief of the National Defence
University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-4661-4265

Valerii Hrytsiuk
Candidate of Historical Sciences (PhD in History), Associate Professor
Leading Research Fellow of the Military History Research Centre
the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-9877-1900

HISTORICAL PERIODIZATION OF ARMED AGGRESSION OF THE RUSSIAN FEDERATION AGAINST UKRAINE (2014–2020)

The processed array of sources and literature makes it possible to reproduce with a high degree of probability the actual course of major events in chronological order and highlight the key milestones of the Russian-Ukrainian armed confrontation at the beginning of the 21th century. According to the nature of hostilities, military-political results and consequences the armed aggression of the Russian Federation against Ukraine in 2014–2020 is divided into initial and three that differ qualitatively in purpose, nature and content of combat (special) actions. The authors prove that it was the aggression of Russian Federation that caused the armed conflict in the East of Ukraine. Ukraine has used the forces of the security and defence sector to repel and deter this aggression. The form of their application from April 14, 2014 to April 30, 2018 was an anti-terrorist operation, and after – the Joint Forces

Operation. This provided a basis for further research into the armed conflict in the East of Ukraine to provide a clear understanding of the nature and essence of Russia's hybrid war against Ukraine, to analyse its evolution, and, moreover, to summarize the experience of countering hybrid threats in the military sphere.

Keywords: *"hybrid war", armed aggression of Russian Federation against Ukraine, military action, political and military strategy, Armed Forces of Ukraine, Armed Forces of the Russian Federation, illegal armed formations, periodization.*

Introduction

Problem statement. At the beginning of the XXI century, the Russian Federation (hereinafter – RF), strengthening the authoritarian regime and strengthening its military potential, began to claim the status of a world power, one of the main centres of global influence on international relations and the modern world order. Remarks such as that not the idea of territorial integrity and constitutional order should be in the epicentre of the formation of the modern Russian nation but the "millennial Russian civilization project" have become more and more common.

In Russia, much attention is paid to the development of theory and practice of hybrid forms and methods of pressure on other states. Hybrid warfare is conducted comprehensively. Its main components are: ideological, informational, military, socio-political, diplomatic, economic and terrorist. In a series of "frozen conflicts" (Nagorno-Karabakh, Transnistria, Abkhazia, South Ossetia), the aggressor – Russia and Kremlin-led local collaborators – followed a similar scenario, but the methods of hybrid action were constantly improved. A common feature of such a "war" is the "blurring" of the features of the armed conflict and the involvement of various non-military forces and means, which fundamentally distinguishes it from war in the classical sense.

In early 2014, Euromaidan demonstrated that Russia was losing control of Ukraine. Under these conditions, the military-political leadership of the RF resorted to armed aggression which was a planned mean of forcible subjugation of Ukraine. Crimea became the

first object of aggression of the RF against Ukraine. The armed aggression of the RF against Ukraine has shown that its conduct is largely a departure from traditional forms and methods of warfare. Military experts from different countries emphasize that Russian aggression is of a hybrid nature.

The military-historical analysis of the Russian armed aggression of a hybrid nature, which began against Ukraine in 2014, envisages a number of successive research stages. The ordering of knowledge about the historical process begins with a chronological fixation and description of the events of the past. Based on a reliable and complete historical chronicle of events related to the aggression of the RF and applying scientific methodology it is possible to identify not only causal relationships, but also to determine the factors due to which these relationships acquire new stable qualities and become objective laws.

Military-historical science considers periodization as one of the methods of studying military conflicts [6; 19; 21; 35; 44]. The essence of this method is the division of wars and armed conflicts into certain time intervals (periods, phases, stages), which differ qualitatively in military-political goals, nature and content of hostilities. The boundaries of the period are determined by events that mark turning points in military conflicts. Each period covers a certain number of military campaigns and operations. It is important to note that the planning and conduct of operations is carried out according to their objectives. In turn, in military history research, while describing operations that have already taken place, they are usually divided into stages. In the Western European military-historical literature, the terms “phase” and “stage” are actively used to periodize historical processes, in particular, to denote the substructural components of the period.

Military experts use different types of periodization of military conflicts, in particular, distinguish between strategic and historical periodization. Strategic periodization is established during the planning of the war and implemented during its development. This involves the division of the war into several successive parts

(campaigns), in each of which certain objectives are achieved by one or another composition of the armed forces. At the same time, military historians use periodization which divides the war according to the actual course depending on the results achieved. Historical periodization is determined by the sequence of actions, each time period of which has its own name according to its content.

The analysis of recent research and publications. A number of studies, diversed in scope and form, have already been devoted to the periodization of the Russian armed aggression against Ukraine, the armed conflict in the East of Ukraine, and the anti-terrorist operation / Joint Forces operation [1–5; 7–9; 11; 16–17; 22–25; 36–41; 51; 53].

In the project by "Information Resistance" group named "The Invasion of Ukraine: Chronicle of Russian Aggression" [17], the events of the armed conflict are presented through the author's analysis of Russian aggression in 2014–2016, which is conditionally divided into 11 stages. Because the book appeals to a wide audience, the periodization of the armed conflict is more popular than scientific.

A Ukrainian national historian Pavlo Guy-Nizhnik divides the events of the Russian-Ukrainian armed conflict into five periods in his scientific work "War in the East of Ukraine: the first phase (March 1 – August 24, 2014)". In their formulation, the author tries to use the style of large-scale periodization of big wars ("position war", "frail war"), but instead of using military terminology he fails to avoid the use of literature cliches (like "Front without resistance", "Minsk trap", "Norman odds", etc.) [10].

Volodymyr Vilk's work "Periodization of the Russo-Ukrainian Hybrid War: 2014–2017" [45], despite its stated name, defines only the periodization of the so-called information-psychological war of the Russian Federation against Ukraine in 2013–2015.

Representative of Lviv Military History School, Doctor of Historical Sciences, O. M. Kutska divides the anti-terrorist operation in two periods within which she allocates 14 stages "in order to identify and isolate indirect changes in studying the experience of

using the Armed Forces and other paramilitary formations of Ukraine (emphasized by us because the term is not precise) within the framework of anti-terrorist operation in 2014–2018" [20]. However, the Lviv researcher does not explain many of her approaches, in particular: why he determines the gap between the second (21.5 – 6.7.2014) and third (7.7.2014) stages of the manoeuvring period (emphasized by us) and does not take into account that the beginning of active actions of the anti-terrorist operation forces accounts for 1 July 2014 – in accordance with the decision of the Supreme Commander of the Armed Forces of Ukraine. The place of the Debaltsevo operation (February 2015) in the periodization remains unclear. The author indicates the date of completion of the ATO – 23.02.2018. In fact, a large-scale anti-terrorist operation in some areas of Donetsk and Luhansk oblasts lasted from April 14, 2014 to April 30, 2018. On that day, the format the anti-terrorist operation in the East of Ukraine was changed for the Joint Forces Operation.

Scientists of the Central Research Institute of the Armed Forces of Ukraine proposed another version of the periodization of the anti-terrorist operation dividing it into stages [12–15; 38; 52]. This approach seems appropriate because the periodization of transactions is carried out as described above in stages. However, if we analyse the armed conflict or war in general and seek to emphasize its significance for Ukrainian society and the international community, in our opinion, it is appropriate to divide the time in history, when the Russian aggression against Ukraine continued, into periods.

Purpose of the report is to offer a version of the periodization of the Russian armed aggression against Ukraine in 2014–2020, to structure the accumulated factual material and create a basis for further scientific research to study this phenomenon to have a clear understanding of the nature and essence of Russia's hybrid war against Ukraine, to analyse its evolution and, finally, to generalize the experience of counteracting hybrid warfare in the military sphere.

Main part

The Scientific Centre for Military History of Ivan Cherniakhovskyi National Defence University of Ukraine worked out the scientific and journalistic publication "White Book of the Anti-Terrorist Operation in the East of Ukraine (2014–2016)" [43]. The cooperative involvement of various structures of the security and defence sector made it possible to comprehensively explore the role and place of the Ukrainian defence forces in counteracting the aggressor [46–50]. The authors carried out a historical periodization of the armed conflict in the East of Ukraine, dividing it into major periods and distinguishing in them the stages that are qualitatively different in purpose, nature and content of hostilities. The authors covered the actual course of the major events in chronological order and highlighted the key milestones of the Russian-Ukrainian armed confrontation at the beginning of 21st century. The periodization of the armed conflict in the East of Ukraine was agreed by the General Staff of the Armed Forces of Ukraine and approved by the Minister of Defense of Ukraine. The English-language version of the book was presented at the NATO-Ukraine Partnership and Collective Security Committee meeting held at Alliance Headquarters in November 2017. The materials of the White Book of the ATO, including the historical periodization of the ATO, have been approved by representatives of NATO countries and taken into account in the coverage of the events of the armed conflict in the East of Ukraine. However, this version of periodization of the armed conflict in the East of Ukraine was not complete enough as it was limited by the events of 2016.

At the request of the Administration of the President of Ukraine, specialists of the Military History Research Center prepared information and reference materials on the chronology of events in 2014–2019 that took place in the Autonomous Republic of Crimea and during the ATO/JFO in the East of Ukraine [52]. Relevant materials [18] were sent to the education authorities, educational

institutions for use in lessons of Ukrainian history, as well as during the organization and conduct of patriotic educational activities.

The authors of this report participated in the development of the historical periodization of the anti-terrorist operation in East of Ukraine, certified in February 2020 by the Copyright Registration Certificate of the Ministry of Economy, Trade and Agriculture of Ukraine (No. 96155, registration date 18.02.2020).

Merging all the developments, we propose such a version of the periodization of the Russian armed aggression against Ukraine in 2014–2020.

The initial period of the Russian armed aggression Occupation by the Russian Federation of the Autonomous Republic of Crimea. Demonstration actions to deploy groups of troops (forces) on the borders. destabilization of the situation by the Russian special services in the Eastern and Southern regions of Ukraine (February 20 – early April 2014) [12].

I period of the armed conflict in the East of Ukraine. Overcoming the "hybrid aggression". The active engagement of the ATO forces in the liberation of Donetsk and Lugansk regions from the Russian terrorist groups. Holding off the Russian troops invasion (beginning of April – September 5, 2014).

- The first stage. Employment of the armed conflict in the East of Ukraine by the intelligence services of the Russian Federation (April – June 2014).
- The second stage. Liberation of the territory of the East of Ukraine from Russian terrorist cells (July 1 – August 24, 2014).
- The third stage. The invasion of the Russian Armed Forces military units on the territory of the Donetsk and Luhansk regions of Ukraine (August 25 – September 5, 2014).

II period of the armed conflict in the East of Ukraine. Conflict localization in certain districts of Donetsk and Luhansk oblasts (September 5, 2014 – April 30, 2018).

- The Fourth Stage. Stabilization of the Confrontation Line in the East of Ukraine (September 5, 2014 – January 14, 2015).

- The Fifth Stage. Repulse of the Second Offensive of the Russian Occupation Forces (January 15 – February 20, 2015).
- The Sixth Stage. Strengthening the Defence Line in East of Ukraine (February 21, 2015 – September 20, 2016).
- The Seventh Stage. Breeding of forces and means of warring parties (from September 21, 2016 – November 2017).
- The Eighth Stage. Improvement of troops (forces) command and control system. Completion of anti-terrorist operation (November 2017 – April 2018).

III period of the armed conflict in the East of Ukraine Conduct of Joint Force Operation (from April 30, 2018).

The use of the Joint Forces in the third period was characterized by a transition to predominantly defensive actions; was determined by the requirements for the withdrawal of heavy weapons from the line of demarcation and the creation of security zones, by stable retention by the joint forces of certain areas, boundaries and positions, a slow advance of Ukrainian subunits deep into the territory and taking control of certain settlements of the so-called "grey zone" without violating the Minsk agreements.

Conclusions

The armed aggression of the Russian Federation against Ukraine has had devastating effects on European and global security. At the same time, the aggression testified that the application of the forces was largely a departure from the traditional forms and methods of warfare and had elements of a "hybrid" nature.

The armed aggression of the RF led to the occupation of the Crimea, and to an armed conflict in the East of Ukraine [26–34]. To counteract and deter this aggression, the Ukraine has deployed the security and defence sector forces. From April 14, 2014 the form of application of the security and defence forces was the anti-terrorist operation (ATO), and from April 30, 2014 it is the Joint Force Operation (JFO).

The events of 2014–2020 became the most serious exam for the existence of Ukrainian state. In this tumultuous time of trials,

military personnel of the Armed Forces of Ukraine, other military formations, representatives of law enforcement and volunteer formations displayed personal courage and heroism in the defence of the state sovereignty and territorial integrity of Ukraine, selfless service to the Ukrainian people.

Ukraine's experience of battling "hybrid" aggression in the military sphere needs a comprehensive study.

The military-historical analysis made in the report is the basis for further scientific research to study the armed aggression of the RF against Ukraine in order to have a clear understanding of the nature and essence of Russia's "hybrid" war, analyse its evolution and finally summarize the experience of countering "hybrid" military aggression in the military sphere, investigate the peculiarities of the military units (sub-units) employment in a "hybrid" type of conflict.

References

1. Analitychna dopovid do Shchorichnoho Poslannia Prezydenta Ukrainy do Verkhovnoi Rady Ukrainy "Pro vnutrishnie ta zovnishnie stanovyshche Ukrainy v 2016 rotsi" (2016), NISD, Kyiv, Ukraine.
2. Analitychna dopovid do shchorichnoho Poslannia Prezydenta Ukrainy do Verkhovnoi Rady Ukrainy "Pro vnutrishnie ta zovnishnie stanovyshche Ukrainy v 2018 rotsi" (2018), available at: http://www.niss.gov.ua/articles/3143/ (accessed 05 January 2021).
3. *Analiz boiovykh dii v raioni Ilovaiska pislia vtorhnennia rosiiskykh viisk 24–29 serpnia 2014 roku*, available at: http://www.mil.gov.ua/news/2015/10/19/analiz-illovausk--14354/ (accessed 5 January 2021).
4. *Analiz Heneralnoho shtabu ZSU shchodo boiovykh dii na Debaltsivskomu platsdarmi z 27 sichnia do 18 liutoho 2015 roku*, available at: http://www.mil.gov.ua/analitichni-materiali/analiz-generalnogo-shtabu-zsu-shhodo-bojovih-dij-na-debalczevskomu-placzdarmi-z-27-sichnya-do-18-lyutogo-2015-roku.html (accessed 5 January 2021).
5. *Analiz vedennia antyterorystychnoi operatsii ta naslidkiv vtorhnennia Rosiiskoi Federatsii v Ukrainu u serpni-veresni 2014 roku*, available at: http://www.mil.gov.ua/content/other/anliz_rf.pdf (accessed 05.01.2021).
6. Berezhynskyi, V.H. (2015), *Metodolohyia y struktura voenno-ystorycheskoho yssledovanyia*, Vydavets Oleh Filiu, Kyiv, Ukraine.

7. Berezovets, T. (2015), *Aneksiia: ostriv Krym: khroniky "hibrydnoi viiny"* [*doslidzhennia zakhoplennia pivostrova*], Brait Star Pablishynh, Kyiv, Ukraine.

8. Bulakh, A., Senkyv, H. and Teperyk, D. (2017), *Pervye na peredovoi: otrazhenie voennoi ahressii Rossii protiv Ukrainy*, International Centre for Defence and Security, Tallynn, Estonia.

9. *Do druhoi richnytsi ahresii Rosii proty Ukrainy* (20 liutoho 2016 roku) (2016), NISD, Kyiv, Ukraine.

10. Hai-Nyzhnyk, P. (2018), Viina na Skhodi Ukrainy: persha faza (1 bereznia – 24 serpnia 2014 r.) "Viina na Donbasi. 2014–2017 rr.", *III Ukrainian scientific military history conference*, National military history museum, Kyiv, Ukraine, 19 April 2018, pp. 29–34.

11. Hladka, K., Hromakov, D. and Myronova, V. (2017), *Dobrobaty*, Folio, Kharkiv, Ukaine.

12. Hrebeniuk, M., Hrytsiuk, V. and Skriabin, O. (2018), The Main Events of the First Period of Armed Conflict in the East of Ukraine (April - September 2014), *Codrul Cosminului*, XXIV, No. 2, Romania, pp. 377–408.

13. Hrytsiuk, V.M. (2016), Rozghortannia voiennoho konfliktu na Skhodi Ukrainy (vesna 2014 roku), *Voienna istoriia*, No. 1(80), pp. 64–69.

14. Hrytsiuk, V.M., Horielov, V.I. and Skriabin, O.L. (2017), Zbroinyi konflikt na Skhodi Ukrainy – naslidok rosiiskoi ahresii "Viina na Donbasi. 2014–2016 rr.", *II Ukrainian scientific military history conference*, 20 April 2017, National military history museum, Kyiv, Ukraine, pp. 206–208.

15. Hrytsiuk, V.M. and Skriabin, O.L. (2017), Periodyzatsiia zbroinoho konfliktu na Skhodi Ukrainy, *Ukrainian scientific practical conference "Rol i mistse natsionalnoi spetssluzhby v istorii ukrainskoho derzhavotvorennia"*, 17 March, Kyiv, Ukraine, available at: http://science.univ.kiev.ua/sbu.pdf (accessed 5 January 2021).

16. Huralska, A. (2015), *Zvit: dobrovolchi bataliony. Vynyknennia, diialnist, superechnist, Antykor*, available at: https://antikor.com.ua/articles/46226-zvit_dobrovoljchi_bataljjoni._viniknennja_dijaljnistj_superechnosti (assessed 5 January 2021).

17. Husarov, V., Karyn, Yu., Mashovets, K. and Tymchuk, D. (2016), *Vtorzhenie v Ukrainu: Khronika rossiyskoy agressii*, Brait Star Pablyshynh, Kyiv.

18. Informatsiini materialy do 5-richchia vid pochatku zbroinoi ahresii Rosiiskoi Federatsii proty Ukrainy, available at: https://uinp.gov.ua/informaciyni-materialy/viyskovym/do-5-richchya-vid-pochatku-zbroynoyi-agresiyi-rosiyskoyi-federaciyi-proty-ukrayiny (accessed 5 January 2021).

19. Kovalchenko, Y.D. (2003), *Metody istoricheskogo issledovaniya*, Nauka, Moscow, Russia.

20. Kutska, O.M. (2019), Antyterorystychna operatsiia na Skhodi Ukrainy (2014–2018 rr.): etapy ta yikh kharakterystyka, *International scientific conference "Liudyna i tekhnika u vyznachnykh bytvakh svitovykh voien XX stolittia"*, Natsionalna akademiia Sukhoputnykh viisk imeni hetmana Petra Sahaidachnoho, 25–26 Jun, Lviv, Ukraine, pp. 16–18.

21. Login, V.T. (1979), *Dialectika voenno-istoricheskogo issledovaniya*, Nauka, Moscow, Russia.

22. Maiorova, A. (ed.) (2017), *Donbas v ohni. Putivnyk zonoiu konfliktu*, Tsentr doslidzhennia bezpekovoho seredovyshcha HO "Prometei", Lviv, Ukraine.

23. Mamchak, M.A. (2014), *Aneksiia Krymu. Anatomiia «hibrydnoi» viiny*, Sevastopol, Ukraine.

24. Marko, S. (2016), *Khronika hibridnoy voiny*, Alterpres, Kyiv, Ukraine.

25. Muzhenko, V. (2015), *Dvanadtsiat dniv shcho zminyly khid ATO*, Narodna armiia, Kyiv, Ukraine.

26. Pro chastkovu mobilizatsiiu (2014), Ukaz Prezydenta Ukrainy vid 17 bereznia 2014 r. No 303/2014, *Ofitsiinyi visnyk Prezydenta Ukrainy*, No. 12, 4 Apr 2014, Art. 469.

27. Pro osoblyvosti derzhavnoi polityky iz zabezpechennia derzhavnoho suverenitetu Ukrainy na tymchasovo okupovanykh terytoriiakh u Donetskii ta Luhanskii oblastiakh (2018), Zakon Ukrainy vid 18 sichnia 2018 r. No 2268-VIII, *Vidomosti Verkhovnoi Rady Ukrainy*, No 10, 9 Mar 2018, Art. 54.

28. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 13 kvitnia 2014 roku "Pro nevidkladni zakhody shchodo podolannia terorystychnoi zahrozy i zberezhennia terytorialnoi tsilisnosti Ukrainy" (2014), Ukaz Prezydenta Ukrainy vid 14 kvitnia 2014 r. No. 405/2014, *Ofitsiinyi visnyk Prezydenta Ukrainy*, No. 14, 14 Apr. 2014, Art. 745.

29. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 2 veresnia 2015 roku "Pro novu redaktsiiu Voiennoi doktryny Ukrainy" (2015), Ukaz Prezydenta Ukrainy vid 24 veresnia 2015 r. No. 555/2015, *Ofitsiinyi visnyk Ukrainy*, No. 70, 09 Oct. 2015, Art. 2592.

30. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 kvitnia 2018 roku "Pro shyrokomasshtabnu antyterorystychnu operatsiiu v Donetskii ta Luhanskii oblastiakh" (2018), Ukaz Prezydenta Ukrainy vid 30 kvitnia 2018 r. No 116/2018, *Ofitsiinyi visnyk Prezydenta Ukrainy*, No. 10, 30 Apr. 2018, Art. 174.

31. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy" (2015),

Ukaz Prezydenta Ukrainy vid 26 travnia 2015 r. No. 287/2015, *Ofitsiinyi visnyk Ukrainy*, No. 43, 09 Jun 2015, Art. 1353.

32. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo vyznachennia daty pochatku tymchasovoi okupatsii (2015), Zakon Ukrainy vid 15 veresnia 2015 r. No. 685-VIII (2015), *Vidomosti Verkhovnoi Rady Ukrainy*, No. 46, 13 Nov. 2015, Art. 417.

33. Pro Zaiavu Verkhovnoi Rady Ukrainy "Pro vidsich zbroinii ahresii Rosiiskoi Federatsii ta podolannia yii naslidkiv" (2015), Postanova Verkhovnoi Rady Ukrainy vid 21 kvitnia 2015 r. No. 337-VIII, *Vidomosti Verkhovnoi Rady Ukrainy*, No. 22, 29 May 2015, Art. 153.

34. Pro zatverdzhennia Ukazu Prezydenta Ukrainy "Pro vvedennia voiennoho stanu v Ukraini" (2018), Zakon Ukrainy vid 26 lystopada 2018 r. No. 2630-VIII, *Ofitsiinyi visnyk Ukrainy*, No. 95, 11 Dec. 2018, Art. 3127.

35. Rohozyna, D.O. (ed.) (2004), *Voina i mir v terminakh i opredeleniyakh*, PoRoh, Moscow, Russia.

36. *Russian new generation warfare handbook* (2016), Asymmetric Warfare Group, Fort Marde, USA.

37. Seheda, S.P., Shevchuk, V.P., Hrytsiuk, V.M. and others (2017), *Bila knyha antyterorystychnoi operatsii na Skhodi Ukrainy* (2014–2016), in Rusnak I.S. (ed.), NUOU, Kyiv, Ukraine.

38. Shevchuk, V.P. and Hrytsiuk, V.M. (2016), *Separatyzm ta teroryzm – instrumenty "hibrydnoi viiny" Rosii proty Ukrainy*, *International scientific conference "Vyklyky polityky bezpeky: istoriia ta suchasnist"*, 16-18 Jun, Natsionalna akademiia Sukhoputnykh viisk imeni hetmana Petra Sahaidachnoho, Lviv, Ukraine.

39. Shtohrin, I. and Loiko, S. (2016), *Aeroport Donetsk 242. Istoriia muzhnosti, braterstva ta samopozhertvy*, Knyzhkovyi Klub "Klub Simeinoho dozvillia", Kharkov, Ukraine.

40. Smolii, V. and Yakubova, L. (2018), *Istorychnyi kontekst formuvannia proektu russkyi myr ta praktyka yoho realizatsii v Krymu y na Donbasi*, NAN Ukrainy, Instytut istorii Ukrainy, Kyiv, Ukraine.

41. Smolii, V. and Yakubova, L. (2019), *Krym i Donbas: problemy y perspektyvy intehratsii v modernyi ukrainskyi proekt NAN Ukrainy*. Instytut istorii Ukrainy, Kyiv, Ukraine.

42. *Territorial integrity of Ukraine: Resolution adopted by the General Assembly* on 27 March 2014 / 68/262 Sixty-eighth session, Agenda item 33, available at: https://www.un.org/en/ga/search/view_doc.asp?symbol=%20A/RES/68/262 (accessed 5 January 2021).

43. The white book of the anti-terrorist operation in the East of Ukraine in 2014–2016 (2017), National Defence University named after Ivan Cherniakhovskyi, Kyiv, Ukraine.

44. Ogarkov N.V (ed.) (1983), *Voennyi entsiklopedicheskiy slovar*, Voenizdat, Moscow, Russia.

45. Vylko, V. (2017), Periodyzatsiia rosiisko-ukrainskoi hibrydnoi viiny: 2014 – 2017 roky "Viina na Donbasi 2014–2016 rr.", *II Ukrainian scientific military history conference*, 20 April, National military history museum, Kyiv, Ukraine, pp. 218–222.

46. MOU (2015), *White Book-2014. Armed Forces of Ukraine*, Kyiv, Ukraine.

47. MOU (2016), *White Book-2015. Armed Forces of Ukraine*, Kyiv, Ukraine.

48. MOU (2017), *White Book-2016. Armed Forces of Ukraine*, Kyiv, Ukraine.

49. MOU (2018), *White Book-2017. Armed Forces of Ukraine*, Kyiv, Ukraine.

50. MOU (2019), W*hite Book-2018. Armed Forces of Ukraine*, Kyiv, Ukraine.

51. Yakubova, L., Holovko, V. and Prymachenko, Ya. (2018), *Russkyi myr na Donbasi ta v Krymu: istorychni vytoky, politychna tekhnolohiia, instrument ahresii*, in Smolii V. (ed.), NAN Ukrainy, Instytut istorii Ukrainy, Kyiv, Ukraine.

52. *Zbroina ahresiia Rosiiskoi Federatsii proty Ukrainy. Informatsiino-dovidkovyi material*, National Defence University named after Ivan Cherniakhovskyi, Kyiv, Ukraine.

53. Zolotukhin, D.Yu. (2018), *Bila knyha spetsialnykh informatsiinykh operatsii proty Ukrainy 2014 – 2018*. – Mininformpolityky, Kyiv.

Vasyl Shkolyarenko
Candidate of Technical Sciences, Senior Researcher
Chief of Multinational Staff Officers Training
and Research Centre of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-8274-2232

Ivan Rudnytsky
Candidate of Technical Sciences, Senior Researcher
Senior Research Fellow of Multinational Staff Officers
Training and Research Centre of the National Defence
University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-6304-3863

CIVIL-MILITARY COOPERATION OF THE ARMED FORCES OF UKRAINE IN COUNTERING THE HYBRID RUSSIAN AGGRESSION IN THE JOINT FORCES OPERATION

This research look at tasks of forces and means of civil-military cooperation (CIMIC) of the Armed Forces of Ukraine (AFU) in countering the hybrid Russian aggression against Ukraine. The aim of this report is defining priority tasks of AFU CIMIC organizational structures in the sphere of countering the hybrid Russian aggression against Ukraine in the Joint Forces (JF) operation.

To achieve this goal and solve problems, there were used generalization and analysis of personal experience of one of the authors serving in the AFU CIMIC group in the zone of anti-terrorist operation (ATO) in 2015, information and analytical materials from open and electronic (Internet) sources on practical activities of AFU CIMIC forces in the zone of ATO / Joint Forces operation (JFO) in Donetsk and Luhansk regions.

The main results of the report are recommendations to the military authorities and scientific and pedagogical communities on counteraction to the hybrid aggression of Russia against Ukraine by the forces and means of the AFU CIMIC.

Conclusions and scope. The priority tasks of the AFU CIMIC in

counteracting Russia's hybrid aggression against Ukraine are protection of civilians, creation of conditions for sustainable social and economic development of the region, building the potential of synergy of civil-military cooperation between the Joint Forces and state and local authorities, interaction with international humanitarian organizations.

Keywords: *Russian hybrid aggression against Ukraine, Joint Forces operation, counteraction, civil environment, civil-military cooperation.*

Introduction

Problem statement. Countering Russia's hybrid aggression is an integral part of ensuring Ukraine's national security. One of the areas of counteraction was the introduction of a comprehensive NATO approach to planning and conducting military operations, which involves building a system of working with the civil environment in the operation zone. This function in the Armed Forces of Ukraine is assigned to the structures of civil-military cooperation of the Armed Forces of Ukraine. Therefore, research is needed in the field of combating hybrid aggression by the forces and means of the AFU CIMIC.

The analysis of recent researches and publications. The formation of the AFU CIMIC was considered in the context of studies of the participation of the Armed Forces of Ukraine in international peacekeeping and security operations in Iraq, Bosnia and Herzegovina, Kosovo, Afghanistan, Somalia, Rwanda and Haiti.

Recently, a number of publications has appeared on the problematic issues of functioning the AFU CIMIC in Eastern Ukraine in the conditions of a hybrid war. These are, in particular, materials of scientific and practical conferences on “Actual problems of interaction between civil society and the Armed Forces of Ukraine”, “Ukrainian society in war: current challenges and prospects for peace”, separate publications by I. Shopina, I. Koropatnik, M. Ozhevan, O. Nozdrachov, O. Milchenko, P. Tkachuk, M. Seredenko and others.

Scientific achievements of the above authors, as well as the results of the analysis of the current regulatory framework of the UN,

NATO and some western countries (USA, Canada, Denmark, Sweden), domestic and foreign public administration practices of the CIMIC have allowed to resume its institutionalization in Ukraine since 2014.

However, issues related to the counteractionby the forces and means of the AFU CIMIC to the hybrid aggression of Russia against Ukraine remain unexplored.

Purpose of the report is to determine tasks of the AFU CIMICforces in the field of counteracting hybrid aggression of Russia in the JF operation zone.

Main part

The practical implementation of the CIMIC in the UAF coincided with the beginning of the Anti-Terrorist Operation in certain districts of Donetsk and Luhansk regions (CDDLR). At that point, the need for civil-military cooperation as a continuous process of supporting and supplying the military forces, establishing liaison with local authorities, partial coordination and involvement of international organizations in the most humanitarian-sensitive areas of the operation became quite obvious.

Having analyzed how the ATO tasks had been accomplished in the first month of the operation, one can see a critical situation in establishing cooperation between commanders of the UAF units, other security and defense sector components, local self-governing authorities and the local population: negative attitude of the locals to the UAF presence, hindering their movement in the operation area, self-removal of the local authorities from performing their functional duties, inability or unwillingness of the law enforcement agencies (police, territorial bodies of the SSU, and SESU units) to perform tasks assigned by their functional duties [1].

Due to this, the UAF General Staff decided to establish CIMIC groups that would purposefully build up cooperation with the civilian population and local authoritiesin the territories where Ukrainian military units were located using the experience of participating in various peacekeeping operations. The first UAF

CIMIC unit consisting of two groups began its work in the Anti-Terrorist Operation zone on May, 2014 [2].

The first CIMIC unit was assigned with three tasks:

– to organize liaison with the civil sector, law enforcement agencies and UAF units;

– to assist the civilian population (to create conditions for obtaining humanitarian aid by educational, medical and social institutions, to involve charitable public organizations in rehabilitation of victims of terrorist acts, and to restore the destroyed infrastructure);

– to assist commanders of the UAF units in accomplishing the assigned tasks.

Taking into account the experience gained by the CIMIC structures at all governance levels in the period from 2014 to 2019, we propose the following meaning of the term "civil-military cooperation": CIMIC is a set of actions carried out by the UAF and other defense forces components, synchronized on aim, objectives, location and time to liaise with local public authorities, self-governments, public associations and other legal entities and individuals in order to provide favorable conditions for military commanders, military formations and units to perform their assigned tasks using military and non-military means.

The content of the CIMIC in the UAF has national connotation in contrast to the CIMIC in international peacekeeping and security operations. The CIMIC was established according to the international experience of coordination between military units and the civilian population, in particular during peacekeeping operations under the auspices of the UN and other international security organizations. At the same time, the current situation in Ukraine has its own peculiarities which were taken into account during CIMIC development and choosing its strategic lines of action.

Ukrainian situation has the following peculiarities:

– liaison with the civilian environment is being established under conditions of strong informational influence of the aggressor state on the local population. At the same time, aggressor state

participation in the war is being firmly denied despite a number of irrefutable evidence. The other party is being accused of the aggressor's own crimes and the international humanitarian law is being ignored [3];

– no language barrier between military and civilians, common historical mentality of the parties involved, knowledge by the military of cultural features of the region, common legal field acts for the military as well as for the civilians;

– better coordination between the military and representatives of other ministries, departments at the state and regional levels;

– performing the assigned tasks by the CIMIC structures in the ATO / JFO area in the 30-50-kilometer zone along the demarcation line [4, p. 15], including within the demarcation (combat) line at the depth of company's area of responsibility, and in the "gray zone", if necessary;

– a part of the humanitarian tasks (restoration of critical infrastructure, humanitarian demining, participation in patriotic education of the civilian population) are performed by the CIMIC structures together with state structures in accordance with their functional purpose;

– no financial and material resources in the UAF CIMIC structures. Therefore, resources of international organizations, NGOs, volunteer organizations, charitable foundations, and government agencies should be actively attracted to implement CIMIC projects.

The UAF CIMIC system development. The CIMIC system means a set of interconnected entities (bodies, forces, and means) of the UAF and other military formations and civil environment entities, as well as technologies of influencing them to prepare conditions for the troops (forces) to successfully perform their tasks.

In 2014, after the liberation of certain territories of Donetsk and Luhansk regions from terrorist militants, there were settlements where local authorities were either discredited or lacking. This created preconditions for a humanitarian catastrophe. So, it was

decided to increase the number of CIMIC groups, diversify military specialties of the UAF personnel involved in the groups, expand activities to other sectors of the ATO zone and create the UAF CIMIC system according to the NATO standards with due account for the peculiarities of the Russian-Ukrainian conflict.

The CIMIC structure includes both in-service and temporarily units of the UAF CIMIC. It has been implementing in the general structure of the UAF and in the ATO areas in Donetsk and Luhansk regions since 2015 [5].

Joint CIMIC centers, CIMIC groups in brigades, and CIMIC operational groups operate at the tactical level of the CIMIC system. All CIMIC units must follow a consistent and coordinated approach to CIMIC activities and plans.

The CIMIC Directorate of the UAF was established in January 2015 in accordance with the decision of the Chief of the UAF General Staff [6]. It focused on the following lines:

– forming a conceptual basis of the UAF CIMIC activities;

– defining functions and tasks of CIMIC organizational structures;

– development of UAF CIMIC capabilities adequate to the needs of the UAF.

The regulatory framework for the UAF CIMIC activities had been elaborated in a very short time.

At the same time, efforts to develop UAF CIMIC forces and means (establishment of UAF CIMIC units, their equipping and professional training) were undertaken. CIMIC groups, CIMIC departments, CIMIC coordination groups, and UAF CIMIC Joint Centers were defined as the main structural elements of the UAF CIMIC.

Measures to join the CIMIC to international military cooperation activities (in particular, the “Partnership for Peace” program, the Plan and Review Process to achieve the objective G1105 “CIMIC Capabilities” of the Operational Capabilities Concept and the Assessment and Feedback Program) were taken.

The activity of the CIMIC structures was regulated in order

to include them into the UAF C2 system: the report forms on civilian environment assessment at all levels of military administration were elaborated, and the CIMIC units were included in the UAF strategic communications system.

The system of information support of the UAF CIMIC was being improved. A "Civil-Military Cooperation" group has been created on Facebook, where the results of the work of the CIMIC groups in the ATO zone (photos, articles, and videos) are periodically presented. Liaisons with Ukrainian NGOs and volunteer organizations were established in order to coordinate their assistance to UAF servicemen and military units [7].

The CIMIC units expanded the field of their functional activities. Based on the order of the Cabinet of Ministers of Ukraine "On the Measures to Immortalize the Memory of the Defenders of Ukraine until 2020", the CIMIC was tasked with finding and exhuming the bodies of the dead servicemen of the UAF, law enforcement agencies and other military formations within the framework of the humanitarian project "Evacuation 200" [8]. From September 3, 2014 to December 2019, CIMIC search teams evacuated 1791 bodies (remains) of the dead servicemen of the UAF, law enforcement agencies and other military formations from the ATO area (including 262 from the temporarily uncontrolled territory) [9]. In this regard, the UAF CIMIC Directorate has established cooperation and is continuously working with the International Committee of the Red Cross in Ukraine.

Information and psychological support of families of servicemen who went missing (died) during the ATO (combat operations) is carried out on the basis of the directive of the UAF GS No. D-8 of February 22, 2016 "On the Organization of Work with Families of Missing (Killed) Servicemen of the Armed Forces of Ukraine" [10].

An important area of improving the CIMIC organizational structure as a component of the security and defense sector is to bring the UAF CIMIC system to NATO type *J*-structures within the transformation of military administration bodies. This will allow the

CIMIC system to gain additional capabilities in promoting democratic civilian control and legal regime of martial law. The CIMIC influence has been expanded due to the organization of CIMIC groups within the National Guard of Ukraine and the State Border Guard Service of Ukraine [11].

Activities of the CIMIC units in the ATO / JFO zone. After reaching the Minsk Agreements [12], the events in the East of Ukraine became less intense, the struggle moved to softer methods of waging the undeclared war. This means that the conflict in the East of Ukraine is not a classical military confrontation. There is a struggle to form a pro-Ukrainian worldview of the residents of Donbas in which the CIMIC groups are in a leading position. Therefore, the activities of the UAF CIMIC in the area of accomplishing measures on ensuring national security and defense, repulse and deter the armed aggression in the Donetsk and Luhansk regions have some peculiarities due to the organization of interaction with defense forces components and civilian environment under the hybrid aggression.

The key task of opponents in a hybrid war is to turn the civilian population to their side. A striking example of this is the "humanitarian convoys" and the "compulsory passportization of Ukraine citizens" by the Russian Federation in the temporarily occupied territories of the certain districts of Donetsk and Luhansk regions (CDDLR). The first step towards neutralizing this action was the instruction of the President of Ukraine to develop a program that will motivate young people from the occupied territories to keep Ukrainian citizenship [13]. The CIMIC structural units efforts in conducting socially oriented projects to counteract the adverse informational influence of Russian propaganda and their participation in information operations deserve special attention.

Under the conditions of countering the hybrid aggression, UAF CIMIC activities started to change in 2018, after the Law of Ukraine "On the Peculiarities of the State Policy to Ensure Ukraine's State Sovereignty in the Temporarily Occupied Territories in Donetsk and Luhansk Regions" [14] had been adopted and the JFO

had been launched. The transition to measures to ensure national security and defense, repulse and deter armed aggression of the Russian Federation required changes in the UAF CIMIC policy. In particular, protecting civilians is the top priority of the Joint Forces Command in the humanitarian sphere during the military operation in the East of Ukraine.

This requires to form new lines of UAF CIMIC activities in countering hybrid aggression. To this end, a system for preventing casualties [15] among the civilian population has been established, efforts in national-patriotic education, mine awareness and restoration of regional critical infrastructure have been intensified, and the humanitarian "Aid East" initiative has been launched in 2018.

Infrastructure restoration is an important line of operationsfor CIMIC. UAF CIMIC groups helped organize restoration of gas supply in Maryinsky district, electricity supply in Krasnohorivka, duplication of the electrical line from Maryinka to Novomykolayivka and many other important projects to restore vital infrastructure [1].

A humanitarian initiative of the Joint Forces Command "Help East" was recognized as an important component of the Joint Forces' activities. It is a multidisciplinary multifaceted program of targeted actions to help Donbas civilians. UAH 5.8 million assistance to medical and social protection establishments has been provided under this project. The number of measures to restore housings, critical infrastructure and social facilities in the areas adjacent to the contact line in Donetsk and Luhansk regions is growing.

The UAF CIMIC groups are tasked with coordinating demining activities in the territories liberated from the terrorists. Since the beginning of the armed conflict in Donbas, sappers found and neutralized 253,716 explosive devices with the coordination assistance of the CIMIC. Demining teams cleared about 4,030 hectares of land and 1,356 kilometers of roads. Today there are about 40 demining groups in the JFO area. Generally, UAF representatives perform tasks on the first line of defense, SESU sappers work on the second and third lines, and the State Special Transport Service is

engaged in demining railway tracks. Representatives of the Armed Forces of Ukraine are also involved in the humanitarian demining of the Donbas territory [16].

In addition to the UAF and SESU units, international and/or non-governmental organizations may be involved in demining activities. In particular, the HALO Trust, the Danish Demining Group (DDG) and the "Fondation Suisse de Déminage"(FSD) as well as national non-governmental operators "Demining Solutions" and "Demining Team from Ukraine" were involved in the JFO. This implies that CIMIC officials (mainly from the CIMIC Joint Center) were actively involved in coordination of these activities.

The CIMIC has been entrusted with some tasks (related to the principles and norms of international human rights and international humanitarian law concerning civilians) which cannot be solved by its forces and means alone. Such tasks require a comprehensive interagency approach and are entrusted to various military units (services), public authorities, government structures, international and/or non-governmental organizations, etc. These tasks, aimed at protecting victims of the armed conflict, include:

– protection of civilians;

– protection of women during armed conflicts and in post-conflict periods;

– protection of children during armed conflicts;

– protection of the cultural heritage [4, p. 119].

Liaisons with educational establishments and participation in military-patriotic education of children and youth, participation in providing certain administrative services to local people may be additional tasks of the CIMIC Joint Center.

Military-patriotic education of youth and local population means participation in arranging lessons of courage and measures for military-patriotic education of youth in a spirit of readiness to defend their homeland.

The UAF CIMIC worked out guidelines[4, p. 37] on civilian environment monitoring and analysis. Such NATO methods as passport of the settlement, PMESII-PT-analysis, ASCOPE-analysis,

ASCOPE-3D-analysis, SWOT-analysis, PMESII-ASCOPE-analysis, link analysis, PMESII-SWOT-analysis, ASCOPE-SWOT-analysis, PMESII-ASCOPE-SWOT-analysis, and civilian environment express assessment have been adapted to the needs of the UAF CIMIC. The attitude of the civilian population towards the UAF is assessed according to "threatening – unfavorable – favorable" scale.

CIMIC servicemen work both in the "gray zone" and along the contact line. Besides, CIMIC groups are making considerable efforts to release Ukrainian servicemen from captivity.

Liaisons with international and/or non-governmental organizations operating in the East of Ukraine have been strengthened. The interests of these organizations include functions of controlling ceasefire, monitoring of respecting human rights, supporting internally displaced persons (IDPs) from the occupied territories, and providing humanitarian aid.

The UAF CIMIC Directorate deals with problems of IDPs in the closest cooperation with the UN Office of the High Commissioner for Refugees. The Office of the UN High Commissioner for Human Rights has focused its activities in Ukraine on documenting human rights violations during the military conflict in Donbas and handing them over to the International Criminal Court. Cooperation with the International Committee of the Red Cross has begun as early as in 2014 in the formsof first aid exercises and direct assistance to civilians. As the next step, the Memorandum of Cooperation and Mutual Understanding was signed in 2017. And representatives of the Red Cross practiced a deployment of a transit camp for evacuees as part of joint exercises already in 2018.

The international NGO "Center for Civilians in Conflict" (CIVIC Center) is implementing "Building Capabilities to Protect Civilians in the East of Ukraine" project [17]. It helps establish and implement a system of collecting and analyzing information about the hostility damage to civilians, train servicemen in preventing civilian casualties and promote formation of state policy on protecting civilians in the conflict. It was also agreed that the Ukrainian side would be able to study the world practices in

development and implementation of systems and processes to protect civilians in operations under conflict conditions according to NATO standards as well as adopted in international peacekeeping missions.

Conclusions

Ukraine is countering Russian hybrid aggression through a set of measures covering all spheres of national life. The UAF civil-military cooperation system created according to NATO standards is one of the entities that counter the aggression.

The main tool for countering the hybrid aggression is arrangement of interaction between the UAF CIMIC structures (and other defense forces components) and the civilian environment in the area were measures on ensuring national security and defense, repulse and deterrence of the armed aggression in Donetsk and Luhansk regions are being performed. To achieve this, coordination groups, search teams, CIMIC groups and joint CIMIC centers work in the JFO zone.

The UAF CIMIC conducts the most effective activities in the military, information and humanitarian spheres.

The UAF CIMIC military forces monitor the civilian environment in the operation area, assess the attitude of the civilian population to the UAF. The CIMIC forces are also tasked with finding and exhuming the bodies of the dead servicemen of the UAF, law enforcement agencies and other military formations within the framework of the humanitarian project “Evacuation 200”. Information and psychological support of families of servicemen who went missing (died) during the ATO (combat operations) is carried out.

The UAF CIMIC forces are involved in strategic communication activities, organize communication with the media, participate in socially oriented projects to counter adverse information influence of Russian propaganda and information operations, and maintain a “Civil-Military Cooperation” page on Facebook.

The JFO Command humanitarian priorities are: protecting

civilians, creating conditions for sustainable social and economic development of the region, building the potential of civil-military cooperation between the Joint Forces, state and local authorities, and interacting with international humanitarian organizations. These objectives are being achieved through the implementation of "Help East" project, which is a multidisciplinary and multifaceted program of targeted actions to help civilians in Donetsk and Luhansk regions.

The UAF CIMIC groups are tasked with coordinating activities of public authorities, special law enforcement agencies, international humanitarian organizations in the field of mine awareness, delivery of humanitarian goods, and restoration of critical infrastructure (power grids, gas pipelines, water supply systems, and housing repairs).

Interaction between the CIMIC groups and international organizations working in the East of Ukraine helps protect the civilian population. These organizations perform functions on controlling ceasefire, monitoring respect for human rights, supporting IDPs from the occupied territories, humanitarian aid, and monitoring compliance with international humanitarian law. The Office of the UN High Commissioner for Refugees, the International Committee of the Red Cross, and the "International Center for Civilians in Conflict" (CIVIC) are the most influential among these organizations.

References

1. Nozdrachov, O.O. (2015), "*Osoblyvosti diyal'nosti grup tsyvil'no-viyskovogo spivrobitnytsva Zbroynykh Syl Ukrayiny*" [*Features of activity of groups of civil-military cooperation of the Armed Forces of Ukraine*] in red. O.L. Karaman, S.O. Vovk and I.M. Shopina, DZ "LNU im. Tarasa Shevchenka, Starobilsk, 64 p.

2. The official site of the Cabinet of Ministers of Ukraine (2014), "*V zoni ATO rozpocyaly roboty operatyvni grupy tsyvil'no-viyskovogo spivrobitnytsva Zbroynykh Syl Ukrayiny*" [*Operational groups of military-civil cooperation of the Armed Forces of Ukraine have started working in the anti-terrorist operation zone*], available at: https://cutt.ly/4j8tdtD (accessed 16 October 2020).

3. Bill (2019), "*Ob otzyve zalavlenija, sdelannogo pri patyfikaziyi Dopolnitel'nogo protokola k Zhenevskym konvenziyam ot*

12 avgusta 1949 goda, kasajushchevosya zashchity zhertv mezhdunarodnykh vooruzhennykh konfliktov (Protokol I) No. 815671-7 vid 17.10.2019" [*Withdrawal of the declaration made upon the ratification of the Protocol Additional to the Geneva Conventions of August 12, 1949, concerning the protection of victims of international armed conflicts (Protocol I) No. 815671-7 dated 17.10.2019*], available at: https://sozd.duma.gov.ru/bill/815671-7 (accessed 16 August 2020).

4. Nozdrachov, O. (2019), "*Metodychnyy zbirnyk dlja viys'k (syl) z pytan' tsyvil'no-viyskovogo spivrobitnytsva*" [*Methodical manual for troops (forces) on civil-military cooperation*], Department of Civil-Military Cooperation of the Armed Forces of Ukraine, Kyiv, 167 p.

5. Order of the General Staff of the Armed Forces of Ukraine (2018), "*Polozhennja pro strukturu tsyvil'no-viyskovogo spivrobitnytsva Zbroynykh Syl Ukrayiny No. 470 vid 29.12.2018"* [*Regulations on the structure of civil-military cooperation of the Armed Forces of Ukraine No. 470 dated 29.12.2018*].

6. Order of the General Staff of the Armed Forces of Ukraine (2015), "*Polozhennja pro Upravlinnya tsyvil'no-viyskovogo spivrobitnytsva Zbroynykh Syl Ukrayiny No. 34 vid 03.02.2015"* [*Regulations on the Department of Civil-Military Cooperation of the Armed Forces of Ukraine No. 34 dated 03.02.2015*].

7. Facebook (2020), *"Tsyvil'no-viyskove spivrobitnytsvo Zbroynykh Syl Ukrayiny*" [*Civil-military cooperation of the Armed Forces of Ukraine*], available at: https://www.facebook.com/cimicUA/ (accessed 14 October 2020).

8. Order of the Cabinet of Ministers of Ukraine (2015) "*Pro zakhody z uvichnennya pamyati zakhysnykiv Ukrayiny na period do 2020 roku No. 998-r vid 23.09.2015*" [*On measures to perpetuate the memory of the defenders of Ukraine for the period up to 2020 No. 998-r dated 23.09.2015*], available at: https://cutt.ly/Qj8tMCB (accessed 14 October 2020).

9. The official site of The Ministry of Defense of Ukraine (2019), "*Za 5 rokiv poshukovymy hrupamy "EVAKUATSIYA 200" vyvezeno z rayonu boyovykh diy 1787 til zahyblykh*" [*For 5 years search groups "EVACUATION 200" took out of the area of hostilities 1787 bodies of victims*], available at: https://cutt.ly/3j8yrPw (accessed 14 October 2020).

10. Directive of the General Staff of the Armed Forces of Ukraine (2016) "*Pro organizastiyu roboty z simyamy viyskovosluzhbovstyamy Zbroynykh Syl Ukrayiny, jaki znykly bezvisty (zagynuly) No. D-8 vid 22.02.2016*" [*About the organization of work with families of servicemen of the Armed Forces of Ukraine who disappeared (No. D-8 dated 22.02.2016)*].

11. The Resolution of the Cabinet of Ministers of Ukraine (2019), "*Pro zatverdzhennya Poryadku v'yizdu osib, peremishchennya tovariv na*

tymchasovo okupovani terytoriyi u Donets'kiy ta Luhans'kiy oblastyakh i vyyizdu osib, peremishchennya tovariv z takykh terytoriy No. 815 vid 17.07.2019" [*On approval of the Procedure for entry of persons, movement of goods to the temporarily occupied territories in Donetsk and Luhansk regions and departure of persons, movement of goods from such territories No. 815 dated 17.07.2019*], available at: https://cutt.ly/0j8ybNv (accessed 14 October 2020).

12. Security Council United Nations (2015), *Resolution 2202 No. S/RES/2202 dated 17.02.2015*, available at: https://cutt.ly/jj8yXU5 (accessed 14 October 2020).

13. The official site of UNN UA (2020), "*Zelens'kyy vymagaye rozrobyty spestprogramu protystoyannya rosiys'kiy pasportyzatsiyi na Donbasi"* [*Zelensky demands to develop a special program to oppose Russian passportization in Donbass*], available at: https://cutt.ly/2j8uqZb (accessed 18 October 2020).

14. The Law of Ukraine (2018), "*Pro osoblyvosti derzhavnoyi polityky iz zabezpechennya derzhavnogo suverenitetu Ukrayiny na tymchasovo okypovanykh terytoriyakh u Donest'kiy i Lugans'kiy oblastyakh No. 2268-VIII vid 18.01.2018*" [*On the peculiarities of the state policy to ensure the state sovereignty of Ukraine in the temporarily occupied territories in Donetsk and Luhansk regions No. 2268-VIII dated 18.01.2018*], available at: https://cutt.ly/uj8ugKJ (accessed 18 October 2020).

15. Order of the General Staff of the Armed Forces of Ukraine (2018), "*Pro utvorennya robochoyi grupy iz zboru ta uzagal'nennya informastiyi pro vypadky poranennya I zagybeli styvil'nogo naselennya No. 851 vid 29.12.2018*" [*On the establishment of a working group to collect and summarize information on cases of injuries and deaths of civilians No. 851 dated 29.12.2018*].

16. The official site of Radio Svoboda (2018), "*Ministersvo oborony rozpovilo, skil'ky vybukhonebezpechnykh predmetiv zntshkodyly z pochatku konfliktu na Donbasi*" [*The Ministry of Defense told how many explosive objects neutralized since the beginning of the conflict in Donbass*], available at: https://cutt.ly/wj8uLXa (accessed 17 October 2020).

17. The official site of The Ministry of Defense of Ukraine (2018), "*Priorytetamy Komanduvannya Obyednanykh sil u gumanitarniy sferi pry provedenni viys'kovoyi na Skhodi Ukrayiny ye zakhyst styvil'nogo naselennya*" [*The priorities of the Joint Forces Command in the humanitarian sphere during the military operation in eastern Ukraine are the protection of the civilian population*], available at: https://cutt.ly/1j8iCcU (accessed 25 October 2020).

Petro Snitsarenko
Doctor of Technical Sciences, Senior Scientific Researcher
Leading Scientific Researcher of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-6525-7064

Yurii Sarychev
PhD (Technical Sciences), Senior Scientific Researcher
Leading Scientific Researcher of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-1380-4959

Volodymyr Tkachenko
PhD (Military Sciences)
Chief of Department of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-9625-2434

Vitalii Hrytsiuk
Postgraduate Student of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-3146-1956

Liudmyla Khomenko
Scientific Researcher of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-4860-9571

INFORMMATION SECURITY IN THE COURSE OF COUNTERACTING HYBRID AGGRESSION

The publication is devoted to outlining a general approach to understanding the theoretical foundations of information security of the state, in particular in the military sphere. Legislative axiomatics is given as a basis for theoretical provisions of information security of Ukraine, including its components - cybersecurity (cyber defense), state communications. In the course of research such methods as analysis,

system approach, axiomatic approach, logical approach, comparison, generalization were used. The implementation of these research results will allow to respond most adequately to "hybrid" threats of an informational nature, including in cyberspace.

Keywords: *"hybrid" aggression, military sphere, information security of the state, cybersecurity, cyber defense, state communications.*

Introduction

Problem statement. One of the main conclusions of Russia's "hybrid" war with Ukraine is the conclusion that the role of its information component has multiplied. The consequence of this is the need for immediate and priority building of the relevant capabilities of the Defense Forces of Ukraine to strengthen the information security of the state in the military sphere in all its components. A significant part of the necessary measures for this is provided by the legislation of Ukraine. In this regard, the Ministry of Defense of Ukraine is tasked with countering special information operations directed against the Armed Forces of Ukraine and other military formations (Doctrine of Information Security of Ukraine, 2017 [1]). In addition, it is responsible for repelling military aggression in cyberspace (cyberdefense), military cooperation with NATO and other defense actors to ensure the security of cyberspace and joint protection against cyberthreats (Cybersecurity Strategy of Ukraine [2], Law of Ukraine "On the basic principles of cybersecurity in Ukraine" [3]). The implementation of these tasks is detailed in the relevant regulatory and planning documents of the national and departmental level.

At the same time, despite the ongoing organizational and executive measures, countering aggressive information actions by Russia, as an integral part of the ways to wage a "hybrid" war with Ukraine, must become more effective. The main condition for this should be the presence of a developed theoretical basis for information security of the state, in particular in the military sphere. However, there is no stable theory on this issue today. This unfortunate situation is a problem that needs to be addressed immediately.

The analysis of resent researches and publications. The current state of the problem of information security, in particular in Ukraine, is characterized by active attempts to develop appropriate theoretical foundations. This is evidenced by numerous publications in scientific journals. Among domestic scientists and specialists this problem is paid attention to in the works of O. Yudin, V. Bogush, V. Gorbulin, M. Bychenok, V. Petryk, V. Ostroukhov, M. Prysyazhnyuk, V. Tolubko, I. Rusnak, V. Telelym [4–8] and others. These works cover the socio-legal aspects of information security, the protection of the information space of Ukraine, provide a number of definitions in this subject area. And in the military sphere the peculiarities of ensuring the information security of the state in the context of counteracting information wars are outlined or the evolution of forms and methods of modern information struggle is described.

At the same time, despite the significant number of professional publications, the issue of information security of the state, in particular, in the military sphere, at the system level in Ukraine is still not properly addressed. There is no common understanding of the basic terminological categories of this subject area. This is detrimental to the creation of an adequate regulatory framework, which negatively affects both theoretical generalizations and practical actions. In this regard, the basic element of counteracting the "hybrid" aggression of Russia against Ukraine today is the task of counteracting information aggression. In turn, this complex task requires a systematic understanding of the theoretical foundations of information security of the state, including its components – cybersecurity, including cyber defense, strategic communications, etc., primarily in the military sphere.

The first attempts to consider the topic of information security of the state from the standpoint of a systematic approach were made in the works of P. Snitsarenko and co-authorship [9–11], including in the military sphere. In these works it is determined that ensuring the information security of the state, in particular in the military sphere, is a systemic problem that needs to be solved in a

complex, without separating one component from another.

Thus, the question of determining the essence of information security of the state, in particular in the military sphere, including the role and place of cybersecurity (cyberdefense), strategic communications, etc. in modern conditions of counteracting "hybrid" aggression, remains insufficiently covered, therefore, it is relevant for research.

Purpose of the report. The purpose of the publication is to determine from the standpoint of a systematic approach to the essence of information security of the state, in particular in the military sphere, as well as cybersecurity (cyberdefense), strategic communications, etc. in modern conditions of "hybrid" aggression.

Main part

A provision from Article 17 of the Constitution of Ukraine states: "…to ensure [Ukrainian] economic and informational security are the most important functions of the State and a matter of concern for all the Ukrainian people." This provision is fundamental to ensuring information security of Ukraine in any sphere of life, including in the military domain. Note that that this requirement is placed on a par with the protection of Ukraine's sovereignty and territorial integrity and ensuring state economic security, which means the highest state priority. Moreover, the Constitution of Ukraine does not mention anything else regarding the information sphere. Therefore, this provision regarding Ukrainian information sphere should be considered and perceived as the *first and key legislative axiom.*

Considering the first legislative axiom for the information sphere of Ukraine, there must be a legislative understanding (interpretation) of the essence of state information security. It should be emphasized that the Ukrainian legislative field does not contain a framework law on the state information security. However, the legislation defines the essence of information security in the "body" of the non-framework Law of Ukraine "On Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007 – 2015" in this edition.

Information security shall be the state of security for vitally important interests of the individual, the society and the state which shall prevent the causing of damages through:

– incomplete, untimely and unauthentic information that is being used;

– negative information impact;

– negative consequences of using information technologies;

– unauthorized dissemination and utilization of information, as well as the breach of integrity, confidentiality, accessibility, and availability of information.

There is no other interpretation, denial or clarification of information security in other legislative acts of Ukraine which relate to the information sphere and came into force after this law. Therefore, it can be perceived as the *next (second) legislative axiom* for the Ukrainian information sphere despite some minor inconsistencies in its definition.

This second legislative axiom details the first constitutional axiom and corresponds to the systematic approach principle. This legislative wording concerning the essence of information security may be further clarified (at least, the damage may be caused by both "untimely" and "absent" information, i.e., information which is impossible of obtain in an urgent need), but in general, the wording is quite clear, generalized and balanced.

The second axiom carries a number of fundamental corollaries.

Corollary 1 of the second axiom. Cybersecurity is information security in the digital information resources domain. Therefore, the artificial (administrative) separation of information security and cybersecurity contradicts the Constitution of Ukraine and logic of all information processes, violates the notional principle of systematicity (the state or quality of being systematic), and, therefore, cannot be accepted in both theory and practice. Unfortunately, this systematic methodological error exists in international and national regulations. This negatively impacts, in particular, the development of national information legislation with further distortion of cybersecurity theory

and practice. This methodological error shall be corrected.

Corollary 2 of the second axiom. Threats to Ukrainian information security (regardless of their origin and form of implementation: information aggression, intentional manipulative and criminal information actions, mechanical destruction, information incapacity, unprofessional actions or official inaction) are becoming obvious. If materialized, they may harm a person, the society or the state. That is, these are such threats:

– incomplete, untimely and unauthentic information that is being used;

– negative information impact;

– negative consequences of using information technologies;

– unauthorized dissemination and utilization of information, as well as the breach of integrity, confidentiality, accessibility, and availability of information.

Note that the National Security Strategy of Ukraine as of the end of 2019 states otherwise. Paragraph 3.6 defines the following threats to information security:

– information warfare against Ukraine;

– no state communication policy;

– insufficient level of media culture of the society.

This does not correspond to the above-mentioned legislative definition of the essence of information security (i.e., axiom 2 and its corollary) and violates the systematic approach principle. Such a strategic narrative can only supplement the above list of threats with the exception of the "information warfare" item as politicized and non-specific in terms of information component itself.

Corollary 3 of the second axiom. Ensuring Ukrainian information security (including in the cyberspace, because the cyberspace is an integral part of the entire information domain) is also a very obvious process (as countering unprofitability) and stipulates implementation of preventive measures against harm due to the following factors:

– incomplete, untimely and unauthentic information that is being used;

– negative information impact;

– negative consequences of using information technologies;

– unauthorized dissemination and utilization of information, as well as the breach of integrity, confidentiality, and availability of information.

The situation is complicated by additional factors:

– absence of a state communication policy;

– insufficient level of media culture of the society.

The strategic nature of such precautionary measures has been highlighted in the same Law of Ukraine "On Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007 – 2015", which defines the way of solving the information security problem. Let us define the *third legislative axiom* based on this provision.

Information security in Ukraine (solving the information security problem) shall be ensured through:

– establishment of a fully functional state information infrastructure and ensuring protection of its critical elements;

– improving state bodies' coordination in identifying, assessing and predicting information security threats, preventing such threats, ensuring recovery, and international cooperation on these matters;

– improving the regulatory framework on ensuring information security, including protection of information resources, countering negative information impact and computer crime, protection of personal data as well as law enforcement activities in the information sphere.

These provisions should also be supplemented with the following: development of a system of state communications: strategic, governmental, and crisis (as a condition for introduction of a mechanism for successful implementation of a holistic state communication policy to neutralize one of the current information security threats).

In our opinion, the above legislative axioms and their corollaries establish the fundamentals underpinning any activity aimed at ensuring Ukrainian information security, in particular, in

the cyberspace. First of all, it is about laying the theoretical foundations of this constitutional direction of activity as a guarantee of taking adequate practical measures and the establishment of an effective nation-wide system and its components, in particular a military component. This requirement is extremely relevant in the context of the current resistance to Russian information aggression as a basic factor of a hybrid war against Ukraine.

Currently, Ukraine's defense forces are holding back the main burden of Russian aggression in the hybrid war against Ukraine, so it is important to consider information security in the military sphere, relying on the above axiomatics.

Conclusions

1. The lack of a stable theory to ensure the information security of the state, including in the military sphere, harms the creation of an adequate regulatory framework, which negatively affects the practical actions. Therefore, the priority task to combat aggressive information influence is the need for a systematic understanding of the theoretical foundations of information security of the state.

Counteracting the aggressive information influence of Russia, as an integral part of the ways of waging a “hybrid” war with Ukraine, can become more effective if there is a developed theoretical basis for information security of the state, in particular in the military sphere.

2. Legislative axiomatics, as well as its obvious consequences, should lay the foundation for any activity aimed at ensuring information security of Ukraine, including in cyberspace, in particular in the military sphere. First of all, it concerns the formation of the theoretical foundations of this constitutional direction of activity as a guarantee of adequate practical measures.

3. In accordance with the provisions of the legislation of Ukraine and the developed theory, the solution to the problem of information security of the state, which will respond most adequately to “hybrid” threats of information nature (including in cyberspace),

should be:

– creation of a fully functional information infrastructure of the state and ensuring the protection of its critical elements;

– increasing the level of coordination of the activities of state bodies in identifying, assessing and forecasting threats to information security, preventing such threats and ensuring the elimination of their consequences, the implementation of international cooperation on these issues;

– improvement of the regulatory framework for information security, including protection of information resources, counteraction to negative information influence and computer crime, protection of personal data, as well as law enforcement activities in the information sphere;

– development of the system of state communications – strategic, governmental, crisis as a condition for the implementation of a holistic communication policy of the state.

References

1. President of Ukraine (2017), *A decree of President of Ukraine is "Doctrine of informative safety of Ukraine*, available at: https://cutt.ly/Sj1ueUW (accessed 11.09.2017).

2. President of Ukraine (2016), *A decree of President of Ukraine is "Strategy of ciber safety of Ukraine*, available at: https://cutt.ly/nj1upsk (accessed 11.09.2017).

3. Verkhovna Rada of Ukraine (2017), A law of Ukraine is "On the basic principles of cybersecurity in Ukraine, available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (accessed 11.09.2017).

4. Yudin, O.K. and Bogush, V.M. (2005), "*Informatsiyna bezpeka derzhavy*" [*Information security of the state*], Konsum, Kharkiv, 432 p.

5. Gorbulin, V.P. and Bychenok, M.M. (2009), "*Problemy zakhystu informatsiynoho prostoru Ukrayiny*" [*Problems of protection of information space of Ukraine*], Institute of National Problems Security, Kyiv.

6. Petryk, V.M., Ostrouchov, V.V. and Prysyazhnyuk, M.M. (2010), "*Informatsiyna bezpeka (sotsialno-pravovi aspekty)*" [*Information security (socio-legal aspects)*], KNT, Kyiv, 776 p.

7. Tolubko, V.B. (2004), "*Informatsiyna bezpeka derzhavy u konteksti protydiyi informatsiynym viynam"* [*Information security of the*

state in the context of counteracting information wars], NUOU, Kyiv, 315 p.

8. Rusnak, I.S. and Telelym, V.M. (2000), "Rozvytok form i sposobiv informatsiynoyi borotby na suchasnomu etapi" [Development of forms and methods of information struggle at the present stage], *Nauka i oborona*, Vol. 2, pp. 18–23.

9. Snitsarenko, P.M. and Veshchitskiy, I.V. (2009), "Wytoky i sutnist informatsiynoji bezpeky Ukrajiny u woienniy spheri ta problemni pytannia jiji zabezpetchennia" [Sources and essence of information safety of Ukraine in a military sphere and problem questions of its providing], *Natsionalna bezpeka: ukrajinsky vymir*, Vol. 5(24), pp. 23–33.

10. Aleshchenko, V.I., Snitsarenko, P.M. and Klyvets, V.V. (2011), "Osnovni umovy efektyvnoho derzhavnoho upravlinnia protsesom zabezpetchennia informatsiynoji bezpeky Ukrajiny u woienniy sphere" [Basic terms of effective state administration of providing of informative safety of Ukraine a process are in a military sphere], *Stratehichni prioritety*, Vol. 4(21), pp. 18–28.

11. Snitsarenko, P.M. (2012), "Orhanizatsiyni osnovy derzhavnoyi systemy zabezpechennya informatsiynoyi bezpeky Ukrayiny u voyenniy sferi" [Organizational bases of the state system of information security of Ukraine in the military sphere], *Informatsiyna bezpeka lyudyny, suspilstva, derzhavy*, Vol. 2 (9), pp. 46–52.

12. Verkhovna Rada of Ukraine (2011), *A law of Ukraine is "About Basic principles of development of informative society in Ukraine on 2007-2015 years*, available at: https://cutt.ly/Pj1ujWm (accessed 11.09.2017).

13. President of Ukraine (2015), *A decree of President of Ukraine is "Strategy of national safety of Ukraine*, available at: https://cutt.ly/Ej1uWXq (accessed 11.09.2017).

Ariadna Sorokivska-Obikhod
Postgraduate Student
of the Hetman Petro Sahaidachnyi National Army Academy
Lviv, Ukraine
https://orcid.org/0000-0002-4413-9480

THE FEATURES OF INFORMATION OPERATIONS COMMITED DURING THE RUSSIAN-GEORGIAN WAR IN AUGUST 2008

The report analyzes practical examples of information operations conducted by the Russian Federation during the Russian-Georgian military conflict in August 2008. The purpose is to cover the main components of information operations (computer network operations, electronic warfare, military deception, operational security, psychological operations) in order to support the kinetic operations of the parties during the conflict. It is possible to draw conclusions about careful information preparation of the Russian Federation for war, active carrying out of multifaceted anti-Georgian information "throw-ins", its struggle for control of information space for reception of geopolitical advantages.

Keywords: *Russian-Georgian war of August 2008, information operations, Russian aggression, post-Soviet space, geopolitics, hybrid war.*

Introduction

Problem statement. The main goal of the Russian Federation is military-political dominance in the post-Soviet space, which is achieved through the using of the "concept of a strong state" in foreign policy towards Georgia, which is implemented through the creation of "buffer zones" and "zones of instability"; redistribution of influence spheres; splitting existing and preventing the creation of new unions. In August 2008, regular military units of the Russian Armed Forces invaded Georgia, carrying out an act of aggression in accordance with international law.

The analysis of recent researches and publications. To the Russian-Georgian August 2008 war topic are devoted the following

works: A. Cohen & R. Hamilton [1] "The Russian Military and the Georgia War: Lessons and Implications", P. Shakarian [2] "The 2008 Russian Cyber Campaign Against Georgia", T. Thomas [3] "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia", R. McDermott [4] "Russia's Conventional Armed Forces and the Georgian War", A. Nicolle [5] "Russia's Rapid Reaction: But Short War Shows Lack of Modern Systems", S. Cornell, N. Nilsson, J. Popjanevski [6] "Russian's War in Georgia: Causes and Implications for Georgia and the World", E. Lucas [7] "The New Cold War: Putin's Russia and the Threat to the West", J. Rogoza [8] "Russian Propaganda War: Media as a Long - and Short-range Weapon", D. Hollis [9] "Cyberwar Case Study: Georgia 2008".

Purpose of the report is to analyze the information support of the Russia's invasion into Georgia in August 2008 and to reveal each component of information operations.

Main part

Tensions between Russia and Georgia began long before the 2008 Russian-Georgian war. The motivating factor was the election of pro-Western President Mikhail Saakashvili in 2004, under whose leadership Georgia applied to join NATO. Although the South Ossetia is located on Georgian territory, it is ruled by Russian-backed separatists whose main goal is to split Georgia and establish Russian control over the strategically important South Caucasus [1].

Even before the official start of the conflict on August 8, 2008, began the information struggle for who, when and how started the war. The conflict was initiated by the Russian Federation, which managed to gain a partial advantage through the use of more resources. The international community has condemned Russia for its aggression against Georgia, but part of the responsibility for the start of hostilities lies with the then Georgian government. During the war, both sides used tactics that included the main components of information operations (computer network operations, electronic warfare, military deception, operational security, psychological operations).

Computer network operations. The Russian-Georgian war of 2008 is a particularly interesting example of computer network operations. Some of the events that have taken place give a unique insight into Russia's strategic and tactical operations, and show security vulnerabilities and initiatives to protect computer networks.

On August 7, at the same time as units of the Russian Armed Forces crossing the border, a cyber attack (which had Russia's trace) was carried out against Georgia. Several Georgian servers and Internet traffic were seized and relocated. On July 20, a first cyber attack was carried out, blocking President Saakashvili's website for 24 hours [10].

Russia's actions in cyberspace continued during the following days of the war and became the first large-scale coordinated cyber attack to take place in parallel with a conventional military offensive. The targets of the cyber attack were the websites of the government, financial, business institutions and the Georgian media. The main purpose of the cyber attack was to support the Russian invasion into Georgia. The Georgian government's ability to resist Russian invasion was thwarted; communication between the government and the public has deteriorated; many payments and financial transactions have been suspended; there was confusion about the development of the situation; the Georgian government's efforts to disseminate information about the invasion were thwarted; the government was deprived of many sources of information; it became more difficult to inform the outside world about what was happening, reducing the chances of receiving outside help [2].

Russian cyber-attacks have been carefully prepared in advance. This is described in a report on developments published by the US-CCU. In particular, it was noted that during the cyber-attacks no stage of reconnaissance or mapping was envisaged, and means were used directly to disrupt the work of websites, which indicates the previous training [9].

Attacks of the "first phase" of the DDOS attack (distributed denial of service) were carried out by botnets and were aimed at news and government websites. This strategy of coordination

allowed Russia to effectively block the lines of communication between the Georgian government and the population, deprived of the ability to communicate within the country and with the outside world during hostilities [2]. This continued throughout the period of the Russian offensive. After the introduction of Russian troops into Georgia, the "second phase" began, with attacks targeting a number of government, educational, financial, and media sites.

In response, the Georgian side moved websites to the "blogosphere" under the shield google.com, and also used the website of the President of Poland, which allowed to manage the work of websites and helped to communicate with the outside world. Cyber-attacks were conducted at 30-minute intervals, beginning at about 5:15 p.m. on August 8 and ending at about 12:45 a.m. on August 11, when Russia announced a ceasefire.

Electronic warfare. It is worth noting the inconsistency of standards, imperfection and inefficiency of Russia's electronic warfare during hostilities. It involves the use of electromagnetic and directed energy to control the electromagnetic spectrum or enemy attack and includes three main components: electronic attack, electronic protection and electronic warfare support. The weakness of Russian units has been electronic protection, which creates the safe use of the electronic spectrum by friendly forces. The command and control of the Russian forces was disorganized due to poor communication. The predominant capabilities of Georgian communications and electronic warfare units have muffled Russian communications and Russian units used less secure communications (mobile phones). As an example, the commander of the 58th Army Anatoly Khrulyov used a satellite phone borrowed from a journalist to communicate with units, and was later injured as Georgian guidance systems detected and destroyed Russian radio and mobile phone signals [3].

Another weakness of the Russian Armed Forces was the support of electronic warfare: due to the lack of space and electronic intelligence data, they did not have accurate locations of Georgian units and used outdated topographic maps. Russian operations were complicated by the lack of satellite targeting to support the artillery, as

in August 2008 the grouping of satellites of the Russian GLONASS navigation system had not yet been completed and the deployed forces were not provided with receivers. Obsolete equipment of the self-recognition system (identification friend-or-foe) was also used, which led to numerous losses due to friendly fire on their units [4].

Russian electronic attacks were also unsuccessful in suppressing the enemy's air defense system: Georgian air defense systems destroyed four Russian aircraft (a TU-22M3 strategic bomber and three SU-25 attack aircraft). Russian forces failed to achieve complete dominance in the air, and its ground forces suffered from Georgian air strikes with SA-8 and SA-11 (ground-to-air) missiles. Also, the Russian side did not have aircraft with surface-to-air missiles capable of night operations and Georgian aircraft operated around the clock [5]. Thus, Russian forces have shown a critical deficit in all components of electronic warfare.

Military deception. Russia actively uses the practice of denial and deception (disguise), which is an integral part of military planning and operations in peacetime and during war. In the spring of 2008, the Russian government significantly increased the number of peacekeepers in Abkhazia and increased tensions in the region [11]. Even before the 2008 war, Russian forces attacked Georgian villages, destroying drones and radars to provoke Georgia into conflict. The build-up of Russian forces took place in the days before the conflict, and Russian units conducted military exercises "Kavkaz-2008" near the borders of Georgia, and after their completion remained on the training grounds [6].

The Russian media played a key role in spreading deceptive propaganda. Channel One showed an interview with an allegedly Abkhazian pilot who destroyed a Georgian UAV on April 20, 2008, indicating a possible Georgian invasion of Abkhazia. The Russian side used this to justify an increase in peacekeeping forces, additional units, equipment and weapons. Mass propaganda continued in the following months, when the media reported a gathering of Georgian forces near the Abkhaz border. In July 2008, Channel One reported that Georgia was planning to invade South

Ossetia, trying to convince the public that the aggressive Saakashvili should be stopped [7]. The illegal distribution of Russian passports among Georgian citizens in the conflict region also played a role. The Russian government justified the war by "protecting its citizens" from Georgian aggression. In fact, the Russian-Georgian conflict of 2008 was an organized campaign of deception aimed at increasing influence in the South Caucasus.

Operational security is a continuous process used to control information and encompasses physical, informational, computer, and communications security to detect and protect critical information. Security of operations was observed among Russian units. On March 11, 2007, a Georgian-controlled Kodori region was attacked by a helicopter. The Russians denied any involvement, saying the attack was a provocation by Georgia, but after an investigation, a UN observer mission in Georgia acknowledged that Russia was responsible. On August 6, 2007, a Russian pilot violated Georgian airspace and tried to destroy a radar installation. Russia has denied any involvement and has persuaded the international community that Georgia is again trying to provoke Russia, although the UN has established Russia's involvement in the incident.

On September 20, 2007, Russian forces attacked a Georgian construction crew near the Kodori Gorge. Georgian troops responded. Although an analysis by the Open Source Center found that the attack was carried out by Russian troops, representatives of Russia and Abkhazia denied the incident, and a request from the UN to investigate the Abkhaz side refused to hide the presence of Russian troops from the international community [12].

Psychological operations are planned operations on the transfer of information to influence the audience, the purpose of which is to change its behavior and create a favorable environment for the organizer of the operation. Russia has conducted psychological operations on the following target audiences: Georgian President Mikhail Saakashvili, the Georgian people, the Georgian armed forces, the United States, NATO and the international community. The main target was pro-Western President Mikhail

Saakashvili, who sought Georgia's membership in NATO, which Russia strongly opposed. A plan was drawn up to push Saakashvili into reckless hostilities and to demonstrate his instability as a NATO partner, while providing a pretext for Russia's intervention in Georgia. The Russia's General Staff used the "theory of reflexive control", the implementation of which allows to control the decision-making process of the opponent [11].

On August 13, 2008, the official newspaper "Krasnaya Zvezda" published a detailed psychoanalysis of Mikhail Saakashvili, which states that "he has a paranoid disorder of the steroid type of personality with a complex of narcissism, he considers the world as a hostile environment" [13]. The Russian side took advantage of this weakness to encourage shelling of Georgian villages by South Ossetian separatists in order to provoke Saakashvili to a military response. The rapid response of Russian units indicates a high level of readiness and careful advance planning. Throughout and after the conflict, Russia claimed about the opening of a criminal case against Saakashvili for genocide and war crimes in South Ossetia, comparing him to Slobodan Milosevic / Radovan Karadzic [1].

The focus on Saakashvili was aimed to discredit him at the international and domestic levels. At the beginning of the conflict, the Russian media completely denied the Georgian state as an aggressor, but later separated "Saakashvili criminal" from the Georgian people, to whom Russian President Dmitry Medvedev expressed "fraternal" support. Russia sought the legitimacy of its invasion into Georgia by influencing the international community, calling its operation a peacekeeping operation, countering "ethnic cleansing" and "Ossetian's genocide" [8].

Conclusions

The Russian-Georgian war in August 2008 between Georgia and Russia showed the growing impact of the information war and at the same time revealed a number of shortcomings of the Russian Armed Forces in this area. The conflict has also accelerated conducting of Russia's military reform, which will include the latest

advances in information technology. The Russian side pushed Mikhail Saakashvili to war, which it used to strengthen its international influence. Russia has managed to suppress Georgian leadership's communication with the outside world and its own citizens, and a brief confrontation on the Internet between Russian and Georgian hackers has sparked widespread debate about the power of the Internet to influence public opinion during the conflict.

References

1. Cohen, A. and Hamilton, R. (2011), The Russian Military and the Georgia War: Lessons and Implications, *Strategic Studies Institute*, pp. 4–45, available at: https://cutt.ly/EjS2Sp2 (accessed 21 January 2021).
2. Shakarian, P. (2011), The 2008 Russian Cyber Campaign Against Georgia, *Military Review*, November-December, pp. 63-68, available at: https://cutt.ly/vjJRYKU (accessed 21 January 2021).
3. Thomas, T.L. (2009), The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia, *The Journal of Slavic Military Studies*, 22(1), pp. 31–67. https://doi.org/10.1080/13518040802695241.
4. Mc Dermott, R.N. (2009), Russia's conventional armed forces and the Georgian War, *Parameters*, 39(1), p. 65, available at: https://cutt.ly/tjJRPAV (accessed 21 January 2021).
5. Nicolle, A. (2008), Russia’s Rapid Reaction: But Short War Shows Lack of Modern Systems, *IISS Strategic Comments*, Vol. 14, Issue 7, pp. 23-27. https://doi.org/10.1080/13567880802482243.
6. Cornell, S., Nilsson, N. and Popjanevski, J. (2008), Russian’s War in Georgia: Causes and Implications for Georgia and the World, *Central Asia Caucasus Institute Silk Road Studies Program Policy Paper*, August 2008, available at: https://cutt.ly/rjJRGIK (accessed 21 January 2021).
7. Lukas, E. (2009), *The New Cold War: Putin's Russia and the Threat to the West*, Palgrave Macmillan, New York, pp. 141-147.
8. Rogoza, J. (2008), Russian Propaganda War: Media as a Long- and Short-range Weapon, *Center for Eastern Studies*, Issue 9, pp. 1–5, available at: https://cutt.ly/0jJRBEf (accessed 21 January 2021).
9. Hollis, D. (2011), Cyberwar Case Study: Georgia 2008, *Small Wars Journal*, available at: https://cutt.ly/QjJRMBh (accessed 21 January 2021).
10. Report (2009), *Independent International Fact-Finding Mission on the Conflict in Georgia*, Vol. II, pp. 218, available at: https://cutt.ly/TjJR3kv (accessed 21 January 2021).

11. Blandy, C. (2009), Provocation, Deception, Entrapment: The Russo-Georgian Five Day War. Advanced Research and Assessment Group, *Defense Academy of the United Kingdom*, available at: https://cutt.ly/QjJR5bR (accessed 21 January 2021).

12. Russell, J. and Kimberly, M. (2012), *Warlords: Strong-Arm Brokers in Weak States*, Cornell University Press, London, 262 p. https://doi.org/10.4000/pipss.4050.

13. Ruchkin, V. (2008), "Virus vozhdizma" [Leadership virus], *Krasnaya Zvezda*, available at: https://cutt.ly/ujJTvlU (accessed 21 January 2021).

Yurii Stasiuk
Candidate of Historical Sciences
Head of Research Laboratory of Research Centre of Military History
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine.
https://orcid.org/0000-0003-3832-4353

Volodymyr Kydon
Candidate of Historical Sciences
Leading Researcher at the Research Centre of Military History
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-3606-8061

THE PHENOMENON OF THE UKRAINIAN VOLUNTEER MOVEMENT IN REPELLING THE RUSSIAN HYBRID AGGRESSION

The authors, basing on the studied open diversified literature, note the contribution of the volunteer movement to the revival of the Ukrainian army, highlight the reasons for the creation of volunteer units and the entry into them of people who supported the Revolution of Dignity and stopping the hybrid Russian aggression. It was noted the active participation and invaluable contribution of public associations and organizations in their emergence. The article gives a conditional division of Ukrainian volunteer formations. The article, basing on Russian sources, focuses on the success of combat operations in the ATO area in 2014 with the participation of armed formations, created and staffed by the aid of the Ukrainian volunteer movement.

Keywords: *Ukrainian volunteer movement, Ukrainian volunteer formations, public associations and organizations, anti-terrorist operation in the east of Ukraine.*

Introduction

During the hybrid aggression in the East of Ukraine, it was unexpected for the Putin regime to meet the activity of the concerned

citizens of Ukraine to protect the state from intervention, which grew into a unique phenomenon into the volunteer movement during the days of Ukraine's independence.

Problem statement. The inability of the state authorities and the armed formations of Ukraine to neutralize the hybrid aggression caused the emergence of the Ukrainian volunteer movement in Ukrainian society, gave impetus to the revival of the Ukrainian army [1–2].

The analysis of the recent researches and publications. With the beginning of the annexation of the Autonomous Republic of Crimea by the Russian Federation, the leadership and representatives of the government of Ukraine drew attention to the power structures and their condition, especially to the Armed Forces of Ukraine, whose main task is to ensure the territorial integrity of the state and sovereignty. However, during the parliamentary hearings in 2014, concerning the aggression, A.V. Turchynov, the Chairman of the Verkhovna Rada of Ukraine, noted, "... when after the fall of the regime, when there was no power in Ukraine, the aggression began, we saw in what a terrible situation our army is ..." [3, pp. 7-8]. We can also quote the words of I. S. Rusnak, the acting Minister of Defence of Ukraine, about the state of the Armed Forces of Ukraine during the report, "... that the national defence capability does not fully neutralize existing threats ..." [3, p. 10]. The modern Russian researcher A. Tsyganok in his work [4] finds out the reasons for the events in the East of Ukraine, analyses the military potential of Ukraine, assesses the activities of the Ukrainian government, the Armed Forces of Ukraine, other military formations, and also considers the opposite side. When describing the combat operations in the summer of 2014 in the Donbas, the author concludes that at that time there was no combat-ready army in Ukraine even to fight the so-called pro-Russian fighters [4, p. 354].

Purpose of the report is to highlight the unique contribution of the Ukrainian volunteer movement during the time of independence of Ukraine in countering the hybrid Russian aggression.

Main part

The main reasons for the formation of Ukrainian volunteer formations in 2014 and the entry of Ukrainian citizens into them were:

– the failure of state authorities, the Armed Forces of Ukraine, other military formations and law enforcement agencies to stop Russian hybrid aggression;

– the low degree of public trust in law enforcement force after the Revolution of Dignity;

– the impossibility of those wishing to be involved in the Armed Forces of Ukraine, other military formations and law enforcement agencies to protect the state for health reasons, age, etc.

The investigated historiographic material on the subject of the study gives grounds to highlight several dominant features inherent of the volunteer armed formations created or self-organized to defend Ukraine - territorial defence battalions of the Armed Forces of Ukraine, units of the Special Tasks Patrol Police of Ukraine of the Ministry of Internal Affairs, volunteer units as part of the National Guard of Ukraine: staffed on a voluntary basis; created on the initiative of the Ukrainian political forces with the outbreak of the armed conflict in the East of Ukraine; the positive attitude of volunteers to the Revolution of Dignity; active participation in the activities of the Maidan; support for the actions of the new leadership of the state; support of these formations by the Ukrainian society; a high degree of confidence of Ukrainian citizens in them in the first period of the armed conflict.

Basing on the analysis of the identified sources, we consider it appropriate to conditionally divide the Ukrainian volunteer formations of 2014-2015 years considering from the perspective of the role of state structures in their creation. The first group includes temporary formations created with the participation of the state (Territorial Defence Battalions as part of the Armed Forces of Ukraine, Special police battalions - the Ministry of Internal Affairs, reserve battalions - the National Guard of Ukraine) together with pro-Ukrainian parties, public associations, local authorities and self-

government bodies.

The second group includes the formations created directly by Ukrainian parties, public associations and at the expense of the charity providers (I. V. Kolomoiskyi - one of the founders of the industrial and financial group "Privat"; G. O. Korban - a member of the Supervisory Board of the Ukrainian oil and gas production company "Ukrnafta" etc.) or self-organized of the concerned citizens, as well as groups of foreigners wishing to defend the territorial integrity of Ukraine. This group includes: The Volunteer Ukrainian Corps (hereinafter - DUK), created by the public organization "Right Sector"; the battalion "OUN" - by the political party "UNA - UNSO"; the special operations volunteer Cossack squadron named after Taras Shevchenko - by the Kyiv Cossack organization "Kyiv Cossack Regiment named after Taras Shevchenko BUK "and others.

So, taking into account the above, we consider that the Ukrainian volunteer formations are the newly-formed temporary volunteer formations as an auxiliary defensive resource of the state, which received weapons to protect the territorial integrity and state sovereignty of Ukraine, in the formation of which state bodies, political parties, public associations and groups took part, self-organized citizens, in compliance with the principle of voluntariness.

The derivatives for Ukrainian volunteer formations were mainly public formations. The Law of Ukraine "On Citizens' Participation in the Protection of Public Order and the State and Frontier" dated June 22, 2000, No. 1835-III standardizes the process of creating public formations based on public associations on a voluntary basis to participate in the protection of public order and the national boundaries, assistance to local governments, law enforcement agencies, the State Border Guard Service of Ukraine and executive authorities, as well as officials in the prevention and suppression of administrative offences and crimes, protecting the life and health of citizens, the interests of society and the state from unlawful encroachments.

Such formations operated, as a rule, within the territorial community, where they actively emerged during the Euromaidan and

the Revolution of Dignity (local Self-defence groups), and with the appearance of the visible terrorist threats in Ukraine in February 2014. An especial need for public formations arose in those regions where the then law enforcement agencies collaborated with Russian militants, were supportive of them, and a high level of corruption was developed in their ranks [5].

Over time, many territorial-public formations became the basis for the creation of Ukrainian volunteer formations, in particular the battalions "Donbas", "Dnepr-1", "Kyivan Rus", "Azov".

The organizational basis for the creation of territorial defence battalions and the definition of the range of their main tasks were the Law of Ukraine "On the Defence of Ukraine" [6] and the Decree of the President of Ukraine "On Approval of the Regulations on the Territorial Defence of Ukraine" dated September 2, 2013, No. 471/2013. Their creation was supposed in the extraordinary period by the current mobilization plan, approved by the mobilization department of the General Staff of the Armed Forces of Ukraine. In compliance with these laws, thirty-two battalions of territorial defence were formed in Ukraine as of October 2014. The article by Yu. Butusov [7] published on August 29, 2014, notes that an order was signed on the creation of the 31 battalions of territorial defence.

The Legal basis for creating and functioning of the special-purpose patrol police units was the Law of Ukraine "On the Police" [8]. Under it, to ensure public order at facilities and territories, the Ministry of Internal Affairs of Ukraine may create special police units. On April 13, 2014, the Minister of the Ministry of Internal Affairs A. Avakov announced the adoption of the decision on the creation in each region of Ukraine under the regional headquarters of the Ministry of Internal Affairs of the special-purpose patrol police units basing on public formations in compliance with the principle of voluntariness [9].

To create volunteer divisions of the National Guard of Ukraine, the Law of Ukraine "On the National Guard of Ukraine" was applied [10]. There were 4 subdivisions in the National Guard of Ukraine.

The public associations that actively created volunteer formations were as follows: the Social-National Assembly, "Patriot of Ukraine", as well as "Avtomaidan", whose activists in May 2014 replenished the "Azov" battalion [11, p. 418], and its backbone was the "Black Corps" partisan detachment founded in April of the same year for the liberation of the East of Ukraine; All-Ukrainian public movement "Self-defence of Maidan", and its representatives became the basis of some volunteer formations, reserve battalions of the National Guard of Ukraine, 24hth Territorial Defence Battalion "Aidar", 25th Territorial Defence Battalion "Kyivska Rus", the unit of the special-purpose patrol police "Lviv" and others. Also, active participants were local public associations of Afghans, the former law enforcement officials, fishermen, hunters, football fans, airsoft players, etc. [11, p. 169].

The UNA-UNSO organization (The Ukrainian National Assembly – Ukrainian People's Self-Defence), after changing its name to the "Right Sector" in March 2014, together with the Right Sector social movement, developed the Ukrainian Volunteer Corps (later the Ukrainian Volunteer Army was created from its members) as a branch of the security-defence social movement, which was not officially included in the legal security, defence and law enforcement structures but actively cooperated with them. July 17, 2014, is considered the day of its creation [12]. In contrast to all other political forces, the "Right Sector" independently created an extensive network throughout Ukraine of reserve battalions that recruited volunteers, and centralized training centres where fighters were prepared for combat, as well as the medical unit that assisted all injured participants of the combat actions in the area of the anti-terrorist operation.

Among the self-organized units, the most famous are: the special operations volunteer Cossack squadron named after Taras Shevchenko, which collaborated with the State Border Guard Service of Ukraine and participated in battles in the sector "M"; the partisan group "Tini" ("Shadows"), which took part in the liberation of the city of Mariupol; the "Donbas" battalion, formed at the initiative of a

group of volunteers and led by Semen Semenchynk in mid-April 2014 as a public formation "Territorial defence battalion of Donetsk region"; the volunteer group "Aerorozvidka" ("air intelligence") under the leadership of V. Kochetkov-Sukach and many others.

Among the progressive-minded people, there is no objection to the significant contribution of the pro-Ukrainian volunteer movement, in particular Ukrainian volunteer formations, in repelling and curbing Russian hybrid aggression. However, as it was known at all times, the assessment of the enemy (the opposite side of the conflict) concerning the opponent's armed forces is worthy. Among the few Russian historiographic works considered to one degree or another the subject of research, our attention was drawn by the monograph by A. Tsyganok. The author, analyzing the battle operations in the Donetsk and Luhansk regions in the summer of 2014, considers, the reason for the stubborn resistance of the Ukrainian troops who were surrounded by there, were battalions formed mainly of volunteers, including in the infamous tragedy near Illovaisk [4, p. 385].

Considering the above, we, therefore, believe that Ukrainian volunteer formations are newly-formed temporary volunteer formations as the auxiliary defensive resource of the state, that received weapons to protect the territorial integrity and state sovereignty of Ukraine, in the formation of which state bodies, political parties, public organizations and groups of self-organized citizens, took part, in compliance with the principle of voluntariness.

Conclusions

So, a unique phenomenon in the days of independent Ukraine, which contributed to the repulsion of Russian hybrid aggression, is its phenomenon - the Ukrainian volunteer movement. The Ukrainian volunteer movement personifies the invincibility and intransigence of the Ukrainian people, who, from everlasting, were fighting and have won freedom and independence. The Ukrainian volunteer movement contributed to the revival of the Ukrainian army and the transmission of the best traditions of the defender of the fatherland.

References

1. Ministry of Defense of Ukraine (2016), "*Kozhen ukrajinecj zrobyv svij vnesok u vidrodzhennja nashogho vijsjka – Ghlava derzhavy*" [*Every Ukrainian made his contribution to the revival of our army - Head of State*], available at: https://cutt.ly/OjBxmGx (accessed at 23.01.2021).

2. ESPRESO.TV (2018), "*Amerykansjki gheneraly nazvaly vidrodzhennja ukrajinsjkoji armiji za korotkyj chas dyvom*" [*American generals called the revival of the Ukrainian Army in a short time a miracle*], available at: https://cutt.ly/4jBzI0d (accessed at 23.01.2021).

3. Verkhovna Rada of Ukraine (2014), "*Postanova pro Rekomendatsii parlamentskykh slukhan na temu: Oboronozdatnist Ukrainy u XXI stolitti: vyklyky, zahrozy ta shliakhy yikh podolannia*" [*Resolution on the Recommendations of the Parliamentary Hearings on the topic: "Ukraine's Defense Capability in the XXI Century: Challenges, Threats and Ways to Overcome Them"*], available at: https://cutt.ly/3jBz3q5 (accessed at 23.01.2021).

4. Cyghanok, A.D. (2016), "*Donbass: neokonchennaja vojna. Ghrazhdanskaja vojna na Ukrayne (2014–2016): russkyj vzghjad*" [*Donbas: An Unfinished War. Civil War in Ukraine (2014-2016)*], AYRO, Moscow, 677 p.

5. Bodnja T. (2014), Bataljjony chekajutj na dobrovoljciv [The battalions are waiting for volunteers], *Urjadovyj kur'jer*, No. 81, p. 2.

6. The Law of Ukraine (1991), "*Pro oboronu Ukrajiny*" [*On Defence of Ukraine*], available at: https://cutt.ly/gjBxi1Q (accessed at 23.01.2021).

7. Butusov, Ju. (2014), "Dobrovoljcheskye bataljony: struktura, strakhy, problemy boevogho prymenenyja" [Volunteer battalions: structure, fears, problems of combat use], *Zerkalo nedely*, available at: https://cutt.ly/ejBxkfG (accessed at 23.01.2021).

8. The Law of Ukraine (1990), "*Zakon Ukrajiny Pro miliciju*" [*Law of Ukraine "On the National Police"*], available at: https://cutt.ly/TjBcgod (accessed at 23.01.2021).

9. Word and Deed (2014), "*Avakov sformuje reghionaljni specpidrozdily MVS na osnovi ghromadsjkykh utvorenj*" [*Avakov will form regional special forces of the Ministry of Internal Affairs based on public formations*], available at: https://cutt.ly/HjBxF83 (accessed at 23.01.2021).

10. The Law of Ukraine (2014), "*Pro Nacionaljnu ghvardiju Ukrajiny*" [*Law of Ukraine "On the National Guard of Ukraine"*], available at: https://cutt.ly/JjBxL5M (accessed at 23.01.2021).

11. Ghladka, K., Ghromakov, D. and Myronova, V. (2016), "*Dobrobaty*" [*Ukrainian volunteer battalions*], Folio, Kharkiv, 570 p.

12. Banderovets (2014), "*Pro stvorennja Dobrovoljchogho ukrajinsjkogho korpusu Pravyj sektor*" [*On the creation of the "Right Sector"*], Banderivecj, available at: https://cutt.ly/ijBx3eX (accessed at 23.01.2021).

Victor Topalskyi
Candidate of Historical Sciences
Leading Researcher of the Research Centre
of Humanitarian Problem of Military Forces of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0003-2074-0121

Serhii Ivanenko
Postgraduate Student of Scientific-Experience Centre
of Military History of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-6382-040X

NARRATIVE "GREAT MILITARY WAR" IN RUSSIAN ANTI-UKRAINIAN PROPAGANDA

The peculiarities of the Kremlin propaganda's use of the narrative "Great Patriotic War" to create an "image of the enemy" from Ukraine, demonization of the state leadership, personnel of the Armed Forces of Ukraine and other law enforcement agencies, as well as legitimizing Russian aggression against our state.

Keywords: *anti-Ukrainian propaganda, discourse, World War II, narrative, Nazis, image of the enemy, memorable dates, victory, fascists, fake.*

Introduction

Problem statement. To generalize the peculiarities of the Kremlin propaganda's use of the "Great Patriotic War" construct in order to create an "image of the enemy" from Ukraine, demonize the state leadership, personnel of the Armed Forces of Ukraine and other law enforcement agencies, and legitimize Russian aggression against our state.

The analysis of recent research and publications: The achievements of modern Ukrainian scientists on the subject of the study allows us to assess the degree of elaboration of the problem. Peculiarities of the use of myths about the World War II by Russian

propaganda were studied by V. Viatrovych, L. Hudkov, T. Zhurzhenko, D. Zolotukhin, S. Lewis, G. Pocheptsov, and Yu. Fihurnyi.

Purpose of the report of the proposed study is to highlight the peculiarities of the operation of the memory of World War II by the Russian Federation among the local population of the so-called DPR / LPR and Russian citizens, in order to form the basis for further escalation of the conflict with Ukraine.

Main part

Celebrating the anniversary of the victory over Hitler's Germany, showing respect and gratitude to all those who fought against Nazi aggression, resisted crimes against humanity has become a good tradition in all countries of the Anti-Hitler coalition. Recently, however, in modern Russia, this event has become an occasion for militaristic propaganda, a way to further formation of the Ukranian prototype of the enemy. Its effectiveness lies in the fact that it is based on social ideas, stereotypes and myths that were formed and maintained by the Soviet regime for decades and live today [1]. This is done to restore Russian influence in the post-Soviet space. A significant place is given to "common history", the central points of which are the concepts of the "Great Patriotic War". Thus, the myths of the past war became a weapon in the modern war.

This discourse occupies an important place in the anti-Ukrainian propaganda of the Russian Federation or, more precisely, with that segment of it, which, according to the established Soviet tradition, is called the "Great Patriotic War" [2]. Russian politicians do not tire of talking about "Nazi" and "fascist" Ukraine. Thus, the head of the Ministry of Foreign Affairs of the Russian Federation, Serhii Lavrov, used the words “Nazis” and “Nazi state” in Ukraine only four times in one interview [3]. Moscow thus justifies its aggression, dehumanizes the enemy, which Ukraine has recently become for the Russians. A similar situation took place in the late 1990s in the Baltic States and later in Georgia in 2008. Through attempts to build their states without dictation from Moscow, these

countries became "Nazi" for the Russians. It is noted that if the country has nothing to be proud of, the presence of the enemy becomes a very powerful factor in internal consolidation and injection of the atmosphere [4]. This is exactly what has happened in Russia in recent years.

The ideological justification of Russian aggression against independent Ukraine was based on the requirements of the memory of the past, and the war in Ukraine was usually interpreted as a continuation of World War II [5]. Saying that fascists and Nazis came to power in Kyiv, Putin raised layers related to the traumas of World War II and the struggle against fascism, which are very sensitive things for the collective consciousness of Russians [6].

Initially, Ukrainian servicemen were deliberately called "punishers." Creating fakes about the so-called "crimes" of the Armed Forces of Ukraine and volunteers, these words began to be systematically spread through the Russian media [2]. In contrast to the servicemen of the Armed Forces of Ukraine, other law enforcement agencies, and volunteer battalions, which in the news the propagandists presented mainly as "punishers" and "fascists", drawing parallels with World War II, the term "militia" was used to refer to separatists and the Russian military. The analogy between the heroic struggle of the Soviet people against German aggression showed that ordinary miners, metallurgists, and tractor drivers rebelled against the Nazis and the Banderas.

Symbolic is the use in Donetsk on August 24, 2014 on the Independence Day of Ukraine, the so-called "parade of shame", in which Ukrainian prisoners were forced to pass in front of an angry crowd of locals who threw rotten food and spat at prisoners, and immediately behind the car cleaned the road. This parade was organized as a repetition of the famous Stalinist "Parade of the Defeated" in 1944, when German prisoners of war marched through Moscow accompanied by sweepers. It was this parallel that directed the explosion of collective emotions here. Pro-Russian organizations used her sacralized narrative to legitimize a ritual act of humiliation arranged as a memorial act.

To draw an analogy between modern events and those that took place during the World War II, pseudo-witnesses of those terrible times are involved. Thus, on November 2, 2014, the First Channel of Russian television told the stories of alleged residents of the village of Stepanovka, Donetsk region, which compared the events of 1941 and autumn 2014. The information was presented in such a way that Ukrainian servicemen were equated with Nazi invaders. The pseudo-witness of those events is an elderly woman Lyudmila, who allegedly turned 80 in 2014. She seemed to have survived the famine of the 1930s and the war [2]. The lie is revealed instantly - you just have to count her age and the events she allegedly went through. It turns out that she was born in 1934 and remembers the Holodomor of 1932-1933. Or, in November 2014, on Russia 1's Sunday Evening with Vladimir Soloviov program, one of the guests told a story at a checkpoint near Kramatorsk, where eggs were taken from elderly people and once a 47-year-old woman was raped. The end of the story ended with the question: "Aren't they fascists?" [7].

Russian propagandists emphasize the brutality of the Ukrainian military with the people, talking about concentration camps for residents of Donbass (like the Nazis). The fake about the concentration camp in Mariupol lived for a long time. He appeared on the program "Special Correspondent" on "Russia 2" on March 1, 2016. Then the "official representative" of the so-called "DPR" stated that on the territory of the city airfield there is a concentration camp and a cemetery with at least 2.5 thousand bodies of people who went missing [2]. To enhance the effect, the material mentioned the anniversary of the liberation of the city from Nazi invaders. And there are many such examples that help to consolidate the "image of the enemy" among Ukrainians. The culmination was the appearance of the "crucified boy".

Russian propagandists often appeal to the narrative of the "single Soviet nation", which is used to influence those Ukrainians for whom this ideology is important [2] even today.

The image of the enemy is not canceled, but simply attached to the new object. Today it is no longer Germans, but "Ukrainian

punishers", "Bandera" and so on. The presence of a dangerous enemy entails the need for constant readiness to counter it. Society is mobilized for a new struggle, and the old stamps are only applied to new objects and situations [8].

According to the head of the Analytical Center Yurii Levada (Levada Center) Lev Hudkov, the victory of the Soviet Union in 1945 - is not only the central semantic node of Soviet history, but in fact the only positive fulcrum of national identity of Russian society, the main symbol that can integrate the nation [9]. The narrative of the Great Patriotic War is essentially a political myth.

The key target audiences for the Russian secret services and the media that work with them in the context of coverage of this Kremlin narrative are, first of all, residents of the occupied districts of Donetsk and Luhansk regions, as well as Crimea, Russians, citizens and political elites of Western Europe and America. For example, the Kremlin monopolized the memory of World War II in Germany. In this European country, Russians are spreading the myth that Ukrainians are "fascists." It is clear that not everyone believes in him, but even those who do not believe, with the help of the Russian media, focus on nationalist sentiment in Ukraine. At the same time, most sometimes do not understand what we are talking about. Indicative in this respect is the story of the greeting "Glory to Ukraine!", which Russian propagandists present abroad as a fascist greeting. Putin's propaganda masterfully uses such opportunities, [10] and for Germans, for example, if something resembles National Socialism, it is very bad.

People close to ex-President Viktor Yanukovych take an active part in anti-Ukrainian propaganda in the role of "exposers of the fascist essence of the Ukrainian regime." Thus, in a speech by ex-deputy V. Oliinyk on June 24, 2018 on Russia's First Channel, it was stated that "the country is under occupation by the grandchildren of Bandera and should be liberated immediately."

Citizens of other states are also involved in propaganda activities against Ukraine. Thus, a journalist of Russia Today TV channel, Graham Phillips, a British citizen, while in the occupied

territory of Donbass, recorded a video interview about alleged foreign mercenaries fighting on the side of Ukraine, destroying the “Russian-speaking population of Donbass” for money [2]. He notes that they are part of the occupation contingent, as are the Ukrainian "fascists" and NATO troops. The Kremlin also engages foreign lobbyists in anti-Ukrainian propaganda, including former high-ranking officials in some European countries.

Russian propagandists and their satellites widely used such forms as staging videos, fake photos, postcards, and posters. The photos, which were initially distributed by Russian propagandists from Komsomolskaia Pravda, Alexandr Kots and Vladislav Berdychevskii from the so-called DPR, show an allegedly unexploded Ukrainian propaganda shell with leaflets inside. The leaflets depicted a Wehrmacht soldier with elements of Ukrainian symbols against the background of killed children and women. It was reported: “We do not need people! We need territory!… We will soon be slaughtering your women and children, and you will meet the new year on earth or in prison!” [11]. These leaflets were prepared by Russian propagandists to discredit Ukrainian soldiers.

Despite the fact that during the World War II our people bore on their shoulders all the horrors of the occupation, Vladimir Putin said that the war would have won without the Ukrainians, which caused the greatest insult to our people, who made a huge contribution to victory over German Nazism [12]. This statement distanced Ukrainians, including war veterans, from this victory. All this is used as a weapon against our state.

Conclusions

Thus, the construct "The Great Patriotic War" is the "basic plot" of the historical policy of the Putin regime. However, only the strengthening of the unity of Ukrainian society on the basis of historical memory, in no way forgetting the contribution of the Ukrainian people to the victory over Nazism, will help debunk the myths of Russian anti-Ukrainian propaganda.

References

1. The site of special project “Ukrainian Second world war” (2016), “*Mify i viina*” [*Myths and war*], available at: https://cutt.ly/xkc6OwC (accessed 7 March 2020).

2. Zolotukhin, D.Yu. (2018), “*Bila knyha spetsialnykh informatsiinykh operatsii proty Ukrainy 2014–2018*” [*White Book of Special Information Operations against Ukraine 2014–2018*], Kyiv, 384 p.

3. Tymots, I. (2019), “Tomos dlia Ukrainy – tse pliuvok u dvoholovoho orla rosiiskoho imperializmu. Treba buty hotovym do vsoho” [Tomos for Ukraine is the spittle of the double-headed eagle of Russian imperialism. You have to be ready for anything], *Kraina*, 8 January.

4. Hudkov, L. (2018), “Faktor vraga. Chto rossiyane dumayut ob ukraintsah” [The enemy factor. What do Russians think about Ukrainians], *The site of “InfoResist”*, available at: inforesist.org/faktor-vraga/ (accessed 7 March 2020).

5. Zhurzhenko, T., Liuis, S. and Fedor, D. (2018), “Viina i pamiat v Rosii, Ukraini ta Bilorusi” [War and memory in Russia, Ukraine and Belarus], *The official site of “Modern Ukraine” magazine*, available at: https://cutt.ly/ZkvtDKj (accessed 10 March 2020).

6. Hudkov, L. (2017), “Ukraina dlya rossiyan – vrag. Boyus, eto nadolgo” [Ukraine is an enemy for Russians. I'm afraid this will be long], *The site of “LiveJournal”*, available at: trim-c.livejournal.com/1861573.html (accessed 7 March 2020).

7. YouTube (2014), “*Marazmyi: Ukrainskie karateli iznasilovali pensionerku*” [*Marasmus: Ukrainian punishers raped a pensioner*], available at: www.youtube.com/watch?v=j-WJSWVeJnA (accessed 10 March 2020).

8. Dodonov, R.O. (ed.) (2017), “*Hibrydna viina: in verbo et in praxi: monohrafiia*” [*Hybrid war: in verbo et in praxi: monograph*], Nilan LTD, Vinnytsia, 412 p.

9. Hudkov, L. (2005), “Pamiat” o voine y massovaia ydentychnost rossyian” [“Memory” of the war and the mass identity of Russians], *The site of special project “Magazine hall”*, available at: https://cutt.ly/ckvtTLY (accessed 9 March 2020).

10. Raitshuster, B. (2019), “Pro Merkel i Nimechchynu v tsilomu” [About Merkel and Germany in general], *The site of “Ukrainian Pravda”*, available at: https://cutt.ly/JkvtB6w (accessed 12 March 2020).

11. The site of “TV Zvezda” (2017), “*Novyiy god vyi vstretite v zemle”: natsionalistyi obstrelivayut Donbass snaryadami s ugrozhayuschimi listovkami*” [“*You will meet New Year in the ground”: nationalists shell Donbass with shells with threatening leaflets*], available at: https://cutt.ly/Ckvywq6 (accessed 11 March 2020).

12. Zubarieva, M.A. (2015), “Analiz informatsiinoi viiny mizh Rosiieiu ta Ukrainoiu v informatsiinomu suspilstvi” [Analysis of information war between Russia and Ukraine in information society], *Information society: an academic journal*, No. 21, pp. 6-11.

Oleksandr Vasyliev
Senior Scientific Researcher of the Centre for Military
and Strategic Studies of National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-9492-5594

ANALYSIS OF THE MAIN ASPECTS OF "HYBRID WAR" AND "HYBRID" ACTIONS IN MODERN CONFRONTATION

The article deals with the main aspects of new so-called "hybrid war" concept of military confrontation. The components of "hybrid" actions, which are characterized by economic confrontation, massive information attacks and operations in the cyber space, are analyzed. A systematic approach to the study of this problem is chosen as a methodological basis of the article. Based on the analysis, it is concluded that the threat of "hybrid"actions is extremely relevant at the present time and will continue in the nearest future.

Keywords: *information war, interstate confrontation, hybrid action structure, features of modern warfare, soft power, proxy war, hybrid wars, economic confrontation, hybrid threats.*

Introduction

"Hybrid warfare" is interpreted as "the use of military and non-military tools in an integrated campaign aimed at achieving surprise, seizing the initiative and obtaining psychological advantages using diplomatic opportunities; large-scale and rapid informational, electronic and cyber operations; cover-up and concealment of military and intelligence actions combined with economic pressure" in the military Balance Handbook [1]. One of the definitions emphasizes that "hybrid war is a combination of open and secret military actions, provocations and sabotage combined with denial of one's own involvement, which makes it much more difficult to fully respond to them" [2].

Sometimes "hybrid" actions are considered to be so-called

“proxy wars” (from the English language “proxy war”, or “proxy war”, “war by proxy”). This type of confrontation is understood as an indirect international conflict between two countries that are trying to achieve their goals through military actions taking place in the territory and using the resources of a third country, under the guise of resolving an internal conflict in this country [3]. At the same time, there is a tendency to shift the emphasis of “hybrid” actions from conducting “proxy wars” to the sphere of non-military confrontation.

The phenomenon that is currently called as “hybrid war” and “hybrid forces” is not new, but has historical analogues in the history of mankind.

The analysis of recent researches and publications. “Conflict in the 21st century: The rise of hybrid wars” by F. Hoffman [4] from 2007 to the present time has become the gold standard for understanding the concept of hybrid forces and the synergistic effects they can produce.

“Hybrid war” monograph by T. McCulloch and R. Johnson was published in 2013 [5]. The monograph presents the theory of hybrid warfare, as well as the definitions of hybrid force are given basing on a review of the relevant literature. According to T. McCulloch and R. Johnson [5, p. 9] F. Hoffman’s ideas about hybrid warfare and his approach are revolutionary since he was a person to justify the concept of hybrid warfare. However, to discuss the theory, the authors of the monograph insist, this work has mostly descriptive style and does not give a vision of the form, functions and logic of a hybrid structure and waging a hybrid war. The best explanation of hybrid structures, in their view, lies in direct contact with the theory of principles that provide a broad understanding and justification for the existence of hybrid structures.

The following authors delt with the topic of hybrid warfare: F. Hoffman, T. McCulloch and R. Johnson mention only W. Nemeth [6] and E. M. Simpson [7].

It is worth mentioning two studies, which are available in the open access. These are master theses, similar to the mentioned thesis

of W. Nemeth, which were completed at the same educational institution – Naval Postgraduate School (University / advanced training courses for officers of the US Navy) in 1998 and are devoted to hybrid warfare and hybrid forces. These are the dissertations by James Dugan "Elusive armies and invisible hands: combining conventional and guerrilla forces from 1776 to the present" [8] and Robert Walker "SPEC FI: the United States Marine Corps and special operations" (SPEC FI: the United States marine Corps and special operations) [9].

In his dissertation J. Dugan considers the effectiveness of hybrid forces containing both irregular and regular components [8, p. 4–7] in protracted campaigns at the tactical level. The Dissertation Of J. Dugan could be interesting to those who are seriously engaged in the topic and phenomenon of hybrid warfare.

It should be noted that all three mentioned above dissertations in one way or other touched the topics of hybrid forces or hybrid war (these are the works by J. R. R. Tolkien). One of the dissertation consultants is Gordon N. McCormick, Professor of the Department of analysis of military problems Of the school of advanced training of officers of the US Navy. His research interests include the following topics: special operations, intra-state conflicts, wars involving irregular armed formations (irregular combat operations), and guerrilla warfare. This topic intersects with a range of the scientific interests of another Professor of the same faculty, D. Arquilla, the supervisor of R. Walker's work on the US Marine Corps as a hybrid force capable of fighting as regular and irregular units.

Purpose of the report. The purpose of the article is to analyze the main aspects of the concept of "hybrid war", which is based on one of the most effective ways of conducting interstate confrontation.

Main part

In modern conditions, the attention of researchers is increasingly attracted to the phenomenon of hybrid war as a hidden conflict that has a complex internal structure and proceeds in the

form of an integrated military-political, financial-economic, informational and cultural-ideological confrontation that does not have a certain status.

The essence of a hybrid war, like any other war, is the redistribution of the roles of the subjects of the political process at the global and regional levels. However, it is carried out mainly by non-military means without occupation of the defeated country, destruction of its infrastructure and the mass death of the population. Information and communication technologies allow to achieve the transfer of the country under external control with a minimum level of military violence due to concentrated pressure in the financial and economic, information and psychological spheres and the use of cyber weapons.

The content of hybrid warfare is reduced to a comprehensive competition for the role of leader and expanding access to resources. The winner is the state or coalition that have managed to impose their inherent vision of the world, values, interests on the enemy and the understanding of “fair” distribution of resources corresponding to their worldview.

The main instrument of warfare is the army, irregular armed and paramilitary formations capable of conducting continuous and systematic military operations. Along with the armed struggle, which is the specific content of war, it also uses economic, diplomatic, scientific and technical, informational, ideological, psychological means and methods of imposing one’s will on the enemy, weakening his military capabilities and strengthening his own positions.

However, it is precisely military violence, the use of technical means (weapons) to physically suppress the enemy, to subordinate him to his will, that constitutes the essence of war, is its defining feature. The war differs from other types of political struggle and various forms of use of weapons in the following ways: invasion, military incident, military blockade, threat of force, special operation, including anti-terrorist.

At the same time, in modern conditions, war does not necessarily have to be associated with the beginning of hostilities.

The continuation of politics can be carried out by force not only by military, but also by non-military means.

With the advent of the post-industrial era, information warfare was supplemented by actions in cyberspace [10] and the use of destructive socio-political technologies [11].

The latter are now used so intensively that they can be distinguished as another component of the "hybrid war". Moreover, their diversity even allows for an internal classification of such actions: from simple financial and informational support for opposition movements and the creation of a "fifth column" within the enemy state, to the introduction of agents of influence that ensure the so-called "soft occupation" of the country and its transition to external control. The methods used vary in intensity and degree of stealth applied depending on the opponent against whom they are used.

Typical examples of the modern use of such technologies are the organization of so-called "color" revolutions through the activities of various non-profit organizations. Practice shows that such actions are not only more effective, but also significantly cheaper than direct military intervention.

In the era of globalization and the information revolution, the activity of information warfare and the use of destructive socio-political technologies has become so extensive that experts are talking about the outbreak of the so-called "post-truth" era [12, 13]. One of the aspects of the practical application of information warfare can be considered the use of the national issue as a justification for "hybrid" actions.

In recent history, with the growing mobility of the population, such "pre-hybrid" actions can be implemented by obtaining citizenship in the territory of a foreign state, legitimizing citizens by buying land or real estate, and migrating. All this increases the danger and can be considered one of the elements that precedes and brings the "hybrid war" closer.

The most important aspect of "hybrid" wars is an economic component. In historical retrospect, its use began with the transition

from subsistence farming and separate national economies to a global economic system associated with the interstate division of labor and international trade. History shows a large number of methods used within this component of the confrontation. For example, France during the Napoleonic wars forged English, Austrian and Russian banknotes.

Nowadays, with the advent of the era of globalization, the financial component of "hybrid wars" has significantly increased. The variety of methods are used in terms of the scale of application. The latter range from direct blocking of financial accounts of individuals and even governments of opposing States to indirect methods based on prohibitions. An example of the first type of action is the blocking of foreign accounts of Iraq in 2012 and Venezuela in 2019. Indirect methods are clearly visible in the bans on the passage of funds through "third countries" and companies to block access of Iranian banks to the SWIFT system in 2018.

Another component of the economic confrontation, which lies on the verge of humanitarian-permissible – resource confrontation. Its varieties have been used since ancient times, in the form of blocking fortresses during a siege, blocking access to food and water.

With the growth of technical capabilities and the diversity of economic relations in the modern world new forms of resource confrontation in the form of transport, energy and even water blockade are emerging, leading to the ecocide of entire territories nowadays. A typical example of such actions is the attempt to divert the waters of the Jordan river from Israel, which served as one of the causes of the "six-day war" in 1967.

The potential use of climate weapons can be considered very close to the resource confrontation in terms of characteristics. There is no confirmed information about its presence, there are only assumptions about its development by some countries [14]. However, such weapons would be an ideal means of conducting a "hybrid" confrontation.

Analyzing the history, we can conclude that modern "hybrid

wars" are not a new phenomenon, but only a continuation of the previously used various forms of interstate confrontation. Such war differs by the complex use of various forms of military and non-military confrontation; significantly increased technological capabilities for the implementation of certain forms of hybrid actions; the scale determined by the globalization of the modern world. Hybridity is a property of any war, since the warring parties necessarily strive to use all the forces, means and methods of warfare at their disposal.

Today, the concept of "hybridity" reflects significant changes in the nature of modern wars, which are diverse, and military operations in the event of a conflict with a high – tech enemy will be conducted both in the already familiar environments – on land, in the sea and in the air, and in new areas-space and cybernetic. Another important characteristic of modern wars is multi-dimensionality, which involves a combination of information, military, financial, economic and diplomatic influence on the enemy in real time.

Conclusions

The analysis allows us to draw certain conclusions:

1. A "Hybrid" conflict can be waged without entering the phase of direct military confrontation, without passing the level of "proxy" war.

2. The Variety of "hybrid" actions shows that "hybrid" wars differ in goals, methods used and the degree of intensity [15].

3. The Widespread use of "hybrid" methods of confrontation in the economy, socio-political sphere and cyberspace, in the modern globalized world, has a destructive impact no less than local armed conflicts.

4. Effective measures to counter the hybrid war to the present time has not been developed [16, 17].

5. Features of "hybrid wars", the frequency of their occurrence, call on the armed forces of all States that are expected to pursue an independent policy, to clarify the structure of the armed

forces, methods of their use, adjustments of guidelines in the sphere of national security and defense.

First of all, taking into account the peculiarities of the transition of the "hybrid" confrontation to the power phase: clarifications in terms of increasing the readiness of the armed forces to act in peacetime, without declaring war, to expand the autonomy of military units and increase the independence of their commanders in decision-making. New concepts and methods of conducting "hybrid wars" have been developing very quickly, which requires a revision of the classical military methods of forecasting and planning both offensive and defensive operations.

References

1. International Institute for Strategic Studies (2015), *The Military Balance-2015*, available at: https://cutt.ly/wjML8Mk (accessed 25 January 2021).
2. Markus, Dzh. (2014), "*Gibridnaya voina Putina-golovnaya bol' NATO*" [*Putin's hybrid war is a NATO headache*] available at: https://cutt.ly/7jMZnc5 (accessed 25 January 2021).
3. Mumford, A. (2013), *Proxy Warfare*, Polity Press Publ., Cambrige, 180 p.
4. Hoffman, F.G. (2007), *Conflict in the 21-st century: The rise of hybrid wars*, Potomac Institute for policy studies, Arlington, 72 p.
5. McCulloh, T. and Johnson, R. (2013), Hybrid Warfare, *JSOU Report*, 4(13), 137 p.
6. Nemeth, W.J. (2002), *Future war and Chechnya: a case for hybrid warfare*, Naval postgraduate school, 100 p.
7. Simpson, E.M. (2005), *Thinking About Modern Conflict: Hybrid Wars, Strategy, and War Aims*, Midwest Political Science Association, Chicago.
8. Dugan, J.C. (1998), *Elusive armies and invisible hands: combining conventional and guerrilla forces from 1776 to the present*, Naval Postgraduate School, Monterey, 164 p.
9. Walker, R.G. (1998), *SPEC FI: The United States Marine Corps and special operations*, Naval Postgraduate School, Monterey, 117 p.
10. Vypasnyak, V.I., Tikhanychev, O.V. and Gakhov, V.R. (2013), "Kiber-ugrozy avtomatizirovannym sistemam upravleniya" [Cyber threats to automated control systems], *Bulletin of the Academy of Military Sciences*, 1(42), pp. 103-109.

11. Sharp Gene (1973), *The Politics of Nonviolent Action*, Porter Sargent, Boston, 72 p.

12. Harsin, J. (2015), Regimes of Posttruth, Postpolitics, and Attention Economies, *Communication, Culture & Critique*, 8(2), pp. 327–333.

13. Parmar, I. (2012), US Presidential Election 2012: Post-Truth Politics, *Political Insight*, vol. 2, pp. 4–7.

14. Ginestet, A. (2019), *Climate-security nexus: System Theory of Violence and Complexity Architecture*, COBAWU Institute, Wuppertal, 8 p.

15. Fadeev, A.S. and Nichipor, V.I. (2019), "Voennye konflikty sovremennosti, perspektivy razvitiya sposobov ikh vedeniya. Pryamye i nepryamye deistviya v vooruzhennykh konfliktakh XXI veka" [Military conflicts of our time, prospects for the development of methods of their conduct. Direct and indirect actions in armed conflicts of the XXI], *Military Thought*, vol. 9, pp. 33-41.

16. Mack, A. (1975), Why big nations lose small wars: the politics of asymmetric conflict, *World Politics*, Vol. 27, No. 2, pp. 175-200.

17. Neimatov, A.Ya. (2016), "Sovremennye tsvetnye revolyutsii v kontekste nauchno-tekhnologicheskogo podkhoda" [Modern color revolutions in the context of a scientific and technological approach], *International Relations*, vol. 1, pp. 106 –110.

Dmitry Viter
Doctor of Philosophical Sciences, Senior Researcher
Leading Research Fellow of the Centre for Military and Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org//0000-0002-7330-1280

MILITARY AND NON-MILITARY FORCES AND METHODS OF WARFARE IN THE HYBRID WAR: THE THEORY OF SPECIAL OPERATION

The military and unmilitary forces and methods of warfare in the hybrid war in aspect of the special operation theory' framework considering. The ways of informational and psychological impact to the enemy in contemporary warfare on the theory of special operation and deterrence theory basis are defined. An actuality of need to rethinking the main principles and approaches of SO' theory, links of it with deterrence theory and really practice of contemporary warfare, which determines a new methods of influence to enemy as a way of contemporary warfare main goals achievement is accented.

Keywords: *deterrence theory, forms of warfare, hybrid war, informational and psychological operation, special operation, theory.*

Introduction

Problem statement. Ensuring the military security and protection against aggression by the use of exceptionally armed forces in the present conditions of warfare and military operations confronts with the problem of the use of forces and means of information and psychological warfare, which are characterized by greater activity, along with conventional forces and means of ensuring the victory over the enemy. The speed of operative response to changes in the combat environment, as a factor of victory, necessitates the creation of a situation in which the suppression of the enemy troops (forces) morale spirit, which is integral to its physical destruction, is ensured. Success in the effective planning

and conduct of information and psychological operations (IPO) guarantees the keeping of a large part of own forces and means that involved in military operations. The tasks that solving in the framework of the psychological operations should take into account the main priorities of the domestic and foreign state policy, for providing on the territory of conducting all-military operations and warfare conditions, under which the troops (forces) of the enemy and the local population will be subject to constant influence of significant demoralizing factors. This implies expanding the sphere of IPO, which should cover political, socio-economic, cultural, religious features of specific territories where military, special operations (SO), stabilization actions are planned or carried out. In fact, this all are the part of sphere that consider by the deterrence theory in aspect of preparing to war. Coordination of it (special actions) is important question that is in sphere of SO' theory in contemporary context of military and unmilitary forces and methods of warfare in the hybrid war.

The analysis of recent researches and publications. The "classical" theory of special operations pay attention to the special operations forces (SOF) gain the advantage when they have a simple plan, carefully concealed, realistically rehearsed and executed with surprise, speed and purpose and this advantage is tenuous however, and is subject to the frictions of war [1]. But that theory does not cover the full range of SO; specifically it fails to address the indirect component of SO, unconventional warfare. In this case the theory of relative superiority has a sense, because indirect relative superiority, as object of that theory, is achieved when a counter state gains and maintains a decisive advantage over a state in an armed political struggle. W. McRaven argued that can obtain relative superiority through the use of six principles of indirect offensive operations that are "applicable across the spectrum of special operations" [2, p. 3]: security, networking, purpose, indoctrination, influence, and agility [1, p. 11].

R. Modigs think that the SO are distinguished from unconventional operations and strategic military intelligence operations. In this aspect a viable EU Special Forces concept must,

first of all, have a strategic utility to conduct Special Operations but not Unconventional Operations [3].

H. Yargerthink that future warfare would be all irregular [4, p. 8] and a special operations may include unconventional warfare, counterterrorist operations, collective security, psychological operations, and civil affairs measures [4, p. 18]. In this context he argued that "the form of warfare is the tactical and operational art – the organization, technology, and doctrine. Form changes as necessary in response to the value of the reasons for conflict and the interaction of the parties involved" [4, p. 30].

R. Spulak, developing the theory of SO, advances a concept for enhancing the rapid innovation that enables SOF to stay ahead of our adversaries on the battlefield [5]. He suggests that innovation can occur in science and understanding, new tools and technology, and new ways of performing the mission. As result, SOF must learn to comingle these three areas in order to speed up the process of innovation to bring new concepts quickly to bear at the point of the spear [6].

Innovational potential of the SO' theory development is also opening in a cybernetic approach to special operations, when the central element is the delineation of a "cybernetic advantage", which amounts a relative differential in the speed, accuracy and effectiveness of implementation of decisions made by opposing commanders, and the efficiency of conversion of combat potential to combat power. Also surveys the use of special operations to achieve key foreign policy objectives and the ability of combat simulation to provide answers to potential questions and to stimulate queries to subjects that operators may not have considered germane to the outcome of the mission [7].

Purpose of the report. The military and unmilitary forces and methods of warfare in the hybrid war in aspect of the theory of SO' framework considering.

Main part

The theory of SO pay main attention to forms of a geopolitical interests ensuring, a geopolitical confrontation, the war in geopolitical sphere and a special methods of warfare. The theory

of SO is differentiated by the orientation to the goals and means of achieving them in the process of complex influence on objects throughout the depth of the enemy's rear area. Such influence is ensured and made possible by [8]:

– the creation and using of small and effective means of defeat, which significantly expand and increase the loss of the enemy, in the case of the special methods use provided;

– the using of special means of removing combat formations in the rear of the enemy;

– vulnerability of objects in the enemy's rear area;

– dependence of troops (forces), that located on the line of direct contact of the parties, on the state of command of the troops, arms and comprehensive ensuring;

– improving the technical capabilities of large-scale information and psychological impact on the troops (forces) and the enemy population;

– efficiency, owing to the low degree of vulnerability, sabotage and sabotage-intelligence formations in the case of conventional methods of warfare using.

That conditions, in itself specifics, are characterized by the mass using of certain specific means in carrying out of SO. Increasing of that conditions as a result have a fact the contemporary theory of SO focuses on the implementation of the idea about comprehensive impact on the entire depth of the enemy's rear zone by means of defeat, Special Forces, air and naval troops, forces and means of psychological struggle to deprive the enemy of material and moral ability and desire to fight, and the further struggle. That is why, according to the theory of SO, the basic principle is to overcome the enemy's resistance by depriving him of his ability to fight. This principle defines the specific ways and methods of achieving the goals that focusing on undermining the military, information, socio-economic, scientific and technical, moral potential of the state and its armed forces by means of SO. Such actions are essentially hybrid, synthetic character, encompassing the essence and content of SO as a set of actions aimed at reducing the available and possible potential of

the enemy in various spheres of society, state and personality (religion, culture, worldview, education, art, language, traditions, education) life. But in whole, the principles of SO reflect the specific patterns of warfare by the special methods. The basic principles of SO are related to the precise selection of special goals from the multivariate list of special action goals, the definition of special tasks and their accomplishing. The basic principles determine that the main efforts should focus solely on the weakest and most vulnerable place in the system of comprehensive ensuring of the enemy. The basic principles also point to the priority of disorganization and disorientation of the enemy in the real environment in order to diversify his efforts. And the basic principles of SO' theory implementation is connected with such basic directs of warfare by special methods, such as the demoralization of troops (forces) and the enemy' population, ignoring restrictions, the variability of SO.

The demoralization of the troops (forces) and the enemy population implies inflicting, as a result of the information and psychological struggle, the information and psychological defeat for the troops personnel and the population of the enemy in order to break his will to continue the armed struggle and resistance [9]. The importance of this task is determined by the fact that the effectiveness of information and psychological combat in contemporary warfare is higher than the armed struggle, because significantly increases the number of conflicts that only allow for the open use of military force by the parties of the conflict. This task must be taken into account when planning, organizing and conducting the SO in the rear of the enemy, or in enemy' controlled territory.

In that case a priority is the removal and disregard of any restrictions on the decisions of the commander and the actions of unit personnel in point if view of all elements of the operational environment using in order to succeed in completing the task, that determines the methods and means which necessary to succeed in conducting a SO. In fact, takes on especially significance a designing and calculating a large number of variants for a SO conducting can't be attachment to time and place, because taking into account the

invariance of the situation in the rear of the enemy, the randomness of conditions and the multiplicity of available connections in the infrastructure are significantly reduce the planning capabilities and detailing of each particular SO.

In point of view the theory of SO the information potential of the parties in the conflict (in some cases it even refers to the “law of the dependence of the course and the outcome of the war on the ratio of the information potentials of the parties in the conflict” [10]) becomes a priority in view of the new forms of war development, when the warfare gives way to an information one. It is the information fight that sees the ability to achieve military and political goals – in ideally case without an open warfare. Such information war is actively used by influencing to the personnel of the armed forces and the enemy population. Such war is waged always, even in the absence of direct armed opposition, and, essentially, is an information-psychological struggle. In the context of such struggle, coherence and coordination within the framework of the sole purpose of a SO of information-psychological and law-enforcement special actions (SA) are an important issue.

There are two main directs [8]. A first is connected with that the purpose of information-psychological SA is to change the behavioral and emotional attitudes of the armed forces personnel and the enemy population on certain issues in the direction that determined by the overall strategy of achieving the military and political goals of the struggle. This purpose is realized at the same time as taking measures to counteract the propaganda of the enemy, his attempts and efforts to exert information-psychological influence on the armed forces personnel and the population.

Contradiction point of view taking into attention that the purpose of law-enforcement SA is to protect the constitutional system and state order of the country, property and rights of the state and its citizens abroad, to ensure the fulfillment by the state and foreign state (states) of their obligations to protect and respect human rights against the citizens of their state, to ensure the actions of the armed forces in sphere of fulfillment of resolutions of international and domestic law

enforcement agencies. American position in that question is "CI activities are conducted to detect, identify, assess, exploit, andcounter or neutralize the threat posed by foreign intelligence entities, or by individualsengaged in espionage, sabotage, or terrorism. CI identifies vulnerabilities and assesseshostile forces capabilities to target military operations. CI activities may also provide formalliaison with HN, intelligence, law enforcement, and security activities to assist operationsand provide force protection support to joint forces" [7, p. 74]. This purpose involves the use of the armed forces and SO forces units of the whole complex of SA (including armed) in the territory of their own and foreign country. Due to this broad understanding of he armed forces and SO forces tasks, the defense doctrine of the state should be guided by the need to ensure the national security review of the "defensive" nature of its own armed forces actions, because the combat activity on the enemy' territory becomes one of the main elements of the state defense. Functionally, the achievement of the law-enforcement SA goal is able to provide the psychological superiority over the enemy, to form in him a stable confidence in the lack of full protection in his own territory, and in his own deep rear. At the same time, the functional focus of law-enforcement in the areas of armed conflict, in the places of real or potential danger to the state should extend to the protection of the economic, financial and other national interests of the state. Geopolitical realities and interests, the attainment of geopolitical preferences: today are most often provided to certain states through the application of law-enforcement SA to the enemy.

That main directs in the theory of SO forming a content of common approach to military information support operation (MISO, which from 2010 changed by self the traditional Psychological Operations (PSYOP)). The purpose of the changes is to ensure the asymmetry of the modern wars and fighting ways of waging in the direction of the PSYOP from tactical to strategic level of application. The possibility of integrating the PSYOP into the REI' units as a separate path of the PSYOP development is consider [11]. Need to make changes in the approach to theoretical thinking and practical

implementation of basic principles and approaches to SO be determined by the fact the low effectiveness of military operations at the tactical level in combat deployment of units that engaged in stabilization actions. That has led to the need to organize and deploy the mobile teams in civilian specialists of informational enduring, advisers and militaries, first at all, in the field of information infrastructure and communications renewal, solving the social problems of the local population, counteracting the situation of destabilization, including the ensuring the regional security, supporting the incumbent government, and assisting to local government in outreach (in sphere of information and propaganda) activities. In result was formed other level of SO representing – strategic level. That is why R. Spucal makes an accent to "the characteristics of SOF include strategic initiative, integrated operations, unconventional operations, certain access, and relative superiority" [6, p. 40].The strategic level of the IS provides for active and comprehensive involvement of the media representatives in fulfilling their tasks (from covering necessary information in the content and orientation of the leading mass media to securing journalists in the divisions directly involved in hostilities). In addition to comprehensive coverage of the information and the formation of a positive attitude of the world community to hostilities and military operations, it provided an opportunity to create a controlled positive image of the troops in the media, avoiding the appearance of blatantly critical information units by providing "vision of events from within" [7]. The empathic method in this case is also effectiveness in terms of influencing the individual consciousness of the media, which makes a possible to develop the new methods of IPO' planning and realization. The innovative methods (such as the use of social media technologies) help to improve IPO at a strategic level and ensure of it effectiveness.

Conclusions

The changes in structure, organization, methods, means of military-political confrontation, changes in the content of war and ways of achieving the goals, changes in understanding of the

variability of the violence forms, that can be applied to the enemy in order to win – a decisive achievement ting military and political objectives without the use of direct armed violence – arising informational, cultural, economic, ideological, social and others sphere of public life as object of influence. The priorities of such forms of large-scale organized influence on the enemy are the logical conclusions in that case. In fact, any sphere of human activity can become the object of such influence, and turn into a "battlefield" in order to achieve the main actors of geopolitical confrontation of their goals. That actualizing need to rethinking the main principles and approaches of SO' theory, links of it with deterrence theory and really practice of contemporary warfare, which determines a new methods of influence to enemy as a way of contemporary warfare main goals achievement.

References

1. McRaven, W.H. (1993), *The Theory of Special Operations: thesis*, Naval Postgraduate School, Monterey, California, 604 p.
2. McRaven, W.H. (1995), *Spec Ops: Case studies in special operations warfare: theory and practice*, Presidio Press, Novato, 432 p.
3. Modigs, R. (2004), *Special Forces capabilities of the European Unionmilitary forces*, School of Advanced Military Studies, Fort Leavenworth, 94 p.
4. Yarger, H.R. (2013), *21st Century SOF: Toward an American Theory of Special Operations*, The JSOU Press, MacDill Air Force Base, 83 p.
5. Spulak, R.G. (2007), *A theory of special operations – The origin, qualities, and use of SOF*, JSOU Press, HurlburtField, 45 p.
6. Spulak, R. (2019), *Innovate or Die: Innovation and Technology for Special Operations*, JSOU Press, HurlburtField, 80 p.
7. U.S. Department of Defense (2014), *Joint Special Operations Joint. Publication 3-05*, Washington, 183 p.
8. Kiras, J.D. (2006), *Special operations and strategy: From World War II to the War on Terrorism*, Routledge, New York, 230 p.
9. Huth, P.K. (1988), *Extended Deterrence and the Prevention of War*, Yale University Press, New Haven, 227 p.
10. Smith, Robin R. (1996), *The utility of high resolution modeling in Army Special Operations Aviation mission planning: thesis*, Naval Postgraduate School, Monterey, 143 p.
11. Snyder G.H. (1961), *Deterrence and Defense: Toward a Theory of National Security*, Princeton University Press, Princeton, 294 p.

Antonina Voloshenko
Doctor of Economic Sciences, Associate Professor
Chief Researcher of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-2087-3365

CORRUPTION AS AN ELEMENT OF HYBRID WAR: WAYS TO PREVENT AND MINIMIZE

The analysis of the content of factors and the main areas of application of corruption as an element of a hybrid war is carried out. It has been proved that under war conditions, corruption takes on a new meaning: ideological, since the ultimate goal in this case is to change the state structure. A review of the negative consequences of corrupt practices, among which the most resonant for national security are identified: a decrease in combat effectiveness due to the impact on the moral and psychological state of military personnel, a decrease in confidence in the troops and state power among the population, harm to the economic interests of the state and the international image of Ukraine. The ways of preventing and minimizing corruption in the legal, informational and cultural plane are proposed.

Keywords: *corruption, hybrid war, national security, destabilization.*

Introduction

Problem statement. The rapid development of technology has changed the conditions of warfare, in which the emphasis has shifted from the usual hostilities to non-military methods of pressure on the enemy, primarily with the help of political (diplomatic), economic and humanitarian elements. Particular attention is paid to "asymmetric measures", in which scientists include: the activities of special forces, support for the internal opposition and collaborators, as well as an increase in targeted information impact on the object of the attack [1].

Hybrid wars are not a discovery of our time, they have existed for centuries, although no specific period has been defined that would cover them [2]. According to recent studies and publications, the concept of hybrid war is widely used as a combined, integrated military-political and economic confrontation in the form of a statusless, often latent conflict.

Corrosion of the central state power is a characteristic that is decisive in "new wars", because the aggressor country uses the shortcomings of the state chosen for aggression to destabilize the situation and weaken it. And it is corruption that is a threat to the rule of law and a violation of civil and political rights and freedoms. Corruption has long been used during wars to gain advantages, but recently, some governments - primarily China and Russia - have turned it into a global weapon.

A characteristic distinguishing feature of conflict and post-conflict states from stable rule of law and democratic states is the degradation or complete destruction of state and public mechanisms for ensuring basic human rights, a significant increase in the level and scale of the spread of corruption.

In Ukraine, this negative phenomenon is of a systemic and institutional nature. The consistency of which is manifested in the penetration into almost all sectors of the national economy, a complex interweaving of corruption networks, the emergence of which is possible only when the structures of state authorities, administration and society are merged. Therefore, the issue of defining corruption as an element of hybrid warfare is relevant and debatable.

The analysis of recent researches and publications. Studies of various aspects of hybrid warfare are highlighted in the works of such scientists as V. Gorbulina [3], M. Deland [4], O. Duz`-Kryatchenko [5], M. Kaldor [6], Ye. Magda [7], G. Pocheptsov [1], A. Sirotenko [8], F. Hoffman [9], etc.

The influence of corruption on the politics of European countries and the United States is studied in the works of S. Wessier [10], L. Diamond [11], F. Zelikov [12], E. Edelman [12], and others.

Geopolitical and economic transformations on a global and local scale are accompanied by an increase in corruption actions of a strategic direction, respectively, this phenomenon as an object of scientific research is gaining more and more attention.

Purpose of the report to argue the need to consider corruption as an element of hybrid war, and also to determine the main ways to prevent and counteract it.

Main part

The issues of countering the threats of a hybrid war for Ukraine are topical, since covert hostile actions on the part of Russia were carried out for a long period through political and economic pressure, influence on personnel policy, as well as through energy aggression and a trade war. On February 20, 2014, they switched to an open form of armed aggression during the military operation of the Armed Forces of the Russian Federation to seize part of the territory of Ukraine - the Crimean Peninsula, and later, in April 2014, the occupation by Russian regular troops and illegal military formations controlled by the Russian Federation of certain areas of Donetsk and Luhansk regions of Ukraine.

Armed aggression is only one element of Russia's hybrid war against Ukraine. Other elements are:

– propaganda based on lies and substitution of concepts;

– trade and economic pressure;

– energy blockade;

– terror and intimidation of Ukrainian citizens;

– cyber attacks;

– the categorical denial of the very fact of the war, despite the presence of many irrefutable evidence;

– taking advantage of pro-Russian forces and satellite states;

– accusing the other party of their own crimes [13].

In the specified list of elements of a hybrid war given by the Ministry of Foreign Affairs of Ukraine, there is no such fundamental and powerful method from the arsenal of the special services as corruption, because money allows you to bribe people, make them

obligated and dependent, and therefore vulnerable.

The ultimate goal of economic corruption is to obtain illegal income, political − to achieve power, in a war, corruption takes on a new meaning: ideological, so strategic task in this case is to change the state structure.

Ukraine is called the victim of Russia's hybrid war. But Russia is actively applying its methods of soft influence to other democratic states, first of all, we are talking about operations to form a pro-Russian lobby among European politicians with the help of corruption schemes, bribery, blackmail [10].

The Russian export of corruption erosion today is the most effective instrument of creeping influence, which can include various assistance (primarily financial) to pro-Russian political forces in Europe. An example of this is the well-known facts of Russian financing of the French National Front party.

In November 2014, the popular German newspaper Bild accused the Kremlin of creating over a long period of time a network of right-wing populists in Western Europe, in particular by providing loans to them through "banks linked to the secret services" [14].

American experts also point to the fact that state-owned companies and illegal financial flows are used for direct penetration into Western governments and institutions. Scientists note that, knowingly or unknowingly, Canadian banks, British real estate firms, American lobbyists and PR-companies today serve the interests of authoritarian regimes. As noted in a 2016 study by the Center for Strategic and International Studies: "Russian influence is focused on weakening the internal unity of societies and reinforcing perceptions of the dysfunction of the Western democratic and economic system. This happens by influencing the institutions of democratic governance and undermining them from within" [12]. Larry Diamond, an American leading expert on political sociology and democracy, sees the main internal threat to democracy, which makes it vulnerable to destruction by external forces, in large-scale endemic corruption [11].

In a hybrid war, for the sake of imposing one's own will on another state, all kinds of vices of the state are used, therefore, in

order to achieve the set goal, an attack occurs on the weak points of society [15]. Thus, the high level of corruption of the Ukrainian customs officers led to the fact that, according to the Security Service of Ukraine, the Russian Federation used the channels of commodity smuggling in order to transfer weapons in the east of Ukraine and Crimea at the first stages [16].

A study conducted by the Independent Anti-Corruption Committee on Defense Issues on illegal trade with the occupied Donbass showed that trade with uncontrolled territories was often interpreted as supporting militants. At the same time, the largest volumes of goods move to certain areas of the Donetsk and Lugansk regions (CADLO) with the assistance of individual military personnel and officials. Situations were monitored when between units, separately from each other, they contributed to the illegal movement of goods (CADLO), conflicts arose, including the use of weapons.A special threat to national security is the acquisition by illegal trade of a systemic nature, and, accordingly, the ramifications of corruption ties, thanks to which it has the ability to exist and expand. It was revealed that not only rank-and-file servicemen, but also middle-level commanders, intelligence officers and civil servants of various branches of government were involved in the machinations [17].

There are other attempts to influence national security through corruption, for example, a series of "projects" to destroy the Ukrainian state and its territorial integrity through "soft federalization." Within the framework of this project, it was planned bribing deputies of local councils by representatives of business to make decisions on the economic autonomy of territories, it is clear that the so-called "business representatives" are employees or agents of the Russian special services [16].

Scientists have proven that hybrid warfare is primarily a war with the population [1]. At the same time, due to its non-traditional nature, most people do not see it as a military threat. Confirmation of this is the statistical data of the sociological study "Corruption in Ukraine: understanding, perception, prevalence" conducted by the

National Agency for the Prevention of Corruption (NAPC) and the Anti-Corruption Initiative of the European Union. According to the survey, 69% of Ukrainian citizens consider corruption the second of the biggest problems in Ukraine, military actions in eastern Ukraine are considered a problem by 72.7% of Ukrainians. In addition, it was revealed that the majority of respondents do not have a clear understanding of what practices should be considered corrupt, and tolerates some of them [18].

Conclusions

We can determine that the negative consequences of corrupt actions are a decrease in combat effectiveness due to the impact on the moral and psychological state of military personnel, a decrease in confidence in the troops and state power among the population, damage to the economic interests of the state and the international image of Ukraine.

For Ukraine, effective countering corruption is a guarantee of support by international institutions, since it is anti-corruption reforms that are an indicator of the government's success and is a significant factor in providing economic and military assistance from the EU and the United States.

The issue of corruption as an element of a hybrid war must be considered both in the legal plane, since it acts as an instrument of subversive activity, and therefore poses a threat to national security, which requires the development of instruments of legal protection and counteraction, as well as information and cultural. Today, a significant part of society has an acceptable attitude towards corruption as a norm and does not understand its destructive impact on statehood. Accordingly, it is necessary to form a social culture through educational and information and communication activities to consolidate the affirmation of corruption as an element of hybrid war, both among the military and among the civilian population.

References

1. Pochepczov, G. (2017), "*Gy`bry`dnaya vojna: kogda naseleny`e okazuvaetsya cel`yu*" [*Hybrid warfare: when the population is targeted*], available at: https://cutt.ly/ (accessed 20 January 2021).

2. Kurban, O. (2016), "Suchasni informacijni vijny` v social`ny`x onlajn-merezhax" [Information wars in social online networks], *Informacijne suspil`stvo*, 23, pp. 85-90.

3. Gorbulin, V.P. ed., (2017), "*Svitova gibry`dna vijna: ukrayins`ky`j front*" [*World hybrid war: ukrainian front*], FOLIO, 496 p.

4. Delanda, M. (2014), "*Vojna v epohi razumnui mashy`n*" [*War in the era of intelligent machines*], Cabinet Scientist, Yekaterinburg, 338 p.

5. Duz`-Kryatchenko, O.P. and Pankratov, Ye.Ye. (2014), "Dosvid ta uroky` vnutrishn`ogo voyennogo konfliktu ta zbrojnoyi agresiyi proty` Ukrayiny" [Experience and lessons of internal military conflict and armed aggression against Ukraine], *Scientific Works of NAUO*, No. 4 (125), pp. 9–10.

6. Kaldor, M. (2012), *New and Old Wars: Organized Violence in a Global Era*, Polity Press, Cambridge, 268 p.

7. Magda, Ye. (2017), "*Gibry`dna agresiya Rosiyi: uroky` dlya Yevropy*" [*Russia's hybrid aggression: lessons for Europe*], Kalamar, 268 p.

8. Sy`rotenko, A.M. ed., (2020), "*Voyenni aspekty` proty`diyi gibry`dny`j agresiyi: dosvid Ukrayiny*" [*Military aspects of combating hybrid aggression: the experience of Ukraine*], NUOU, Kyiv, 176 p.

9. Hoffman, F.G. (2009), Hybrid warfare and challenges, *Joint Force Quarterly*, No. 52, pp. 34-39.

10. Vess`ye, S. (2016), "Merezhi Kremlya u Franciyi" (vy`tyag z kny`gy`) [Kremlin network in France], *National Security and Defence Journal*, No. 9-10 (167-168), pp. 98-108.

11. Diamond, L. (2019), *Ill Winds: Saving Democracy from Russian Rage, Chinese Ambition, and American Complacency*, Penguin Books, 368 p.

12. Zelikov, F., E`l`dman, E., Xarrison, K. and Gventer, S. (2020), "Kak gosudarstva prevratili vzyatki v oruzhie" [How states turned bribes into weapons], *Russia in global affairs*, available at: https://globalaffairs.ru/articles/podyom-strategicheskoj-korrupczii/ (accessed 6 November 2020).

13. The official site of Ministry of Foreign Affairs of Ukraine (2019), "*10 faktiv pro zbrojnu agresiyu Rosiyi proty` Ukrayiny`*" [*10 facts about Russia's armed aggression against Ukraine*], available at: https://mfa.gov.ua/10-faktiv-pro-zbrojnu-agresiyu-rosiyi-proti-ukrayini (accessed 5 November 2020).

14. Tiede, P. (2014), “Lassen Sie sich von Putin finanzieren, Herr Lucke?” [Do you let Putin finance you, Mr. Lucke?], *Bild*, 26 November, available at: https://cutt.ly/hj7EqGz (accessed 5 November 2020).

15. The official site of Radio Svoboda (2018), “*Novi texnologiyi i metody` gibry`dnoyi vijny` – ce vy`kly`k mizhnarodnij bezpeci*” [*New technologies and methods of hybrid warfare are a challenge to international security*], available at: https://www. radiosvoboda.org/a/ 29591806.html (accessed 1 November 2020).

16. The official site of aspi.com.ua (2020). “*Novy`ny` polity`ky`: Kreml` planuvav «m'yaku federalizaciyu» v Ukrayini*” [*Political news: Kremlin plans soft federalization of Ukraine*], available at: https://cutt.ly/Yj7EoeW (accessed 1 November 2020).

17. The official site of Independent Defence Anti-Corruption Committee (2017), *Crossing the line: how the illegal trade with occupied Donbas has undermined defence integrity*, available https://cutt.ly/Oj7EkF4 (accessed 25 October 2020).

18. The official site of National Agency on Corruption Prevention (2020), “*Korupciya v Ukrayini 2020: rozuminnya, spry`jnyattya, poshy`renist`*” [*Corruption in Ukraine 2020: understanding, perception, prevalence*], available at: https://cutt.ly/Ej7EvJj (accessed 1 November 2020).

Stepan Vozniak
PhD (Technical Sciences), Senior Researcher
Chief of the cell of Transformation and Integration Processes
in the Military Sphere of the Centre for Military Strategic Studies
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-9015-813X

Andrii Ivashchenko
PhD (Technical Sciences), Associate Professor
Leading Researcher of the cell of Transformation and Integration
Processes in the Military Sphere of the Centre for Military Strategic
Studies of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-8131-5463

Dmitry Fedianovych
PhD (Military Sciences), Senior Researcher
Chief of Department of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-9896-8655

Nina Andriianova
PhD (Political Sciences)
Senior Researcher of the cell of Transformation and Integration
Processes in the Military Sphere of the Centre for Military Strategic
Studies of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-7115-2445

INTERNATIONAL DEFENSE ASSISTANCE AS A WAY TO COUNTER HYBRID AGGRESSION

The issues of providing international assistance to Ukraine in the conditions of hybrid aggression of the Russian Federation are considered. It is determined that in the conditions of limited possibilities of the domestic defence-industrial complex, resources, personnel

training, military-technical assistance plays a significant role in resolving the conflict. Today, there are many types of assistance, from consultative to direct military assistance from partner countries and international security organizations. But little attention is paid to determining the effectiveness of this assistance. To determine the effectiveness of international assistance to Ukraine in the context of hybrid aggression, it is proposed to use a methodology based on known approaches to fuzzy set theory and cluster analysis. The effectiveness of assistance for different phases of modern military conflicts with signs of hybridity is calculated.

Keywords: *Assistance, methods, effectiveness, modern military conflict.*

Introduction

Problem statement. An analysis of the experience of resolving modern military conflicts (MMC) has shown that an effective way to stabilize the situation and restore peace is to increase the capacity of national defence forces to counter hybrid threats. But the capabilities of the national economy, defence-industrial complex is not always able to increase the capabilities of national defence forces. Obtaining foreign military assistance and attracting the capabilities of international organizations for security and cooperation as ways to counter hybrid threats is actual.

The analysis of recent research and publications. Studies conducted by Uppsala University (Sweden) have shown [1] that armed conflicts in which both parties receive support have a longer duration. That is, a balance of power is created in which neither side can successfully end the conflict (there are enough resources, there is an opportunity to rearm). At the same time, external support from one of the parties to the conflict (military means) can also reduce the duration of the armed conflict and speed up the negotiation process. Which confirms the statistical analysis of the data by the Military Balance – Institute's annual assessment of the military capabilities and defence economics of 171 countries worldwide [2].

Thus, it can be stated that there is a certain contradiction regarding the influence of external support of the parties to the

conflict. On the one hand, support can reduce the duration of an armed conflict by changing the balance of power in favour of one of the parties, and on the other hand can increase its duration by establishing a balance of power by the parties.

At the same time, military, military-technical assistance to the parties to the conflict plays a significant role. This is due to the limited capabilities of the domestic defence industry, resources, training and other factors.

Purpose of the report is to determine the effectiveness of international assistance to Ukraine in the context of hybrid aggression.

Main part

In 2014, when Russia unleashed its aggressive actions in Donbas and occupied Crimea, the United States provided Ukraine with military equipment to the value of more than $118 million.

After providing the first 330,000 field rations and equipment (body armors, medical kits, helmets, etc.), then-US President Barack Obama also expressed his intention to hand over $5 million worth of military equipment to the UAF, equivalent to 600 night-vision devices. At the same time, Russia provided $250 million to support illegal military formations in the East of Ukraine in the first two months alone.

The US allocated $ 175 million for Ukrainian defence in 2015. In particular, it refers to 130 armored vehicles, 5 boats for the Ukrainian Navy and radars [2]. The following types of radars were delivered to Ukraine:

AN/TPQ-36 – serves to locate firing positions of enemy mortars, guns, and MLRSs;

AN/TPQ-48 – serves to fight mortars; detection range – 6 km;

AN/TPQ-49 – serves to fight mortars; detection range – 10 km.

The United States also provided Ukraine with a $7.6 million-worth military field hospital.

The hospital consists of four tents and can provide medical care to three thousand servicemen at a time. The hospital can be deployed

within 24 hours and can operate autonomously for up to 10 days.

In 2016, the US allocated $335 million for Ukrainian defense: 2,500 night vision devices, 40 ambulances and 14 radars were procured for this amount. $12 million was also spent on drones for the UAF. A shipment of RAVEN RQ-11B unmanned aerial vehicles was delivered. Each of the UAVs comes with a video surveillance camera and a night vision device. A UAV weights 1.9 kg, its cruising altitude is up to 150 m, range – 10 km, flight endurance – 1–1.5 hours. It has an electric motor and cruising speed of 50 km/h. Given the price of the order (about $120,000 – $150,000 per 1 kit of such devices), the US Army has delivered 24 kits (with 3 UAVs each), i.e. 72 UAVs and additional equipment for the claimed amount of the contract.

In 2017, the US allocated $560 million for Ukrainian defence to provide the UAF with the necessary equipment. In particular, it refers to lethal weapons that the US supplied to Ukraine in 2017. After a shipment of 12.7 mm Barrett M82 and M107 calibre sniper rifles for the UAF and the National Guard, the US made a new delivery of PSRL-1 hand grenade launchers. Cargo planes also transported additional radar kits from the US to Ukraine. Besides, Ukraine received new ambulances and diving equipment.

In 2018, the US allocated $350 million to strengthen Ukraine's defense. In February, the US government handed over 2,500 night-vision devices to the UAF for a total amount of $5.8 million. In April, long-awaited "Javelin" anti-tank missile systems – one of the most expensive ATGM systems in the history of such systems design and use (about $ 100,000 each) – arrived in Ukraine.

The United States also handed over two radars, small arms, ammunition, and mine detectors to Ukraine.

In September 2018, Ukraine received two boats ("Drummond" and "Cushing") free of charge. Additional costs ($10.1 million) for depreservation, installation of the removed systems, maintenance, crew training and transportation to Ukraine were paid by the MoD of Ukraine.

Negotiations to hand over four more boats (also free of

charge) to Ukraine are being held. It is only necessary to decide on upgrade of the radioelectronic weapons and other technical issues.

The Ukrainian Navy plans to form a division of six "Island"-class boats which will be able not only to control the short-range maritime zone, but also to go to the Mediterranean to support NATO ships.

The boats can be equipped with a variety of weapons: from minesweeping modules, which is now critical for Ukraine, to the American "Harpoon" or Ukrainian "Neptune" ASCMs, which are being tested.

In August 2019, the state enterprise "Shipbuilding Research and Design Center" began to develop an option to upgrade "Island" patrol boats on its own initiative. The final upgrade version will be adopted after the Ukrainian Navy receives practical experience in their use.

A total of 63 radars (up to $1.5 million each) including 13 AN/TPQ-36, 20 AN/TPQ-48, and 30 AN / TPQ-49 kits were delivered in 2014–2018.

In 2019, the US allocated $250 million to strengthen Ukraine's defense. The US took a new step: it drafted a law which would allow to hand over surface-to-air and anti-ship missiles and coastal defense weapons to Ukraine.

In 2020, the planned military assistance to Ukraine will increase to $300 million of which $100 million may be spent for lethal weapons.

Therefore, Ukraine received US assistance totalling more than three billion dollars. From 2014 to 2019, the value of only military equipment handed over to Ukraine (night vision devices, body armors, vehicles, radars, armored vehicles, boats for the Navy, etc.) totalled more than $1.3 billion. Modern "Javelin" anti-tank missiles have been delivered to Ukraine since last year. The amount of assistance to the UAF totals about US $361 million.

The US Congress is considering a new draft law to provide support to Ukraine to defend its independence, sovereignty, and territorial integrity, and for other purposes which envisages military

assistance, including lethal weapons, means of cyber defence and a status of a major non-NATO ally until Ukraine becomes a member of the Alliance [3].

If the US had granted Ukraine the major non-NATO ally status, Ukraine would certainly not have received security guarantees. But under Section 2350-a of the United States Code, Ukraine would have been given an opportunity to participate in Pentagon contracts outside the US; to conduct joint research, including related to counter-terrorism; and to carry out joint research and development with the United States in favor of national defence. Under section 2321-k, Ukraine would have had a right to receive depleted uranium armour-piercing munitions; to place US military stocks on its territory; to organize and finance military exercises together with the USA; to use US military assistance for commercial lease of certain categories of military products; to rent components and equipment for joint R&D; to promptly acquire American licenses for commercial satellites, their technologies and components [5]. The above list does not include issues of countering Russian hybrid aggression, but it is another achievement among many others which allows for more stable defence against prolonged military pressure from the RF. It is worth fighting for this achievement without losing the sense of reality. A decision of the US President is enough to obtain the status of a major non-NATO ally. Under certain circumstances, Ukraine can obtain it as quickly as Brazil in its day. But the decision will not be effective if the time for its adoption is too long, as it happened with Afghanistan. Granting the status of a major non-NATO ally corresponds to the United States' own understanding of its far-reaching interests, but another attempt to obtain such a status expands Ukraine's opportunities for military cooperation with the US anyway.

According to NATO 2010 Strategic Concept [5], the Alliance focuses on three main tasks to ensure defence and security of its members:

– collective defence in accordance with Article 5 of the effective NATO concept on the obligation of member states to assist

each other in case of an attack on any of them;

– crisis management in accordance with the effective NATO concept envisaging integrated use of appropriate political and military instruments at all stages of a conflict: at its emergence, settlement, and recovery;

– ensuring security through cooperation and promoting liaison with other international organizations and non-NATO countries in the following areas: strengthening arms control, promoting the non-proliferation regime, continuous expansion process through an "open door" policy, and improving the system of partnerships.

The NATO Summit in Wales (UK) has determined another line of its work aimed to strengthen security and defence capabilities of non-NATO partner countries. A new initiative is called "Security Force Assistance" (SFA) [6].

Summing up the two-year outcome of the SFA's implementation, the Warsaw Summit communiqué stated that the SFA allowed to strengthen NATO's role in ensuring a comprehensive approach to security and stability in the current environment by supporting security and defence capabilities in its partner countries.

To implement its new initiative, NATO has adopted a number of guiding documents.

According to the guiding documents, the SFA means the ability "to train and develop national forces in crisis areas" so that "national authorities of partner countries may build their capabilities to maintain effective security without international assistance" [6].

The SFA includes "all NATO actions that develop, improve or directly support the development of national security and defence forces and their associated institute") [6]. The SFA covers all activities aimed to develop and prepare national security and defence sector. It is conducted at the tactical, operational, strategic and military-political levels and envisages advisory assistance to all: from a platoon to a ministry.

In a broader context, the SFA, although militarily oriented,

includes political, economic, informational, legal and other mechanisms of preventing modern military conflicts. The NATO leadership and individual NATO member countries have taken a range of practical steps to implement the SFA in Ukraine.

Particular attention is paid to the development of UAF Special Operations Forces capabilities. The real special forces operational capabilities to perform important tasks, including in hybrid conflicts, are taken into account. Servicemen of SPECOPS units are trained from the perspective of general specificity of the use of these units (groups) in achieving specific military-political and military objectives. It includes destruction of enemy's strategic facilities, its nuclear-missile and missile weapons, electronic reconnaissance, organizing guerrilla movements, sabotage, and elimination of key state and military leaders of the opposing side. Advanced methods and ways to perform special operations are implemented with due account for the experience gained during military conflicts. Attention is paid to the principles of conducting information and psychological operations, arranging propaganda, misleading the enemy, informing civilian population and discrediting opposing side's authorities.

Multinational exercises are held annually to solidify the results of combat training achieved by the partner countries' formations, as well as to determine the degree of their readiness for combat operations in modern conditions. Exercise scenarios usually imply emergence of a crisis situation in a conditional region which requires an intervention of NATO forces to be resolved.

In addition to assistance in personnel training on national territory, the SFA provides an opportunity to send UAF servicemen to educational establishments of NATO countries. Military and civilian specialists of the security and defence sector is trained in: international and national security, information and cyber security, peacekeeping operations, intelligence, military medicine, staff and engineering preparation, advanced training of military police officers, training of junior command staff, foreign language studies, training of personnel specialists, etc.

Partner countries' servicemen are actively involved in NATO joint operational and combat training on the territory of NATO member countries. During these exercises, considerable attention is paid to arranging workflow of the joint headquarters to fully support actions of a multinational formation [4].

SFA events (including exercises with ground, air, naval, air-assault, and special operations forces and the National Guard) lead by advisers allow to:

– increase professional preparedness of servicemen, first of all, from all-arms military formations, air-assault brigades and marines;

– develop capabilities of partner countries' special operation forces, as well as special units of other security and defence sector structures using the experience of the armed forces of NATO member countries;

– ensure permanent presence of a contingent (in average from 500 to 900 servicemen of the Allied Forces as advisers and instructors) in the territory of the partner country.

An issue of improving the regulatory framework remains relevant. The legislation should allow to significantly increase, if necessary, the number of foreign military advisers (up to several thousand for the entire duration of an SFA operation) [4].

To optimize international support for more effective coordination of efforts, qualitatively assess the existing and further assistance to Ukraine, assess the effectiveness of international and coalition counteraction to the hybrid aggression (which consists of providing a wide range of assistance to the country which is countering against the hybrid aggression) a method based on cluster analysis and fuzzy set theory approaches is proposed [7; 8].

The method aims to provide the Ukraine security and defence sector structures as well as international and regional security organizations with a tool to assess the effectiveness of various ways of assistance aimed to resolve modern military conflicts, including with the signs of hybridity [9].

In the first block, a list (a database) of modern military conflicts

is formed. The method uses conflict indicators obtained from international security organizations, research canters and institutes as the input. If a part of input data is missing, an expert survey (a questionnaire according to the Delphi method) is conducted.

Based on this information, the second block clarifies sets of conflict development phases (stages). Next, the whole set of phases (stages) is divided into clusters according to an algorithm. Accomplished procedures of the block result in a clarified set of modern military conflicts development phases (stages) grouped into clusters of similar phases.

The third block compares the set of ways of assistance in resolving a conflict with its specific phase and assesses their effectiveness for its prevention. The result is a function which shows the effectiveness of each way (format) of assistance depending on the modern military conflict phase (stage).

The method has been tested on the basis of conflicts that have been taking place since 2000: Iraq (2003-2011); Afghanistan (since 2001); Chechnya (1999-2009); Georgia (2008); Libya (2014-2018); Syria (since 2011); Ukraine (since 2014); Yemen (2014-2015); Syria (since 2015); Islamic State (since 2014) .

The most significant ways (formats) of assistance from international security organizations are: military assistance (MA); special intelligence (SI); direct actions (DA); annual national programs (ANP); force planning and evaluation process (FPEP); and peacekeeping operations (PKO).

As a result of calculations, conflict development phases (stages) have been specified. They include: peacetime; period of threats; armed conflict; stabilization; peacetime after the stabilization of a modern military conflict.

The calculations allowed to obtain the value of effectiveness of the ways of providing assistance.

So, according to the calculation results, 5 phases (stages) of the modern military conflict development have been determined and the most effective ways (formats) of assisting the UAF depending on the conflict development phase (stage) have been specified.

But it is necessary to build a flexible system (combination) of measures within different support formats, which will be adequate to the realities of the process of counteracting military threats of a hybrid nature.

This provides a basis for the development of the Concept of Using the Capabilities of NATO and Other Security Organizations to Support Ukraine's Security and Defence Forces", as a document that will develop a Strategy for Ukraine's Security and Defence Sector Support (NATO, Security Organizations and Individual Countries) and other policy documents, outside of such cooperation mechanisms as the NATO-Ukraine Commission, the NATO-Ukraine Joint Group on Military Reform, etc.

Conclusions

The complexity of the application of the capabilities of various spheres of national security will allow: rational use of the state's potential to counter hybrid threats; determine the priority of receiving foreign military assistance.

Cooperation with NATO in the framework of Security Force Assistance is a promising area of foreign military assistance to counter hybrid threats, as this area of the Alliance's activities is directly aimed at strengthening the security and defence capabilities of Partner countries, which is NATO for Ukraine today.

It is necessary to develop a national concept that should define the essence, purpose, principles, approaches, target guidelines, methods and mechanisms for using the capabilities of NATO, other international security organizations and individual countries to provide military assistance (support) to Ukraine's security and defence forces.

References

1. Stockholm International Peace Research Institute (2018), *SIPRI Yearbook 2018: Armaments, Disarmament and International Security*, Translated by Razumkov Centre, Zapovit, Kyiv, 504 p., available at: https://cutt.ly/oky2CrF (accessed 28 January 2021).

2. The International Institute for Strategic Studies (IISS) (2020), *The Military Balance*, Published Routledge, 504 p.

3. Ivashchenko, A.M. and Pavlikovskyi, A.K. (2016), "Analiz osnovnykh napriamkiv rozvytku operatyvnykh spromozhnostei Pivnichnoatlantychnoho Aliansu pislia Varshavskoho sammitu" [Analysis of the main directions of development of operational capabilities of the North Atlantic Alliance after the Warsaw Summit], *Collection of scientific works of the Center of Military and Strategic Studies*, No. 3(58), pp. 18-23.

4. Ball, T. (2017), *Replaced Security Force Assistance Brigades vs. Special Forces*, available at: https://cutt.ly/Sj65dDR (accessed 28 January 2021).

5. The official site of NATO (2010), *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, available at: https://cutt.ly/1j65v01 (accessed 28 January 2021).

6. NATO (2017), *The Concept of the NATO "Security Force Assistance Centre of Excellence"*, available at: https://cutt.ly/vky3ZSl (accessed 28 January 2021).

7. Vozniak, S.M., Ivashchenko, A.M., Fedianovych D.L. and Shpura M.I. (2018), "Metodyka otsiniuvannia rezultatyvnosti shliakhiv vzaiemodii ZS Ukrainy z Pivnichnoatlantychnym Aliansom" [Methods for evaluating the effectiveness of the ways of interaction between the Armed Forces of Ukraine and the North Atlantic Alliance], *Collection of scientific works of the Center of Military and Strategic Studies*, No. 13(54). pp. 11-17.

8. Bocharnikov, V.P. and Vozniak, S.M. (1999), "Alhorytm klasteryzatsii voienno politychnykh syl v umovakh nevyznachenosti" [Algorithm of clustering of military-political forces in conditions of uncertainty], *Scientific and Technical Collection*, No. 3, pp. 35-42.

9. Syrotenko, A.M. (2020), "*Voienni aspekty protydii hibrydnii ahresii: dosvid Ukrainy*" [*Military aspects of counteracting hybrid aggression: the experience of Ukraine*], NUOU im. Ivana Cherniakhovskoho, Kyiv, 176 p.

Sergii Zalkin
Candidate of Military Sciences, Senior Research
Lead Researcher of Ivan Kozhedub Kharkiv
National Air Force University
Kharkiv, Ukraine
https://orcid.org/0000-0002-0518-4414

Konstantin Khudarkovskij
Candidate of Technical Sciences, Associate Professor
Senior Research Associate of Ivan Kozhedub Kharkiv
National Air Force University
Kharkiv, Ukraine.
https://orcid.org/0000-0002-9508-9014

ORGANIZATION OF COUNTERACTION TO INFORMATION AND PSYCHOLOGICAL INFLUENCE ON THE PERSONNEL OF THE ARMED FORCES OF UKRAINE IN THE CONDITIONS OF HYBRID ARMED CONFLICT

The article presents system of counteraction to negative information and psychological influence on the personnel of the Armed Forces of Ukraine, which consists of subsystems of warning conditions for the implementation of negative information and psychological influence, detection of negative information and psychological influence and counteraction to negative information and psychological influence. For each of the subsystems of counteraction to the negative information and psychological influence, the main measures are presented. The interaction of the components of these subsystems reflects the mechanism of counteraction to the negative informational and psychological influence on the personnel of the Armed Forces of Ukraine. The proposed mechanism of counteraction to negative informational and psychological influence involves the implementation of number of activities related to both preventing, identifying and eliminating the consequences of exposure. It is noted that the effectiveness of protection of personnel from negative information and psychological influence is achieved by taking into account the features

and psychological regularities of perception, continuity and systematic organization of measures of moral and psychological support. An important factor in protecting personnel from negative information and psychological influence is the interaction of military authorities with the media, civic organizations and associations.

Keywords: *informational and psychological influence, informational and psychological operation, object of information and psychological influence, system of counteraction to negative informational and psychological influence.*

Introduction

Problem statement. The results of the analysis of local wars and armed conflicts at the beginning of the 21st century indicate that the content of the purpose of the war has radically changed. It is not aimed at seizing enemy territory, but it is focused on psychological suppression of enemy resistance. The conflict between Ukraine and the Russian Federation (RF) showed the nature and means of new types of armed conflicts - the so-called "hybrid wars" replaced the classical forms of armed conflict. Instead of the traditional use of military units, non-military means of force influence, namely, information, cybernetic, economic means acquire key importance [1-6]. Information warfare has become one of the components of armed struggle. Gaining information superiority is one of the most important factors for the positive result of the use of armed forces in military operations and warfare. The possibility of information and psychological influence (IPI) on various target audiences during information and psychological operations reached qualitatively new level. The spread of the Internet and unlimited communication in social networks have significantly supplemented variety of means for conducting information and psychological operations and ensure the formation of integrated information environment.

Information and psychological operation is set of information actions coordinated and interconnected by purpose, tasks, objects and time, as well as events carried out concurrently or sequentially according to one plan for solving information and psychological influence on target audience [7].

The appropriate structures of information and psychological warfare were created to conduct information and psychological operations and achieve information and psychological advantages during the warfare in the leading countries of the world. The forms, methods, ways of information and psychological warfare are constantly updated. Therefore, the problem of counteraction to the information and psychological influence of the enemy is urgent. It acquires special acuity for the Armed Forces of Ukraine due to the hybrid aggression of RF against Ukraine.

The analysis of recent researches and publications. In the conditions of hybrid armed conflict, the personnel of the Armed Forces of Ukraine and the population are under constant psychological and information influence. It is especially evident in the area of Joint Forces Operation and in areas bordering RF.

Informational and psychological influence is the action of information using special methods, means and technologies that threatens the information security of individual, society, state, poses danger to individual or public consciousness, harms a person's physical or mental health or causes him to take certain actions (inaction).

The potentially negative consequences of IPI on the personnel of the Armed Forces of Ukraine is [1–6]:

– obliterating sense of pride in one's own country, belonging to its armed forces, devaluing constitutional duty to protect one's country;

– decrease in moral and mental stability, creating uncertainty among the personnel regarding their own future, the future of the armed forces and the state, weakening of the will to carry out constructive reforms, and in time of war to resist;

– split of military collectives for political, religious, ethnic, official and other reasons, the opposition of privates, sergeants and officers;

– decrease in the combat effectiveness of military units and subunits by reducing official activity, desertion, simulating the illness, avoiding the orders of commanders, treason, doubts about the reliability of weapons, invincibility, suppressing the will, creating

distorted picture of the warfare, the combat situation;

– misperception by the military of the existing threats to national security, the real plans and intentions of the enemy and so on.

All this, with legislative and technical measures to ban and counteract negative content and disseminate their own information of given direction, requires series of measures to protect troops from enemy IPI.

The protection of troops from enemy IPI is component of moral and psychological support, targeted set of measures carried out in peacetime and during special period by command, headquarters, educational work bodies and other officials to prevent, detect, neutralize (weaken), block and liquidation of consequences (minimizing the effect) of enemy IPI on the military and the population [7].

The main subjects in counteracting IPI are:

– public authorities and local authorities;

– appropriate structures of the Ministry of Defense, the General Staff, and the branches of the Armed Forces of Ukraine;

– commanders, headquarters, structures and specialists working with personnel at all levels;

– appropriate forces and means of the heads of military branches of the armed forces and services (intelligence, radioelectronic warfare, structures and specialists working with personnel) and so on.

Today, we can assume that the information security system of Ukraine was not completely prepared to neutralize new challenges and requires some improvement [5-6; 8-11].

The purpose of article is to determine the main tasks that must be implemented in the system of counteraction to IPI on the personnel of the Armed Forces of Ukraine and the implementation mechanism.

Main part

The counteraction to IPI is component of the state's information and psychological security and it is aimed at its own

audience. This audience is the target for special propaganda (information and psychological operations) of the enemy, in order to neutralize or minimize the effect of IPI. It includes the set of measures for the analysis, forecasting, prevention and disruption of enemy IPI, neutralizing attempts to misinform and demoralize the personnel of the troops and the population, and disorganize the combat activity of the troops.

The organization of counteraction to IPI provides:

– maintaining high level of moral and psychological stability of personnel to IPI of the enemy, the formation of readiness of the personnel of the Armed Forces, the population for the armed defense of the country;

– reconnaissance, study, analysis and forecasting of possible directions, forms, methods and ways of using the enemy forces and means of information and psychological operations;

– forecasting and preventing IPI of the enemy at the strategic, operational and tactical levels;

– purposeful study of the socio-political and moral-psychological situation in the region, the area of deployment of the military unit (the area of warfare), the identification of negative factors that can affect the personnel, and their neutralization;

– study of the individual psychological characteristics of personnel, the identification of persons who may adversely affect the moral and psychological state of personnel, and their neutralization

– reconnaissance, identification of forces and means of information and psychological operations of the enemy, materials of IPI and timely suppression, destruction;

– organization of planned, targeted information of personnel.

To organize counteraction to IPI, first of all, on the personnel of military units and subunits of the Armed Forces of Ukraine, an effective counteraction system should function. The mission of the system of counteraction to IPI is the timely warning, identification and neutralization of negative IPI.

The main functions and tasks of the system of counteracting IPI are shown in Tabl. 1 [6].

Table 1

The main functions and tasks of the system of counteraction to IPI

Main functions	Main tasks
Goal setting	Formation of IPI countermeasures in the face of changes in the external and internal security sphere of the state information environment (Armed Forces of Ukraine)
	Formation of new vision on IPI counteraction system in which it will meet new requirements (conditions) based on the realities of the situation
	Timely decision-making and monitoring of the implementation of decisions to prevent the conditions for the implementation of IPI, its identification and IPI counteraction, making adjustments based on the results of their implementation
Organizational and managerial	Organization of IPI counteraction system
	Organization of the implementation of concepts, doctrines, orders, programs in the field of information security of IPI counteraction
	Organization of integrated personnel, financial, material, technical and other support of the components of the system for the performance of tasks for the intended purpose
	Evaluation of the effectiveness of IPI counteraction system
	Improving IPI counteraction system
	Implementation of international and experience of NATO member countries in IPI counteraction
Forecasting	Forecasting of external and internal threats for the implementation of IPI
	Forecasting of the possible effects of IPI on troops and population
	Forecasting of the consequences of the introduction of international and the experience of NATO member countries in countering negative IPI in the domestic system for IPI counteraction
Program-theoretical	Development (clarification) of concepts, doctrines, orders, programs in the field of information security of IPI counteraction
	Development of technologies of anticipatory impact on the causes of the threat of IPI

Table 1 (end)

	Development of IPI neutralization technologies
	Improving the organizational structure of IPI counteraction system
	Development of personnel training programs for the operation of IPI counteraction system
	Development of scientifically based proposals and recommendations on the organization of IPI counteraction
Planning	Planning specific measures of anticipatory impact on the causes of the threat of IPI
	Planning specific IPI responses
	Integrated personnel, financial, material, technical and other support of the components (structural elements) of the system to perform tasks as intended
	Planning the training of forces and means of the software counteraction system of IPI
	Planning for reform of IPI counteraction system
	Participation in cooperation with the international community and NATO member countries on the organization on IPI counteraction
Integration	Development of cooperation with international organizations in the interests of ensuring information security
	Deepening partnership with NATO member countries on IPI counteraction
Monitoring	Identification and assessment of external and internal threats and destabilizing factors in the implementation of negative IPI
	Monitoring the information environment on the feasibility of IPI
	Assessment of the level of information security achieved by IPI counteraction system at the moment
	Comprehensive monitoring of all events occurring in all components of IPV counteraction system
Control	Monitoring of certain tasks of IPV counteraction
	Evaluation of the effectiveness of actions of IPV counteraction and determine the costs of these actions

To implement these basic functions and tasks, the system of counteraction to IPI should consist of three subsystems:

– warning of the implementation of IPI (subsystem I);

– identification of IPI (subsystem II);

– counteraction to IPI (subsystem III).

The interaction of the subsystems of the system of counteraction to IPI is reflected in the diagram of the functional model of the counteraction system, is shown in Fig. 1.

Counteraction to IPI of the enemy can conditionally be divided into several stages [6].

At the stage of familiarization with the situation and its analysis are determined:

– moral attitudes of the personnel and factors of the combat, socio-political and psychological situation that can be used for IPI on the personnel of the unit;

– objects of protection from IPI (governing bodies, communication channels, personnel, members of military families, etc.).

At the stage of threat detection is carried out:

– identifying the beginning of enemy IPI and their level. The level of IPI is the number of information psychological influences for certain time, which can carry out information and psychological threat to the personnel of the armed forces (population);

– identifying signs of decrease in the moral and psychological state of personnel and the combat effectiveness of units.

At the analytical stage is carried out:

– analysis of the dynamics of IPI and their impact on the moral and psychological state of personnel and the combat readiness of units;

– formation of conclusions on the assessment of the level of IPI and the ability to perform tasks assigned to units (parts)

– identifying channels of IPI;

– determination of the possible consequences of the implementation of IPI.

At the stage of determining countermeasures:

– planning of countermeasures is carried out, the most effective methods and methods of protection against IPI are determined;

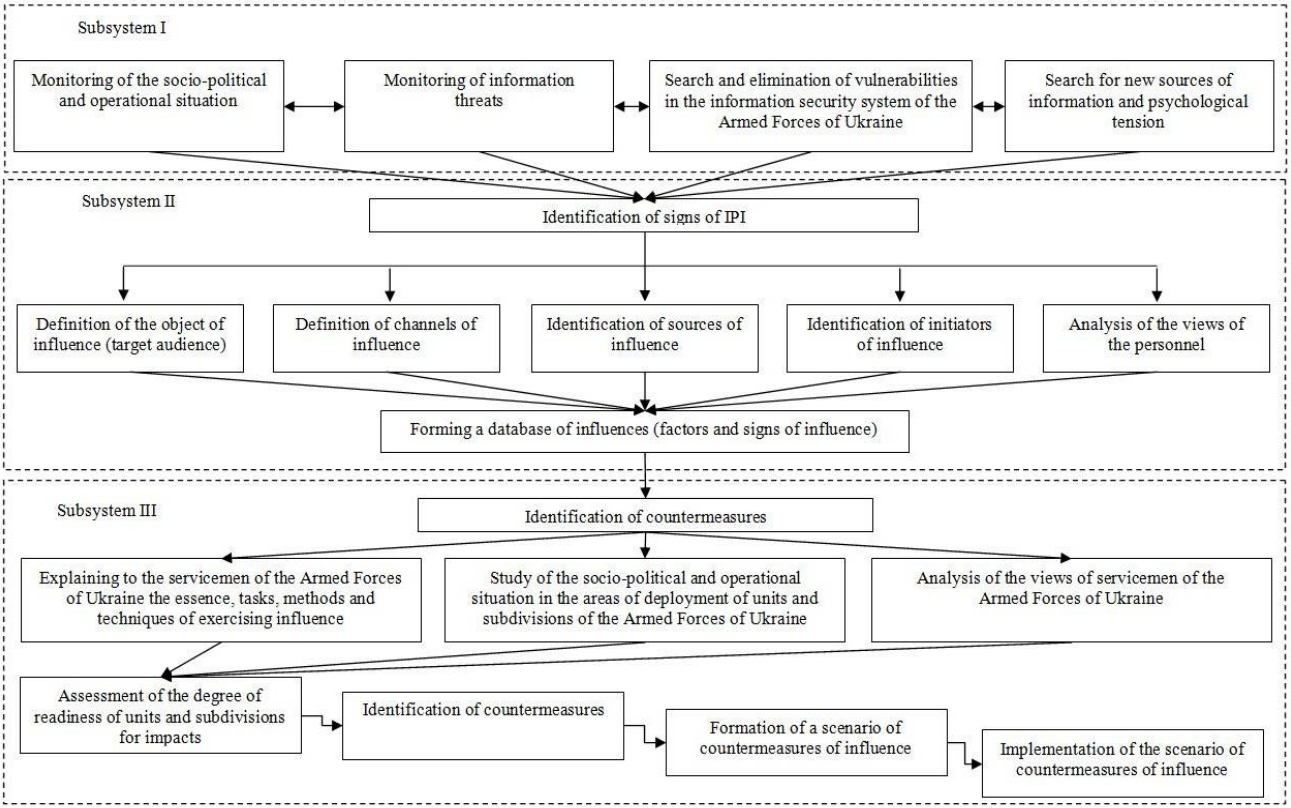

Fig. 1. Scheme of the functional model of the system of counteraction to IPI

– measures are defined to muffle, destroy or suppress IPI, neutralize the distribution channels of rumors, misinformation;

– cooperation is being organized on issues of IPI counteraction with state and local authorities in the region of residence, law enforcement agencies, explanatory work is being conducted among the local population and others.

At the decision-making stage, a plan of IPI counteraction of the enemy is approved.

At the stage of implementation of the planned measures, measures are taken to counter impact in accordance with the approved plan.

At the stage of monitoring, control and correction of measures taken to counter the following:

– control of information flows in communication channels

– monitoring the effectiveness of measures taken to counter influence and their adjustment;

– providing objective, comprehensive information about events

The organization of IPI counteraction on the personnel of the Armed Forces of Ukraine is shown in Fig. 2 [12].

The effectiveness is the main requirement for IPI counteraction of the enemy. It is achieved by:

– timely identification and evaluation of information and psychological influence of the enemy;

– high readiness of forces and means of subjects of information and psychological influence to fulfill tasks;

– integrated use of different means of counteraction to the informational and psychological influence of the enemy.

The effectiveness of measures of IPI counteraction can only be evaluated by the fact of changes in the behavior of the personnel. The result, firstly, depends on how much the principles of prevention, reach and emotional richness of the events will be implemented in practice. Secondly, the results of the counteraction will be determined by how much the leadership of the military units and units takes into account the regularities of the functioning of the psyche of personnel in a combat situation and can influence the

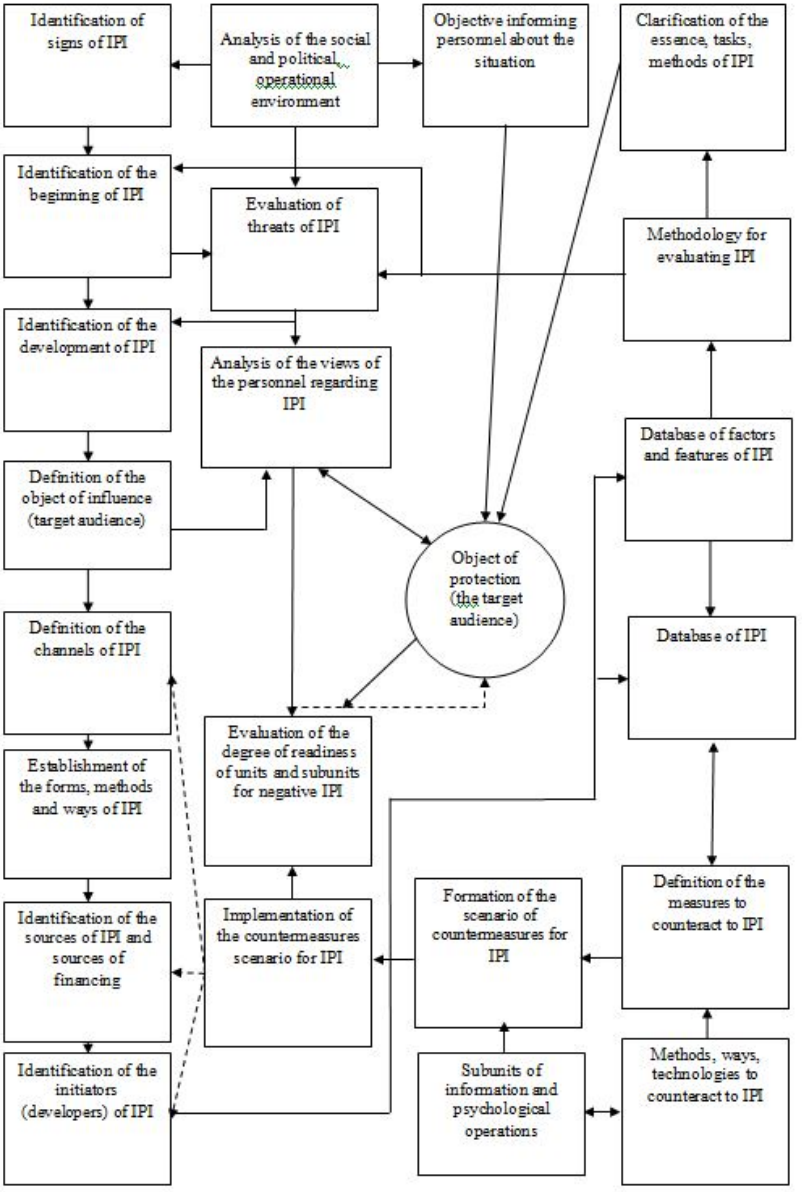

Fig. 2. Scheme of organization of counteraction to negative information and psychological influence on personnel

emotional state, motivation and argumentation of actions, decisions made and the behavior of subordinate personnel. Thirdly, the effectiveness of IPI counteraction depends on the possibility of electronic suppression or physical destruction of sources of destructive effects.

Conclusions

To date, the problem of effective counteraction to information and psychological influences, primarily, on the personnel of military units and units of the Armed Forces of Ukraine is urgent, since significant range of threats to information and psychological security requires the creation of effective methods and technical means for identifying information and psychological influence, determining its negative aspects and the development of measures to counter such influence. Effective counteraction to threats to information and psychological security of the personnel of the Armed Forces of Ukraine and the population in Ukraine is possible provided that structured defense system is created and functioning, the components of which are the legal, organizational, technological and personnel. The implementation of such a system is possible with a targeted information policy of the state, provides for legal support, establishing relations and control over the media, ideological work with the population within the internal information and psychological space and the formation of positive image abroad.

References

1. Moroz, Y. and Tverdokhlib, J. (2016), "Informatsiino-psykholohichni operatsii v umovakh hibrydnoi viiny" [Psychological operations in hybrid warfare], *Visnyk of the Lviv University. Series International Relations*, No. 38, pp. 97–105.

2. Horbulin, V.P. (2015), "Hibrydna viina" yak kliuchovyi instrument rosiiskoi heostratehii revanshu" ["Hybrid War" as a key tool for Russian geostrategy of revenge], *Strategic priorities*, No. 4(33), pp. 5-12.

3. Bohdanovych, V.Yu. (2015), "Modeliuvannia stratehii, oriientovanoi na zminu rezhymu u vybranii kraini-misheni cherez yii zanurennia v khaos, na osnovi metodu funktsionalno znachymykh promizhnykh staniv" [Modeling a strategy aimed at changing the regime in

the selected target country through its immersion in chaos, based on the method of functionally significant intermediate states], *Modern information security*, No. 2, pp. 44-53.

4. Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), "*Informatsiino-psykholohichna borotba u voiennii sferi: monohrafiia*" [*The information and psychological struggle in the military sphere*], Rozhko S.H., Kharkiv, 276 p.

5. Pievtsov, H.V., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2013), "*Informatsiyna bezpeka u voyenniy sferi: problemy, metodolohiya, systema zabezpechennya*" [*Information security in the military sphere: problems, methodology, system of provision*], Digital Printing House No. 1, Kharkiv, 272 p.

6. Pievtsov, H.V., Zalkin, S.V., Sidchenko, S.O. and Khudarkovskij, K.I. (2020), "*Informatsiino-psykholohichni operatsii: planuvannia, protydiia, tekhnolohii: monohrafiia*" [*Information and psychological operations: planning, counteraction, technologies*], DISA PLUS, Kharkiv, 252 p.

7. Military Standard of Ukraine (2014), "*01.004.004-2014(01) Voienna polityka, bezpeka ta stratehichne planuvannia. Informatsiina bezpeka derzhavy u voiennii sferi. Terminy ta vyznachennia*" [*01.004.004-2014(01) Military policy, security and strategic planning. Information security of the state in the military sphere. Terms and definitions*], Kyiv, 22 p.

8. Derkachenko, Ya. (2016), "*Informatsiino-psykholohichni operatsii yak suchasnyi instrument heopolityky*" [*Information-psychological operations as a modern instrument of geopolitics*], Hlobalna orhanizatsiia soiuznytskoho liderstva, available at: goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/.

9. Vorobyov, I.V., Matsegora, Ya.V., Prikhodko, I.I., Timchenko, O.V., Kolesnichenko, O.S., Lipatov, I.I. (2016), "*Informatsiino-psykholohichna protydiia v Natsionalnii hvardii Ukrainy (psykholohichnyi aspekt): monohrafiia*" [*Information-psychological counteraction in the National Guard of Ukraine (psychological aspect)*], National acad. NGU, Kharkiv, 265 p.

10. Hvorost, X.Yu. (2016), "Informatsiino-psykholohichnyi vplyv u rozrizi bezpeky zdorov'ia" [Information-psychological impact in the context of health security], *Science and education*, No. 2-3, pp. 184-191.

11. Kurban, O. V. (2016), "*Suchasni informatsiini viiny v merezhevomu on-lain prostori: navchalnyi posibnyk*" [*Modern information wars in the on-line network space: tutorial*], VIKNU, Kyiv, 286 p.

12. Khudarkovskij, K.I., Zalkin, S.V., Pievtsov, H.V., Pacek, P. and Sidchenko, S.O. (2020), "Mekhanizm protydii nehatyvnomu informatsiino-psykholohichnomu vplyvu na osobovyi sklad Zbroinykh Syl Ukrainy" [Mechanism of counteraction to the negative information and psychological influence on the personnel of the Armed Forces of Ukraine], *Science and Technology of the Air Force of Ukraine*, No. 1(38), pp. 72-78.

TRAINING OF PERSONNEL FOR COUNTERING HYBRID THREATS IN ARMED CONFLICTS

Vadym Artamoshchenko
Candidate of Military Sciences, Associate Professor
Doctoral Researcher of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-7734-4210

THE CONCEPT OF MILITARY EDUCATION AND TRAINING OF DEFENSE FORCES: METHODOLOGICAL ASPECT

The abstract contains brief conclusions on the analysis of the security environment and modern requirements for military education and training of defense forces, promising ways to develop it according to NATO norms, principles and standards. The structure and essence of the future concept of military education as well as methodological aspects of its formation using defense planning approaches based on capabilities on DOTMLPFI components, SMART criteria, SWOT-analysis of Program and Project Management are considered.

Keywords: *concept, defense forces, military education, training, capabilities, program and project management.*

Introduction

Problem statement. The National Security Strategy of Ukraine [1] defines the threats to the national security and national interests of Ukraine. The key ones are continuation of aggression by the Russian Federation against Ukraine, conduct of a hybrid war, which involves systematic use of political, economic, informational, psychological, cyber and military means to renew its influence on Ukraine, violation of human rights and freedoms in the temporarily occupied territories of the Autonomous Republic Crimea and in Sevastopol, in some districts of Donetsk and Luhansk regions of Ukraine.

The analysis of recent researches and publications. Russia is strengthening its position in Europe, using energy and information "weapons", trying to influence the domestic political situation in

European countries, fueling protracted conflicts, increasing its military presence in Eastern Europe. Therefore, the priorities on providing national security of Ukraine are as follows: defending the independence and state sovereignty; restoration of territorial integrity within the internationally recognized state border of Ukraine; development of human capital; protection of the rights, freedoms and legitimate interests of citizens of Ukraine; European and Euro-Atlantic integration [1]. In this situation, development and capacity building of the defense forces in accordance with NATO norms, principles and standards becomes an integral condition for ensuring the priorities.

It is a well-known fact that the military education is the basis for training all components of the defense force. Conditions, environment and tasks form the requirements for development of military education capabilities.

The Law of Ukraine "On National Security" [2] defines the powers of the Ministry of Defense of Ukraine to organize defense planning measures in the defense forces and to form the principles of military personnel policy in the field of defense.

The Ministry of Defense of Ukraine uses the methodology of Program and Project Management (PPM) to implement projects including military education system development projects since 2018. They are based on a key methodology of assessing joint (combined) capabilities according to the components of *DOTMLPFI (Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities, Interoperability)* in the defense planning system in the armed forces of NATO member states [3–6].

Within the framework of the project concerning the military education development the changes to the legislation on new levels of military education (tactical, operational, strategic), testing of new educational and professional training programs, changes to the management system, improvement of infrastructure and logistics have been introduced. An important task is formation of a new "Concept of military education and training of defense forces" (hereinafter – the Concept).

Purpose of the report is to define the structure and essence of the "Concept of military education and training of defense forces", methodological aspects of its formation using the approaches of defense planning based on capabilities and PPM.

Main part

The task of professionalization of the military education system and joint training of the Defense Forces will be fulfilled through introducing a new system of individual training courses at the appropriate levels of military education, which are currently being tested.

At the strategic level of military education, the "Senior Management of Strategic Level Course (L-4)" includes the study of the formation and implementation of national security state policy in the military sphere, defense and military construction spheres.

At the operational level of military education, the "Joint Operations Staff Officers Training Course (L-3)" includes the study of Joint Operation Planning Process of troops (forces) formations according to NATO standards in joint headquarters. Completion of the training course will be obligatory for applicants for the position with a staff category not lower than "lieutenant colonel".

At the tactical level of military education the "Army Command Staff Course (L-2)" is aimed at implementing the procedures for military decision-making according to NATO standards – MDMP (Military Decision Making Process) into the activities of brigade (battalions) headquarters. Besides, the tactical level of military education introduces basic and professional training courses (L-1), which will be conducted simultaneously with obtaining a Bachelor's degree or on the basis of this education to obtain the primary officer positions and staff positions with a staff category "captain". NATO's military decision-making procedures (Troop Leading Process) will be studied at the L-1 courses.

Besides, optimization is being conducted and new Master's programs in the field of science "Military Sciences, National Security, State Border Security", including "National Security (by

type and area of activity)" specialty in "Strategic Defense Forces" specialization are being introduced.

All of this is new, therefore is being tested and is the basis for the formation of the Concept and its further implementation.

An important factor is that the Concept will be applied in all components of the defense forces, so it will have a clear structure and meet the requirements of the Cabinet of Ministers of Ukraine [7].

We are going to consider the components, essence of the Concept and methodological approaches to its formation.

1. Defining the problem to be solved by the Concept.

This section formulates the problem, its significance and compliance with public policy priorities, compares the main assumptions for its solution with the relevant indicators of foreign countries and domestic official statistics and research (usually for a period of at least 3-5 years before the development Concepts).

The concept is derived from the "Concept of development of the security and defense sector of Ukraine" [8], which provides for the introduction of an integrated system of education, combat and special training of personnel in the security and defense sector. The annual national program, which is conducted under the leadership of NATO-Ukraine Commission for 2020 [9], defines the strategic goal of "professionalizing the defense forces and creating the necessary military reserve" and the task of "providing centralized training of operational defense personnel" (by 2025).

Thus, the joint training of the defense forces is one of the important goals of the Concept, and the problem is the inconsistency of the current state of the military education system and the training needs of the defense forces, their acquisition of new capabilities according to NATO norms, principles and standards.

2. Analysis of the problem causes and justification of the necessity to solve it.

This section analyzes the causes of the problem highlighted in the Concept, the impossibility of solving it within the previously adopted programs, and identifies the measures to solve the problem.

Defining of the problem causes should be structured

according to the components of the combined capabilities of DOTMLPFI [3; 5]. This approach will allow working out options and ways to implement the Concept on individual elements of the capabilities of the military education system and training of defense forces.

The implementation of the previous concept was completed in 2000 [10], its further implementation is impractical and does not comply with the law [11].

3. Purpose of the Concept.

The purpose of the Concept should be defined clearly and concisely. To define it, it is advisable to use SMART criteria (specificity, measurability, achievability, relevance, time-bound) which are used in PPM [12].

4. Determining the optimal solution of the problem based on a comparative analysis of possible options.

Comparative analysis of possible options with a clear outline of the advantages and disadvantages of each should be carried out by the method of SWOT-analysis [13–15].

It is necessary to evaluate all components of specialized military education and compare the acquisition of formal or informal education, training at the operational and strategic (operational and tactical) level of military education with training at the strategic (operational) levels, training simultaneously with higher education or on the basis of already acquired one.

Each of the options will have its own SWOT-parameters.

5. Ways and means of solving the problem, the time frames of the Concept.

The content of this section is related to the previous one and should outline the best option with the timing of implementation.

6. Expected results from the Concept implementation, its efficiency.

The results of the Concept implementation should be presented with the use of qualitative, time and resource indicators, and their criteria comparable to the official statistical indicators of the nearest reporting year (3-5 years).

7. Assessment of financial, logistical, human and other resources.

Assessment of financial, logistical, human resources required for the implementation of the Concept should include a justification of the amount of financial resources under the relevant budget programs (subprograms), sources of funding with an assessment of the real possibilities of resource provision of the Concept at the expense of the state budget.

Conclusions

The report defines the structure and essence of the "Concept of military education and training of defense forces", provides methodological aspects of its formation using approaches to defense planning based on capabilities and PPM.

Prospects for further research. The direction of further research specification of the constituent elements of the Concept, substantiation of the strategic goal, the optimal option, time frames, ways and methods of implementation of the Concept, its financial and economic substantiation.

References

1. The Law of Ukraine (2020), "*Pro Strategiiu natsionalnoi bezpeki Ukrainy*" [*On the national security strategy of Ukraine*], available at: https://cutt.ly/Xj06Ld2 (accessed 26 January 2021).

2. The Law of Ukraine (2020), "*Pro natsionalnu bezpeku Ukrainy*" [*On the national security of Ukraine*], available at: https://cutt.ly/Nj066p2 (accessed 26 January 2021).

3. Chairman of the Joint Chiefs of Staff Instruction (2015), *Joint Capabilities Integration and Development System (JCIDS)*, available at: https://cutt.ly/9j2qneI (accessed 26 January 2021).

4. Rusnak, I.S., Petrenko, A.G., Yakovenko, A.M., Romaniuk, I.M. and Kokhno, M.D. (2017), "Oboronne planuvannia na osnove spromozhnostei: osoblyvosti ta perspektyvy vprovadzhennia" [Capability-based defense planning: features and implementation prospects], *Science and Defense*, Vol. 2, pp. 3–10.

5. Ministry of Defence of Ukraine (2019), "*Metodychni rekomendatsii z upravlinnia proiektami*" [*Methodical recommendations for*

project management], available at: https://cutt.ly/oj2wrQ1 (accessed 26 January 2021).

6. Artamoshchenko, V.S. and Favorska, O.U. (2019), "Upravlinnia zminamy shchodo rozvytku systemy viiskovoi osvity na zasadakh programno-proiektnogo menedzhmentu" [Management of changes in the development of the military education system on the basis of program and project management], *Science and Defense*, Vol. 2, pp. 40–44.

7. Cabinet of Ministers of Ukraine (2007), "*Pro zatverdzhennia Poriadku rozroblennia ta vykonannia derzhavnukh tsilovykh program*" [*On approval of the Procedure for development and implementation of statetarget programs*], available at: https://cutt.ly/Dj2wFDB (accessed 26 January 2021).

8. President of Ukraine (2016), "*Kontseptsiia rozvytku sektoru bezpeky i oborony Ukrainy*" [*The concept of development of the security and defense sector of Ukraine*], available at: https://cutt.ly/2j2erHi (accessed 26 January 2021).

9. President of Ukraine (2020), "*Richnu natsionalnu program pid egodoiu Komisiyi Ukraina – NATO na 2020 rik*" [*On the Annual National Program under the leadership of the NATO-Ukraine Commission for 2020*], available at: https://cutt.ly/9j2echL (accessed 26 January 2021).

10. Cabinet of Ministers of Ukraine (1997), "*Pro stvorennia yedynoi systemy viiskovoi osvity*" [*On creation of the common system of military education*], available at: https://cutt.ly/2j2rGJg (accessed 26 January 2021).

11. The Law of Ukraine (2020), "*Pro osvitu*" [*On the education*], available at: https://cutt.ly/jj2r4Vy (accessed 26 January 2021).

12. Project Management Institute (2017), *A Guide to the Project Management Body of Knowledge*, available at: https://cutt.ly/wj2trXb (accessed 26 January 2021).

13. Skyba, Yu. (2020), "SWOT-analiz yak instrument vyiavlennia naujovo-pedagogichnogo potentsialu ukrainskykh universytetiv" [SWOT-analysisas a tool for identifying the scientific and pedagogical potential of Ukrainian universities], *Educational Discourse*, Vol. 3, pp. 86–91.

14. Osita, C., Onyebuchi, I. and Nzekwe, J. (2014), Organization's stability and productivity: the role of SWOT analysis, *International Journal of Innovative and Applied Research*, 2(9), pp. 23–32.

15. Dyson, R. (2004), Strategic development and SWOT analysis at the University of Warwick, *European Journal of Operational Research*, Vol. 152, Issue 3, pp. 631-640.

Valentyn Horovenko
Head of the of the National Institute for Strategic Studies
Kyiv, Ukraine
https://orcid.org/ 0000-0002-1061-559X

Petro Krykun
Chief Consultant of the National Institute for Strategic Studies
Kyiv, Ukraine
https://orcid.org/0000-0003-2780-559X

Viktor Pavlenko
Candidate of Military Sciences
Chief Consultant of the National Institute for Strategic Studies
Kyiv, Ukraine
https://orcid.org/0000-0002-1963-0913

FIGHT IN THE ECONOMIC DOMAIN AS A COMPONENT OF HYBRID WARFARE

One of the new world order's manifestations in the beginning of the XXI century was the transformation of such a socio-political phenomenon as war. Its classical type, where the decisive role and classification feature belonged to the armed struggle, was replaced by a hybrid war. It's main features were: an expanded arsenal of means to ensure the political goals of war (means of armed struggle, as well as non-military means - political, economic, informational and others); going beyond the time frame of a purely armed struggle; expanded list of struggle subjects (along with state ones, paramilitary formations and terrorist organizations play an increasingly active role); lack of a clear boundary between its latent and open periods. However, not only using non-military means of struggle determines one of the features of hybrid warfare. The main thing is the growth of their role in such wars. This trend applies to the economic struggle, which is due primarily to the presence of two factors.

Keywords: *"hybrid war", armed aggression of Russian Federation against Ukraine, globalization of international economic relations, national economy.*

Introduction

Problem statement. The first one is the high dependence of the strategic stability of the *state* on the state of the economy and the level of its economic power.

The second one is the globalization of international economic relations, which has the strengthening the interconnectedness and interdependence effect of national economies. This creates new opportunities for each country, but also increases the vulnerability of the national economy to the influence of other countries, especially if these countries are more economically powerful.

The interdependence and openness economies has generated a creation large amount of different economic means (instruments) of influence some countries on others. Socio-economic and financial-economic can be divided into such means.

Socio-economic struggle means are used to undermine the economic potential of the rival state by provoking the secret services or agents of influence (recruited among politicians, public figures, journalists, government officials, religious figures, other influential people) domestic political tensions and social protest in its ultra-extremist form, organizing and financing large-scale strikes, as well as through informational influence on society to reduce confidence in economic institutions [1–2].

Among the financial and economic struggle means may be economic sanctions, embargoes, causing a banking crisis and the collapse of the national currency, manipulation for the economy of the rival state (oil, gas, etc.) prices for imported goods.

Their application in the practice of international relations takes place both in conflict situations in peacetime and in the course of military conflicts.

***The analysis of recent research and publications*.** The issue of economic struggle has become one of the relevant research subjects in the international security domain. However, the huge numbers of different political, economic, social, informational, and

other factors that must be taken into account in this study, expanding dynamics as well as the range of their variations make it difficult to form the essence of this struggle. Therefore, today there is no generally accepted definition of the term "economic struggle in international relations". The analysis of the few definitions found in scientific publications, in particular, the definition of the term "economic struggle in war", given by the Military-Political Dictionary "War and Peace in terms and definitions", leads to the following synthesized definition [3, p. 54].

Economic struggle in the implementation of foreign policy goals - organized and managed by the state economic measures and actions carried out with political goals and aimed at protecting the national economy from the destructive intentions and actions of another state (a coalition of states) and undermining the economic potential rivals.

It is important to note the difference between economic struggle and economic competition. It's mainly consists of two positions:

– the first one is that economic competition, unlike economic struggle, does not pursue political goals. Mostly it comes down to the attempts of market participants to change the market situation in their favour;

– second one is in contrast to the economic struggle, economic competition in the international market does not involve direct state intervention in the activities of economic entities to achieve certain political goals in relations with other states. The role of the state is more often traced in the active implementation of protectionist policies in the interests of the national manufacturer.

Purpose of the report is prove that fight in the economic domain is an important component of hybrid warfare.

Main part

Economic competition in the relations of states is a permanent factor. With the emergence of foreign policy conflict, it is transformed into an interstate economic struggle.

Operating the concept of "economic struggle" in the above interpretation is not always acceptable. The main reason is the limited consideration of this type of struggle – reducing it only to economic measures. In practice, however, economic measures are mainly carried out in combination with political, informational, cybernetic measures, and during a military conflict – with the use of military force. The object of their protection or influence (about the enemy state) is the economy of the state. Here are some examples of actions of the Russian Federation against Ukraine.

One of the most significant areas in which Russia's use of a wide range of means of influence can be traced is Ukraine's energy sector [4]. Economic measures, in particular for the supply of natural gas, were implemented here through pricing policy, bondage terms of prepayment, temporary suspension of gas supply to Ukraine (March 1995, January 2006 and January 2009). In the Russian-Ukrainian gas conflicts, the political component has always outweighed the economic one. It was pressure from Russia to force Ukraine to relinquish its political position.

This was especially evident after the Orange Revolution (2004) when the final reorientation of our country's foreign policy course to the pro-European vector took place.

The intensity of political measures on the part of Russia, accompanied by its own economic projects, has intensified around the construction of the Nord Stream-2 gas pipeline. With the commissioning of it and the Turkish Stream, Russia will have the opportunity to refuse the transit of gas through the territory of Ukraine.

In the arsenal of means of Russian aggression, cyber weapons are becoming more and more widely used, including against Ukraine's energy system. In the period since 2014, there have been at least two notable cyberattacks on Ukrainian energy companies. The first of them, the largest in its consequences, was held on December 23, 2015. It mainly affected consumers of Prykarpattiaoblenerho: about 30 substations were shut down, and about 230,000 residents were left without electricity for one to six hours. The second cyber-attack took place on the night of December 17-18, 2016. The Northern substation

of the Ukrenergo energy company was shut down for more than an hour: consumers of the northern part of the right bank of Kyiv and region districts of the were left without electricity [4].

These examples lead to the conclusion that when planning and conducting the protection of the economy of their own country or undermining the economic potential of a rival country, it is necessary to use the term "struggle in the economic domain."

The struggle in the economic domain in the implementation of foreign policy goals - organized and managed by the state system of economic, political, informational, military, cybernetic, and other measures, which are carried out to protect the national economy from destructive intentions and actions of another state (a coalition of states) and to undermine the economic potential of rival countries.

This approach allows, based on the specific situation, to optimally allocate the available resources (military and non-military) by objects and time for the successful implementation of the tasks of the struggle in the economic sphere.

The formation of the strategy of such a struggle is influenced by a significant number of factors. Consider the main ones on the example of a state that pursues aggressive intentions.

1. The political goal of the state that is the object of influence. It may include, in particular, the forcible annexation (annexation) of all or part of the territory of that state, the disintegration or change of its leadership, inclusion in its sphere of influence, the establishment of full control over the state, and a change in its political course.

2. Available political, economic, social, informational, military, and other resources can be used in the implementation of the struggle tasks in the economic domain.

3. The projected ratio between the effectiveness of achieving a certain goal and the negative consequences, primarily in the foreign policy and economic domain, which may receive the aggressor state as a result of the implementation of its aggressive intentions.

First of all the protecting strategy economy of one's own state from the destructive actions from another state have to take into

account the assessment of possible options for the enemy's actions and the available own resources - both tangible and intangible.

Assessment of interstate conflicts over the past few decades allows us to identify certain periods in the implementation of the strategy of struggle in the economic domain. The first might be *the formation period of the "economic bridgehead"*. The measures taken in this case are aimed at penetrating the economic domain of the country, further strengthening its own economic influence, and establishing control over its domestic and foreign policies.

If we analyse Russia's actions in the Ukrainian direction, this period falls on the 1990s. These were favourable years in the relations between the two countries, in particular: the state border was defined, the Great Treaty of 1997 was concluded and the Black Sea Fleet was divided. But behind the scenes of the ceremonial picture of good neighbourliness was Russia's attempt to secure the status of political and economic centre among the former Soviet republics, as evidenced, in particular, the attempt to form a monetary union within the CIS, including with Ukraine (September 1993). Already in those years, in response to Ukraine's chosen course of European and Euro-Atlantic integration, Russia used its "energy weapons".

With a view to the future, the Kremlin's ideology of "liberal imperialism" as Russia's "mission" in the 21st century has begun [5]. In the economic sphere, it provided for the assistance of the Russian state to the expansion of domestic business to neighbouring countries. The priority was to acquire the ownership of the main economic facilities located in the CIS countries, including Ukraine.

Within the framework of the mentioned ideology, the process of active penetration of Russian capital into strategically important sectors of the Ukrainian economy has been observed since the mid-1990s. Russia's business occupies a significant niche in Ukraine's fuel and energy sector. Under his control is almost the entire aluminium and titanium industry. Its presence in the field of communications and telecommunications reaches a dangerous level.

Russia's Gazprom bank has in fact taken control of Ukraine's largest chemical plants, Sterol, Rivneazot, Cherkasy Azote, and

Severodonetsk Azote. The presence in the banking market of Ukraine of subsidiaries of Russian banks, such as Prominvestbank, VTB Bank, Sberbank, and BM Bank, has increased [6].

As of July 2014, Russian citizens owned every tenth company in the ranking of the 200 largest companies in Ukraine [7].

In the economic struggle against Ukraine, Russia also uses the significant interdependence between the two countries in the production of weapons, military, and special equipment. This has been a problem throughout Ukraine's independence. In the 1990s, the level of such interdependence was characterized by the following indicators: the total cost of Ukrainian-made weapons was up to 60-70% of the cost of Russian components, and the cost of Russian military products - up to 30-35% of the cost of Ukrainian components.

Subsequently, Russia gradually reduced it’s dependence on Ukrainian components in the production of weapons and ammunition by establishing its own production of the necessary components. However, the dependence remained, the most critical - in aircraft engines and major power plants for ships.

If we take into account the information on the program of import substitution of defence industry products, approved by the Russian government in July 2014, we can conclude that Ukrainian defence companies supplied Russia with more than 3 thousand types of components, assemblies, and units. These products were manufactured by almost 160 enterprises of Ukraine, and they were involved in the creation of about 200 models of Russian weapons and military equipment [8].

The issue of reducing the dependence of the Ukrainian defence industry on Russian components has not been the subject of attention of Ukraine's political leadership for a long time; as such dependence was not seen as a threat to national security until the time of Russian armed aggression.

For the second period of the strategy of struggle in the economic sphere, the most accurate may be the name "*soft power*" – a term introduced into scientific vocabulary by James Sherr, a researcher at the Royal Institute of International Affairs (UK) [9].

It means to influence, where coercion is indirect, carried out mainly in non-military forms and in ways that allow maximum use of the advantages of a state in its power over another state. "Soft power" is used by a State Party when it is necessary to compel the political leadership of another State to act accordingly, provided that there is no need for military intervention.

The Russian strategy against Ukraine beginning of the mentioned period of implementation and should be considered the second half of July 2013, when the Russian customs introduced a total inspection of all vehicles transporting products of Ukrainian producers. As a result, the cargo was idle at the border and Ukraine suffered significant losses. By mid-August, about 40 Ukrainian companies were on the Russian customs "risk list".

The Russian Customs Service included all Ukrainian importers in the list of "risky" on August 14, 2013. This led to an actual blockade of supplies of goods from Ukraine to Russia. Subsequently, the customs control procedure was strengthened. Obstacles to the transit of Ukrainian goods through Russia to other countries were also created. The transit of Ukrainian sugar to Central Asian countries was blocked in April 2014.

The purpose of such actions by the Kremlin was to led the Ukrainian political leadership to refuse to sign the Association Agreement with the European Union. The fact of the existence of such a goal was confirmed by the adviser to the President of the Russian Federation Sergei Glazyev, who said on August 18, 2013, that "this inspection was one-time" - with the EU" [10].

The period of struggle in the economic sphere, which coincides in time with the military conflict, demonstrates the combination the combat using armed forces in a single set of economic means.

Unlike the previously mentioned periods, this period is characterized primarily by the physical destruction (decommissioning) of economic facilities and infrastructure with the use of weapons. At the same time widely using political, cybernetic, and other non-military means of influence.

During this period the struggle is directed by the aggressor to achieve two interrelated goals in the economic domain.

The first of them is the direct assistance in carrying out tasks by one's own armed forces. To achieve this goal (under the influence of fire, missile and artillery systems, cyberattacks, etc.) are objects that ensure the using armed forces of the opposing side. Such objects can be enemy transport infrastructure, military property storage bases, objects of the defence-industrial complex, etc.

The second goal directly depends on the political goal pursued by the aggressor in a military conflict. If there are plans to annex the territory of another country, the enemy tries to preserve its industrial potential for its exploitation in the future. If the goal is to disintegrate and change the leadership of the state-object of aggression, to include it in the future in its sphere of influence, the objects of the economy list will be much wider identified for destruction. The objects that directly ensure the defence of the state, may include, enterprises of leading sectors of the economy and objects of livelihoods. The aggressor will try to create a financial and economic crisis and destroying them (disabling them), and will help to achieve politico’s goal in the military conflict catalyse social protest and protests by separatists and other anti-government forces.

As an example, such a target in the local dimension was traced in the actions of militants led by Russian aggressors in January–February 2017 near Avdiivka (Donetsk region). As a result of their shelling by rocket systems of volley fire and large-calibre artillery, high-voltage power lines were damaged. As a result, Avdiivka was left without water (de-energized filtering station), electricity supply, as well as heat supply, which was provided by the Avdiivka Coke Plant. The plant was suspended. A state of emergency has been declared in the city.

Russia widely practices in the Donbas such a form of struggle in the economic sphere as the export of industrial equipment to its territory. Since the beginning of the occupation of some districts of the Donetsk and Luhansk regions, more than a dozen large enterprises have been exported to the Russian Federation.

Among them are the state company Topaz, the Luhansk Cartridge Plant, the Luhansk and Khartsyzsk Machine-Building Plants, and the Luhansk Aircraft Repair Plant.

Along with this, there is a looting of equipment of many enterprises, and supporting metal structures are cut into scrap metal.

Such actions of the aggressor lead to the conclusion that Russia plans to hand over to Ukraine certain areas of Donbas now occupied by it with the almost destroyed economy and besides a critical ecological condition. The revival of these areas will require significant financial and economic resources from Ukraine. And we can assume that Russia predicts the depletion of the Ukrainian economy, the undermining of socio-political stability, and as a consequence the destruction of the state of Ukraine.

When solving large-scale aggression against Ukraine, the threat of which remains real, under the influence of the enemy with the use of the full range of possible means (military and non-military) may be objects of economic infrastructure throughout Ukraine. Along with this, it is necessary to count on the intensification of purely economic measures of influence, in particular: the cessation of supplies to our state and the transit through its territory of gas and oil; complete severance of trade relations; blocking the transit of goods through Ukraine through Russia to third countries. We should expect the strengthening of Russia's destructive influence on the implementation of Ukrainian economic policy using the pro-Russian lobby in other countries and international organizations.

Conclusions

The struggle in the economic domain is becoming an integral part of the aggression. It begins long before the armed aggression and continues after it ends. In combination with other non-military means of struggle in the economic domains can significantly affect the achievement of political goals in interstate conflicts.

There is a need for research on the struggle in the economic domain, possible forms and methods of its conduct, ensuring the

stability of the national economy in the destructive influence of other states, as well as a system of leadership forces and means involved in the struggle in the economic domain.

References

1. Moroz, Y. and Tverdokhlib, J. (2016), "Informatsiino-psykholohichni operatsii v umovakh hibrydnoi viiny" [Psychological operations in hybrid warfare], *Visnyk of the Lviv University, Series International Relations*, No. 38, pp. 97–105.
2. Dubnitskiy, V., Zubrytska, H. and Kobylin, A. (2018), Interval estimation of the number of participants of mass protest actions, *Advanced Information Systems*, 2(4), pp. 11–20. https://doi.org/10.20998/2522-9052.2018.4.02.
3. Rogozin, D. (2017), "*Voyenno-politicheskiy slovar. Voyna i mir v terminakh i opredeleniyakh*" [*Military-political dictionary. War and Peace in terms and definitions*], Veche, Moscow, 640 p.
4. Zetter, K. (2017), *The Ukrainian Power Grid Was Hacked Again*, Vice Media Group, available at: https://cutt.ly/cjXc4lS (accessed at 21 January 2021).
5. Chubais, A. (2003), "*Myssyia Rossyy v XXI veke*" [*Mission Russia in the XXI century*], Nezavysymaia hazeta, available at: https://cutt.ly/Yk2SubI (accessed at 21 January 2021).
6. Crane, K., Peterson, D.J. and Oliker, O. (2005), Russian Investment in the Commonwealth of Independent States, *Eurasian Geography and Economics*, 46(6), pp. 405–444. https://doi.org/10.2747/1538-7216.46.6.405.
7. LB.UA (2014), "*Rosiia vkhodyt do kozhnoho desiatoho biznesu Ukrainy z top-200*" [*Russia is among every tenth business in Ukraine in the top 200*], available at: https://cutt.ly/Zk2F7tT (accesed 1 August 2014).
8. Maetnaya, E. and Bayazitova, A. (2014), "*Prohrammu ymportozameshchenyia otsenyly v 50 mlrd rublei*" [*The import substitution program was estimated at 50 billion rubles*], available at: http://izvestia.ru/news/574998. (accesed 11 August 2014).
9. Sherr, D. (2013), "*Zhestkaia dyplomatyia y miahkoe prynuzhdenye: rossyiskoe vlyianye za rubezhom*" [*Hard Diplomacy and Soft Coercion. Russia's Influence Abroad*], Zapovit, Kyiv, 152 p.
10. Kramar, O. (2013), "*Kreml blefuie. Zalezhnist ekonomiky Ukrainy vid Mytnoho soiuzu svidomo perebilshuietsia*" [*The Kremlin is bluffing. The dependence of the Ukrainian economy on the Customs Union is deliberately exaggerated*], Chasopys Ukrainskyi tyzhden, available at: https://tyzhden.ua/Politics/87609 (accesed 23 August 2013).

Vitalii Khoma
Candidate of Military Sciences, Associate Professor
Chief of Scientific and Methodological Centre for Organization of Scientific, Scientific and Technical Activities of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-9900-855X

Vitalii Bezuhlyi
Postgraduate Student of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-5051-5676

Ihor Mazurenko
Postgraduate Student of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-2233-7563

PROCEDURE PLANNING OF THE TRAINING OF THE INTERAGENCY FORMATION

Based on a systematic analysis of the combat training planning process of the interagency formation (tactical groups) of the state defense forces, a mathematical apparatus for calculating the level of the combat training planning is proposed, which takes into account planning of departmental (stage I) and planning of interagency (stage II) combat training.

The study has its aim to improve the system of combat training to a level that will ensure the achievement of the capabilities of the components of the state defense forces both independently and jointly to perform certain tasks.

The mathematical apparatus is proposed to be used in the development of methods for assessing the level of organization of combat training of units and interagency formations of the state defense forces.

Keywords: *defense forces, combat training, interagency formation, planning, mathematical apparatus.*

Introduction

Problem statement. The adoption of a number of guiding documents defined a new approach to combat training (CT) of the units of the state defense forces (SDF). Therefore, special attention should be paid to the planning of the CT as the main function of its organization, the establishment of an effective mechanism that will ensure the acquisition of capabilities of the interagency formation of the SDF to perform the certain tasks [1–2].

The engagement of military units and subdivisions of the Armed Forces (AF) of Ukraine together with other military formations of SDF components in the anti-terrorist operation and in the interagency forces operation in the east of the country indicated a number of shortcomings of the CT:

– a number of unresolved (problematic) issues in planning of interagency CT activities, which significantly reduces the effectiveness of the CT;

– imperfection of the regulatory framework for ensuring the interagency CT;

– imperfection of the unified management system of CT.

The analysis of recent researches and publications. An analysis of recent researches and publications [3–4], in which solving the CT planning problems of the SDF was initiated, shows that paying tribute to scientific developments in this area, it should be noted that research on theoretical aspects of CT planning of interagency formations does not have yet a coordinated and systematic nature, and developments on this issue are poorly coordinated between scientific institutions and researchers.

The lack of generally accepted theoretical developments on this topic and relevant recommendations that would correspond to the nowadays realities, reduces the effectiveness of CT planning for interagency formations.

Given that planning is the main function of the CT organization and is a complex system, and the whole set of coordinated actions is defined in the relevant documents on the

organization of CT, research on these issues is relevant.

Purpose of the report. The aim is to solve the problem of system analysis of the process, under consideration, and to develop on this basis a mathematical apparatus for calculating the level of CT planning of the interagency formation.

Main part

Analysis of the use of military units and subdivisions of the Armed Forces of Ukraine together with other military formations and law enforcement agencies in the anti-terrorist operation in eastern part of Ukraine indicates a number of shortcomings in the CT of components of SDF [6].

CT of SDF is carried out in two stages and consists of:

– departmental CT (stage I), which ensures the acquisition of SDF units of the capabilities to independently perform assigned tasks (in services, certain types of troops (forces), training in units of the other military formations and law enforcement agencies (separately). This stage ends with tactical (tactical-special, flight-tactical, ship) exercise [1];

– interagency CT (stage II), which ensures the acquisition by the units of the interagency formation of the capabilities to jointly perform certain tasks (with theoretical and practical training (exercises), usually in a collective format). This stage ends with command and staff exercises with practical actions of troops (forces) at the training ranges [1].

To assess the level of CT planning, it is proposed to determine a generalized indicator $N_{ПБП}(t)$ that takes into account the completeness and quality of planning of departmental and interagency CT of interagency formation.

The indicators that characterize the level of CT planning of the interagency formation include the indicator of the level of planning of the departmental CT (I stage) $Z_{ПВП}(t)$ and the indicator of the level of planning of the interagency CT (II stage) $Z_{ПОП}(t)$.

Since the content of departmental CT planning (stage I)

$Z_{ПВП}(t)$ does not depend on the planning of the interagency CT (stage II) $Z_{ПОП}(t)$, it is proposed to use additive aggregation to assess the level of CT planning $N_{ПБП}(t)$:

$$N_{ПБП}(t) = Z_{ПВП}(t) \cdot q_{ПВП} + Z_{ПОП}(t) \cdot q_{ПОП}. \quad (1)$$

The indicators that characterize the level of departmental CT planning (stage I) $Z_{ПВП}(t)$ of the unit to independently perform tasks include: the Individual training programs of the servicemen $C_{nin}(t)$ and the Combat Training Plan of the military unit $C_{nбn}(t)$.

The content of the Individual training programs of the servicemen does not depend on the scope of training and combat tasks, which is defined in the Combat Training Plan of the military unit (unit), and therefore their indicators are not dependent on each other, in order to assess the level of CT planning $Z_{ПВП}(t)$ it is proposed to use additive aggregation:

$$Z_{ПВП}(t) = C_{nin}(t) \cdot q_{nin} + C_{nбn}(t) \cdot q_{nбn}, \quad (2)$$

where $C_{nin}(t)$ – an indicator that characterizes the quality of the Individual training programs of the servicemen at the *t* moment of time;

$C_{nбn}(t)$ – an indicator that characterizes the part of training and combat tasks (TCT) planned for the military unit (unit) performance at the *t* moment of time of their total number, according to the Combat Training Plan of the military unit (unit);

$q_{nin}, q_{nбn}$ – "weight" coefficients of indicators of the Individual training programs of the servicemen and the Combat Training Plan of the military unit (unit).

The indicator of the level planning of the interagency CT (stage II) $Z_{ПОП}(t)$ of the interagency formation is characterized by the quality of the collective training standards (CTS) $C_{стк}(t)$ and the completeness of the Combat Training Plan of the interagency

formation $C_{n\delta n z}(t)$.

Since the content of the CTS of the interagency formation does not depend on the scope of TCT, which is specified in the Combat Training Plan of the interagency formation, and therefore their indicators are not dependent on each other, in order to assess the level planning of the interagency CT (stage II) $Z_{ПВП}(t)$, it is proposed to use the additive aggregation:

$$Z_{ПОП}(t) = C_{стк}(t) \cdot q_{стк} + C_{n\delta n z}(t) \cdot q_{n\delta n z}, \quad (3)$$

where $C_{стк}(t)$ – an indicator that characterizes the quality of the CTS of the interagency formation command at the *t* moment of time;

$C_{n\delta n z}(t)$ – an indicator that characterizes the part of TCT planned for interagency formation command performance at the t moment of time out of their common quantity, according to the Combat Training Plan of the interagency formation and the number of joint exercises and shootings to their total number;

$q_{стк}, q_{n\delta n z}$ – "weight" coefficients of indicators of the quality of the CTS of the interagency formation command the Combat Training Plan of the interagency formation.

Conclusions

The proposed mathematical apparatus for assessment of the level of CT planning of the interagency formation of the state defense forces, unlike others, combines the CT planning of departmental and interagency, and allows making a quantitative assessment of the level of CT planning of the interagency formation of the state defense forces.

The direction of further research is to develop a partial methodology for assessing the level of organization of the CT of the interagency formation of the state defense forces.

References

1. General Staff of the Armed Forces of Ukraine (2020), "*Doktryna spilnoi pidhotovky viisk oborony derzhavy*" [*Doctrine of joint training of state defense forces*], Kyiv, 26 p.

2. Ministry of Defence of Ukraine (2020), "*Yedynyi perelik (kataloh) mozhlyvostei Ministerstva oborony Ukrainy, Zbroinykh Syl Ukrainy ta inshykh skladovykh syl oborony*" [*Nified list (catalog) of capabilities of the Ministry of Defense of Ukraine, the Armed Forces of Ukraine and other components of the Defense Forces*], Kyiv, 626 p.

3. Georgadze, A. and Harabara, V. (2019), Partial method of assessment of tank brigade preparedness level during combat readiness recovery, *Journal of Scientific Papers "Social Development and Security"*, 9(4), pp. 131–142. https://doi.org/10.33445/sds.2019.9.4.10.

4. Heorhadze, O.A., Horbenko, S.V. and Kharabara, V.I. (2015), "Metodychnyi pidkhid shchodo otsiniuvannia yakosti prohramy indyvidualnoi pidhotovky artyleriiskykh pidrozdiliv" [Methodical approach to assess the quality of the individual training program of artillery units], *Systems of Arms and Military Equipment*, No. 2(42), pp. 68-70.

5. Sirotenko, A.M. (2018), Modern views on the forms and methods of application of groups of troops (forces) of the Armed Forces of Ukraine, other military formations, *All-Ukrainian scientific-practical conference "Joint actions of military formations and law enforcement agencies of the state: problems and prospects"*, Odessa, pp. 8.

Oleksandr Maistrenko
Doctor of Military Sciences
Leading Researcher of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-9900-5930

Vitalii Khoma
Candidate of Military Sciences, Associate Professor
Chief of Scientific and Methodological Centre for Organization
of Scientific, Scientific and Technical Activities of the National
Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-9900-855X

Volodymyr Kurban
Candidate of Military Sciences
Deputy Chief of Scientific and Methodological Centre
for Organization of Scientific, Scientific and Technical
Activities of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-4794-0169

DETERMINATION OF REQUIREMENTS FOR INFORMATION AND COMMUNICATION TECHNOLOGIES IN MILITARY EDUCATION AND ANALYSIS OF EXISTING MEANS

The use of the information and communication technology in the military has long been not a tribute to fashion, but an urgent need. After all, the development of military art determines the growth of requirements for communication needs in the military sphere. Thus, the definition of requirements for the information and communication technology tools on the basis of the analysis of the specifics of the conditions of military service, the educational process in the institution of higher military education and existing communication software tools that would satisfy the condition for the integration of opportunities to

meet communication needs in these spheres of life is an urgent need.

The main idea of this study is to identify problems associated with the implementation of information and communication technologies in the military sphere in general, and in military education in particular. To do this, the study analyzed the features of military service, the educational process in the institution of higher military education and existing communication software tools. Based on this, the problems of the use of information and communication technologies and the requirements for them were identified. So, these requirements include: the ability to mask the signs of the functioning of the tool; Security Service of Ukraine certification; the ability to restrict access to certain information to certain officials; the ability to access the necessary databases even offline; intuitive tool interface; the ability to easily operate with information that is in databases; ensuring a dynamic change in the situation and its buildup, the means of managing the facility should, if possible, be unified with other means of the information and communication technology; the tool should be able to port to various devices; the ability to perform official and educational tasks; the possibility of continuously attracting cadets (military personnel) to participate in the process of completing combat training missions; the need to maintain at least a local communication network; the ability to synchronize data on various devices; the possibility of battery life; the ability to process and coordinate a large amount of data; the ability to use the specified tool after completion of training.

Based on the analysis and the formulation of requirements for the information and communication technology tools, it was found that the Ukrainian messenger for communication and interaction MilChat most meets the specified requirements.

Keywords: *simulation modelling; skills acquisition; cadets; the Armed Forces of Ukraine.*

Introduction

Problem statement. The development of information and communication technologies (ICT) causes a change in almost all aspects of human life, society, and this fully applies to military service in the Armed Forces (AF). Due to the fact that the Armed Forces are designed to operate in extreme conditions (increased risk to human life and health, use of weapons), they have increased requirements for the use of new technologies, especially information and communication

[1]. Unfortunately, the introduction of new ICTs is often accompanied by a number of problems. Such problems include: lack of adapted to change structural, functional links, mechanisms for the introduction of new ICTs, inability to determine the possibilities (efficiency, sustainability) of the facility, the system in the implementation of new ICTs, insufficient training and psychological barrier of servicemen use of new ICTs. The most significant, according to the author, is the last problem because the unpreparedness of the application of these technologies in practice leads to a decrease in the capabilities of objects, systems, where these technologies are used.

The reason for this problem, according to the author, is the peculiarities of the introduction (application) of the latest ICT in the Armed Forces of Ukraine. One of such features is: giving priority to the provision of troops [1], leaving somewhat out of consideration higher education institutions (HEIs) and training units. This feature leads to the fact that the graduate of a higher education institution or training unit needs to adapt after arriving at the unit to the peculiarities of combat missions using new ICT.

Another feature of the use of ICT in the educational process of the Armed Forces of Ukraine is the use of information with limited access, which significantly complicates the educational process.

Despite this, ICTs are used in some way in the learning process, but most often as a demonstration object, very rarely as a means of communication. This leads to the fact that cadets perceive these technologies as something complex and incomprehensible. At the same time, they easily learn modern means of information communication (messengers, file sharers, social networks), perceiving them as something simple and clear.

The general problem of the introduction of ICT in military education, according to the author, is the lack of a common tool for the Armed Forces of Ukraine (network, messenger) with sufficient access to use it in education.

However, returning to military education, it should be noted that the root causes of problems related to the study of new ICTs are: the lack of connection between training and communication of

cadets; weak link between training and further service; lack (limited access) to the database (methodical materials, textbooks, manuals).

Thus, in the practice of military education there is a discrepancy between the need to introduce the latest ICT in military education and the lack of effective mechanisms to do so**.**

The analysis of recent research and publications. Issues related to the use of ICT in higher (including military) education are devoted to a number of studies, including: D. Mesland (John W. Masland) and L. Redway (Laurence I. Radway) [2], Douglas Nobel D. Noble) [3], Huan-Chao Keh, Kuei-Min Wang, Shu-Shen Wai, Jiung-Yao Huang, Hui Lin and Ji-Jen Wu [4], Sae Schatz, David Fautua, Julian Stodd and Emilie Reitz [5], David Fautua, Sae Schatz, Emilie Reitz and Patricia Bockelman [6], O.V. Boyka [7], A.V. Yankovets [8], V.V. Stadnyk [9], I.F. Goncharenko [10], I. Zaitseva [11].

In the work of D. Mesland and L. Redway (John W. Masland, Laurence I. Radway) [2] based on the analysis of the impact of changes in the use of information technology on professional military education, the authors present a clear analysis of military competencies, form and content of military education taking into account information technology. In this paper, the analysis is based on hundreds of interviews and questionnaires and a detailed study of the history and programs of military academies, command and staff schools, the Armed Forces, the National Military College, three military colleges, the Industrial College of the Armed Forces and other institutions.

Douglas D. Noble's study [3] explored areas such as engineering psychology, artificial intelligence and cognitive sciences, as well as military training. This paper also describes research in the field of computer education in terms of these areas.

In the article by Huan-Chao Keh, Kuei-Min Wang, Shu-Shen Wai, Jiung-yao Huang, Hai Lina Lin and Ji-Jen Wu [4] considered the features of distance learning in higher military education. This study presents the architecture of the prototype of higher military education - distance learning (AME-DL) for advanced military distance learning,

it combines a modern e-learning tool, simulation technology and web technology, which provides a selection of learning topics that are easily accessible anywhere and anytime via web browser. The article by Sae Schatz, David Fautua, Julian Stodd, and Emilie Reitz [5] identifies five favorable conditions for the future military training environment. the possibility of joint design of the military education system taking into account the strategic result, optimization of the whole system (against attempts to optimize its parts) and consideration of the human element during all project stages is considered.

A study by David Fautua, Sae Schatz, Emilie Reitz, and Patricia Bockelman [6] examined the stages of building a blended learning system (using ICT tools and traditional methods) over a three-year project, as well as evaluated the effectiveness of the implemented components, in particular in relation to information and communication technologies. This paper states that the results of a blended learning system gave 21% higher results in learning and acquiring skills, when additional e-learning courses preceded the exercise, and when additional training of team training was added to the preparation for exercises, 62.9% of participants indicated who feel more confident in performing their tasks.

The article [7] solves the problem of determining the pedagogical conditions for the effective implementation of modern information and communication technologies in the educational process of higher military education.

The study [8] is devoted to the problem of application of information and communication technologies for independent study of a foreign language by cadets in higher military educational institutions. In particular, a method of organizing independent work with the use of computer-generated educational computer programs has been developed.

In [9] features of training of reserve officers are considered. In particular, the need for wider use of simulation, situational, multimedia and information technologies in the educational process was emphasized. There is also an example of improving the mastering of material on the subject "Methods of work on

humanitarian issues", through the use of web-quest technology to prepare for a seminar on "Organization of psychological training in the armed forces of NATO member countries."

Article [10] is devoted to determining the place and role of information and communication technologies in the scientific and pedagogical activities of scientific and pedagogical workers of the military medical sphere. The attitude of scientific and pedagogical workers to the use of information and communication technologies and teaching aids in the system of training and advanced training in the field of military medical postgraduate education is revealed. The results of a survey of research and teaching staff on the use of ICT are presented. The problems of formation of information and communication competence of the scientific and pedagogical worker in the field of military medicine in the organization and carrying out of advanced training which scientific and pedagogical workers now see in use of ICT in the course of their teaching activity are allocated and generalized.

In the article [11] the author made an attempt to reveal key aspects of the use of information and communication technologies in the educational process of higher education institutions based on the analysis of legal documents, research of modern scientists, as well as requests for the practice of higher education institutions. Based on the analysis of government documents, the essence of the definition of information technology, which is interpreted as electronic computers, software, mathematics, linguistic and other software, information systems or their individual elements, information networks and communication networks used to implement information technology. The essence of information and communication technologies is established, as well as the factors that influence the use of information and communication technologies in education. The list of means of information and communication technologies (hardware and software) is specified. Forms of work in classes in higher education institutions, as well as ways to use information and communication technologies in higher education institutions are presented. The conclusion about expediency and efficiency of use of means of information and

communication technologies in educational process of establishments of higher education is made.

These studies have made a significant contribution to the introduction of ICT in the educational process of a higher education institution, including the military. However, the issue of integration of communication (software) products (tools, technologies) into all major spheres of military service remains unresolved. That is, there is no clear delineation of requirements for communication (software) products (tools, technologies) that would satisfy the conditions of use in official activities, educational process and everyday life. It is clear that such requirements can be determined only on the basis of an analysis of the specifics of the conditions of military service, the educational process in the institution of higher military education and existing communication software.

To simplify the presentation of the material further in the text, it is proposed to use the term - ICT tool instead of the term - communication (software) product (tool, technology).

Purpose of the report. Thus, the purpose of the report is to determine the requirements for the ICT tool based on the analysis of the specifics of military service, the educational process in higher military education and existing communication software that would meet the integration of opportunities to meet communication needs in these areas.

Main part

Theoretical fundamentals of research. Before conducting the declared analysis, it is proposed to determine the general outline of the requirements for such a tool on the basis of consideration of these problems. Thus, such a tool should: combine the possibilities of using it in official activities, the educational process and in everyday life; provide opportunities to restrict access to information; be ergonomic and adaptable to a variety of devices and conditions.

However, in order to specify these requirements, the same tasks of service, educational process and full life should be defined, military service should be eliminated in order to successfully

complete tasks, acquire knowledge and navigate to ensure off-duty communication. This requires a detailed analysis of the previous features of military service.

It is clear that the peculiarities of military service are the same basic factor that is studied not only by the use of ICT in the military department, but also the level of interest of servicemen through a particular tool (product) and the acquisition of new knowledge and navigation.

The results of the analysis of military conflicts of recent decades [12–18] and the possible future nature of the war [19] Michael Macedonia invites to identify the features of military service, which significantly affects the results of military conflict.

Thus, during operations in Iraq, Afghanistan, the anti-terrorist operation (ATO) (Joint Forces Operation (JFO)) in eastern Ukraine [12–15], the installation changed so quickly (from a few minutes to several hours) that The management organization did not have time not only to make decisions, but also to display relevant information. Dose often this has led to inconsistencies, losing initiative and failure to perform combat missions. Thus, a feature of recent conflicts is the relatively rapid change of change.

During the military conflicts between the federal troops of the Russian Federation and the Armed Forces of Ichkeria, the federal military commissions of the Russian Federation and the Armed Forces of Georgia [16–18], despite the number, fire and strike advantage of the federal troops of the Russian Federation, the Armed Group due to the use of new ICT. Thus, the latest ICTs provided an advantage in time, accuracy, maneuverability, screening, which allowed to perform a task not caused by this advantage. If another feature is the fight against the enemy for the gain in time, accuracy, maneuverability, secrecy.

The limited time for studying renewals and making decisions about training is due to another feature of the service activities of servicemen. This feature is the formalization of information about the quality of circulation in control networks. The results of the analysis of combat operations of full special purpose AZOV show that the use of a formalized SALUTE report on the results of the

review allowed for a shorter period of time to obtain more information [20]. Of course, another feature is the formalization of official information.

Another feature is due to the increase in intelligence, which leads to the need to study this information. It is clear that this allows for more effective decision-making, however, and requires an increase in the capabilities of the forces and means involved in the information processing process. Thus, the next feature is the relatively large amount of data that must be operated when deciding on combat use (combat).

Returning to the results of the analysis of the military conflict between the federal troops of the Russian Federation and the Armed Forces of Ichkeria [16–18] it should be noted that quite often to preserve the military formation of the Armed Forces of Ichkeria changed This became possible only due to the coordination of actions and a clear structure of subordination, which is another feature of the successful service of servicemen.

The results of the analysis of the anti-terrorist operation (ATO) in eastern Ukraine [14–15] show that units in low-intensity military conflicts can cover large enough areas of the line of combat. This leads to the need to change your location to perform tasks and act autonomously for some time. This requires the military to have sufficient knowledge and skills to make decisions on their own if necessary. That is, the next feature of official activity is the relative autonomy of the unit in terms of provision and location.

Thus, the features of military service, which determine, among other things, the requirements for ICT, include: rapid change of circumstances; competition with the enemy for time gain, accuracy, maneuverability, secrecy; formalization of official information; relatively large amount of data that must be operated when deciding on combat use (combat operations); coherence of actions and clear structure of subordination; relative autonomy in terms of security and location.

***Research methodology*.** These features of military service in some way determine the features of the educational process in the

institution of higher military education.

One of the main features of the organization of the educational process in the institution of higher military education is the use of information that is a state secret. This requires the implementation of a set of measures, including granting access and access to state secrets to cadets and teachers, appropriate equipment of the training venue, use of certified by the Security Service of Ukraine (SSU) equipment and software. It is clear that the use of the latest ICT tools is complicated in this situation.

Based on the above, it is possible to formulate several requirements for the ICT tool. First of all, it is the SSU certification of this tool. Another requirement is the possibility of restricting access to certain information to certain officials to whom this information does not apply. Also no less important feature is the ability to mask the signs of the tool.

Another feature of the educational process, which is likely to be inherent not only in the military, but in general are the features of modern higher education is the transition from knowledge accumulation to the operation of information. Having simplified access to a relatively large amount of information somewhat reduces the value of owning this information. At the same time, the role of the ability to operate with a variety of information is increasing. Which forms a certain trend in the development of higher education.

With regard to military education, this trend is somewhat weaker due to the relatively complex procedure of staffing research and teaching staff who understand the current priorities of higher education. However, this trend determines the peculiarity of modern higher education, namely the shift of emphasis from the acquisition of knowledge to the ability to operate with information.

This feature makes it possible to formulate several more requirements for the ICT tool. So it is possible to access the necessary databases even offline. The next requirement is an intuitive interface. Another requirement is the ability to easily manipulate the information contained in databases.

Also a feature of the modern educational process, including

the military, is the inclusion in the educational process of an increasing number of electronic learning tools. In general, this significantly increases the digestibility of the material. In addition, it speeds up the time for feeding the material and allows to ensure the proper quality of control over the assimilation of the material. Thus, a feature of the modern educational process is its informatization. However, the increase in the number of e-learning tools leads to the fact that it takes some time to master the order of its use by cadets. Thus, the results of the analysis of the educational process in the institution of higher military education show that up to 50% of the study time using ICT tools is devoted to the study of software tools.

Based on this, several requirements for the ICT tool can be formed. In particular, this - the use of the tool should be intuitive, ie the tools should be, if possible, unified with other ICT tools. Next, the tool must be able to be ported to a variety of devices. Another requirement is the ability to use the tool for business purposes and during training.

In a separate feature, despite the interaction with the previous feature, it is necessary to highlight the use of simulation tools. Modern military higher education quite powerfully uses such a tool as a means of simulation. This allows you to significantly reduce the cost of material resources, time. However, simulation tools are stationary, i.e. used only during classes. Despite the fact that classes on simulation tools are conducted in the form of command and staff exercises, , i.e. almost continuously for several days, it is difficult to create conditions for complete immersion in the situation. These classes are perceived as something temporary and superficial. This leads to a decrease in motivation to learn the material.

Thus, in view of the above, it is possible to formulate another requirement for the ICT tool. The ICT tool should provide a dynamic change of the situation and its increase, as well as continuous involvement of the cadet to participate in the process of training and combat missions.

Considering the previous feature, we can identify several more features that are directly related to the specifics of military

education. Thus, considering such types of classes as command and staff training, group exercise, tactical training, a set of practical classes, it should be noted that these classes have a relatively long duration from several hours to several days.

It is clear that the provision of communication between the participants of the educational process given the duration is problematic. After all, it is impossible to keep cadets in the training place for a long time without losing the productivity of learning the material. Moreover, ensuring the continuity of learning and performing different tasks in one study group at the same time necessitates the possibility of transferring data from one device to another or using them on different devices simultaneously. Also, the specifics of such classes is the ability to perform part of the training and combat tasks in the field (without stationary power supplies).

Thus, this feature provides the formation of the following requirements for the ICT: the need to maintain at least a local communication network; possibilities of data synchronization on different devices and autonomous work (without a stationary power supply).

Considering in more detail the classes with a relatively long duration, it should be noted that in addition to the duration of these classes is a large amount of information, as well as a relatively large number of training and combat missions. And these tasks can be different at the same time for different cadets. In addition, the information circulating in the network of communication links of the participants of the educational process should not be contradictory.

This indicates another feature of military education, namely: a relatively large amount of information and tasks that are assigned to certain classes. This feature makes it possible to formulate the following requirement for the ICT tool: the ability to process and reconcile large amounts of data.

There is another feature of military education, which is due to the development of military science.

Military science, developing in the paradoxical logic of war, quite often and radically changes its vector. This leads to changes in

the forms and methods of combat operations, methods of combat missions and the use of weapons and military equipment. Accordingly, it affects military education. That is, planning documents and methodological materials must be changed in accordance with the requirements of modern martial arts. The same goes for ICT tools. So another feature is: a relatively rapid loss of relevance of certain methods and techniques of tasks.

This feature allows you to formulate certain requirements for the ICT tool: the ability to update databases; the ability to use this tool after graduation (implementation of the principle of training without separation from service).

Thus, the peculiarities of the educational process in the institution of higher military education at the present stage of development are: the secrecy of a certain part of the information; shifting the emphasis from the acquisition of knowledge to the ability to operate with information; informatization of the educational process; use of simulation tools; relatively long duration of certain classes; relatively large amount of information and tasks that are submitted to certain classes; relatively rapid loss of relevance of certain methods and techniques of tasks.

These features make it possible to formulate a number of requirements for the ICT tool. In general, these requirements can be hierarchically divided into two levels: general, those formulated on the basis of problem analysis and detailed, those formulated on the basis of feature analysis. Hierarchical interconnectedness of ICT implementation problems in military education; features of the conditions of military service, the educational process in the institution of higher military education and the requirements for the means of ICT are presented in Fig. 1–2.

In line with the purpose of this study, the next step is to analyze existing ICT tools. The results of the analysis of existing ICT tools that are used (or can be used) in the educational process in higher military education institutions allow to classify these tools. Thus, to simplify further research, it is proposed to distribute ICT tools on the basis of the scope: the educational process itself, the

organization of the educational process, communication (messengers).

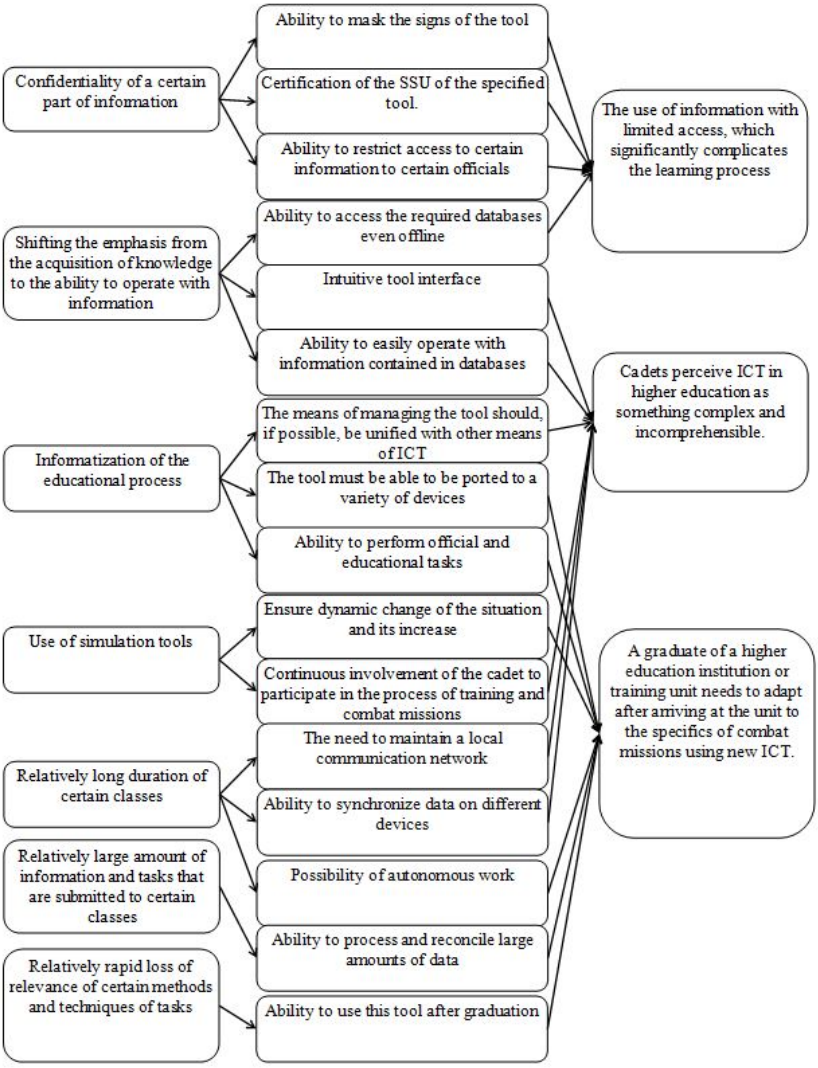

Fig. 1. The interrelation of the peculiarities of the conditions of military service, the educational process in the institution of higher military education and the requirements for the ICT tool with the problems of the introduction of ICT in military education

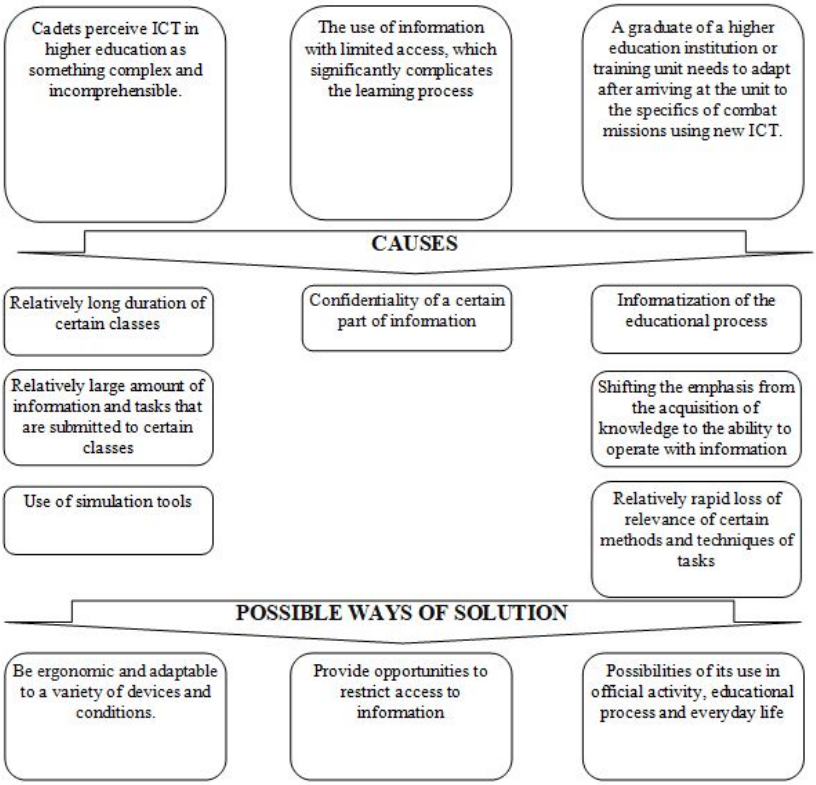

Fig. 2. Problems of ICT implementation in military education, the reasons that caused them and possible solutions

It is clear that this classification is conditional and certain ICT tools may belong to several classes. However, in order to highlight those features of ICT tools that are extremely important for the formation of knowledge and skills of cadets, such a classification is appropriate. Moreover, this classification correlates with the problems of ICT implementation in the educational process of higher military education institutions.

Analysis of ICT tools used directly in the educational process shows that their main function is to increase the efficiency of learning material. The implementation of this function is achieved by performing a number of tasks, in particular, the demonstration of

educational material, modeling situations or certain actions, simplification of the operation of educational information.

Such tools include: multimedia devices for displaying educational information (infocusses, TVs, multimedia boards); simulation tools (Follow me, JCATS, Battle command, simulators); computers and specialized programs (computer classes, design and calculation tasks) [21].

The main advantages of using these tools for further implementation of ICT in military education are: clarity of educational material, concentration on certain tasks and actions, reduction of time for submission and mastering of educational material.

At the same time, the disadvantages of these tools, given the identified problems of ICT implementation in military education are: the difficulty of using them at a convenient time for the cadet (independent training, free time); the need for certification of each tool separately for the submission of information with limited access; the means of control of these means (interfaces) of these means are different; conditional binding of the information submitted for further official activity.

The results of the analysis of ICT tools used for the organization of the educational process show that the main function of such tools is to increase the efficiency of classes. The implementation of this function is achieved by performing a number of tasks, in particular, storage, control of learning material, analysis of the success of cadets and the activity of research and teaching staff.

Such tools include: learning environments (Moodle, Blackboard Learn, Eliademy); school management tools (MySchool, Schoology); distance learning tools (GetCourse, Edmodo) [22].

The main advantages of using these tools for further implementation of ICT in military education are: access to information at a time convenient for the cadet; the ability to port the tool to various devices; the possibility of remote tracking of learning material.

At the same time, the disadvantages of these tools for use in

higher military education are: the inability to provide information with limited access; impossibility of joint performance of group tasks with other cadets; impossibility of use in further official activity; inability to access information in offline mode.

their main function is to ensure communication between cadets and teachers. The implementation of this function is achieved by providing: voice communication during classes, information exchange, setting tasks and monitoring their implementation.

Such means include: means of digital communication (trunking radio stations); messengers (MilChat, Edmodo) [23–24].

The main advantages of using these tools for further implementation of ICT in military education are: the ability to use both in training and further service activities; possibility of use at any time, convenient for the cadet; intuitive interface; ability to encrypt information.

At the same time, the disadvantages of these tools for use in higher military education are: the inability to store databases; the need for certification of each sample by the Security Service of Ukraine; inability to operate with a large amount of information; inability to use offline.

Results of the research. Considering the existing ICT tools, the specifics of military service and education, it can be noted that the prospect of developing ICT tools for the military is to create a unified software for training and service with the ability to port to various devices. The general characteristics of such a tool are due to the requirements identified during this study.

The Ukrainian messenger for communication and interaction MilChat belongs to such means which most meet the specified requirements. It is proposed to consider in more detail its possibilities in the perspective of its application for military education and to identify possible further ways of its development.

MilChat is a specialized military mobile messenger, which is much more functional than well-known civilian messengers. MilChat Messenger is designed to: send text messages and files of any type; private or group work with electronic maps to apply a tactical situation;

sending and receiving formalized SALT / SALUTE reporting reports; ensuring reliable and encrypted (end-to-end) data exchange; unlike civilian messengers, MilChat encryption is always active.

An important feature of this messenger is the ability to integrate with other military programs such as ArtOS, MilStaff

Reference [24]: ArtOS - a complex of automated fire control of artillery batteries, mortars and rocket-propelled grenade launchers of various calibers, includes an innovative solution to the problems of communication, intelligence collection and ammunition accounting. MilStaff is a staff artillery control kit that is installed on a secure PC and is designed to automate combat planning, control of artillery units equipped with ArtOS during combat and fire control.

Another feature of MilChat is cross-platform, which allows you to run on operating systems such as Android. IOS, Windows, macOS and GNU / Linux and can work offline.

In general, MilChat can be integrated into the ecosystem ArtOS - MilChat - MilStaff, the main purpose of which is - more effective combat missions.

This eco-system provides the following opportunities:

– all software is mutually integrated, which makes the transmission of orders and targets instantaneous through any means of communication;

– more efficient receipt of intelligence information with its further analysis;

– joint efforts to obtain intelligence information by all participants in the ecosystem;

– speeding up the sending of reports on the state of equipment and personnel, as well as on the state of ammunition and logistics from the lower headquarters to the highest;

– the ability to both receive intelligence and share it with specific users.

The results of the analysis of MilChat messenger show that it meets most of the requirements for the ICT tool for military education. However, there are still some issues that need to be addressed. Yes, it would be advisable to implement the ability to

save training (reference) material both directly to the device and in the cloud storage. You can also enter the database update feature when connected to the network. Another useful innovation would be the certification of the software by the SSU.

Conclusions

Thus, the article defines the requirements for the ICT tool for the needs of servicemen, based on the analysis of the specifics of military service, the educational process in higher military education and existing communication software that would meet the integration of opportunities to meet communication needs in these areas.

1. The study found that the features of military service, which determine, among other things, the requirements for ICT, include: rapid change of circumstances; competition with the enemy for time gain, accuracy, maneuverability, secrecy; formalization of official information; relatively large amount of data that must be operated when deciding on combat use (combat operations); coherence of actions and clear structure of subordination; relative autonomy in terms of security and location.

2. It is also determined that the peculiarities of the educational process in the institution of higher military education at the present stage of development are: the secrecy of a certain part of the information; shifting the emphasis from the acquisition of knowledge to the ability to operate with information; informatization of the educational process; use of simulation tools; relatively long duration of certain classes; relatively large amount of information and tasks that are submitted to certain classes; relatively rapid loss of relevance of certain methods and techniques of tasks.

3. These results of the analysis allowed to form requirements for the ICT tool for the needs of servicemen, in particular: the possibility of masking the signs of the tool's functioning; SSU certification; the possibility of restricting access to certain information to certain officials; the ability to access the necessary databases even offline; intuitive interface; the ability to easily operate with information contained in databases; ensuring dynamic change of the

situation and its increase; the means of control of the means should, if possible, be unified with other means of ICT; the tool must be able to be ported to various devices; ability to perform official and educational tasks; the possibility of continuous involvement of cadets (servicemen) to participate in the process of training and combat missions; the need to maintain at least a local communication network; the ability to synchronize data on different devices; possibility of autonomous work; ability to process and reconcile large amounts of data; the ability to use this tool after graduation.

Based on the analysis and formulation of requirements for ICT tools, it was found that the Ukrainian messenger for communication and interaction MilChat best meets these requirements. The results of the analysis of MilChat messenger show that it meets most of the requirements for the ICT tool for military education. However, there are still some issues that need to be addressed. Yes, it would be advisable to implement the ability to save training (reference) material both directly to the device and in the cloud storage. You can also enter the database update feature when connected to the network.

Prospects for further research are the development of teaching materials using the latest ICT tools, which took into account the specifics of military service, the educational process in higher military education and their (ICT tools) capabilities that would meet the integration of opportunities to meet communication needs spheres of life.

References

1. The Order of the Ministry of Defense of Ukraine (2014), " *Pro zatverdzhennia Kontseptsii informatyzatsii Ministerstva oborony Ukrainy No. 650 vid 17.04.2014*" [*On Approval of the Concept of Informatization of the Ministry of Defense of Ukraine No. 650 dated 17.04.2014*], available at: https://cutt.ly/8j4kq1u (accessed 27 January 2017).

2. Masland, J.W. and Laurence, I. (2014), *Radway Soldiers and Scholars: Military Education and National Policy*, Nabu Press, 556 p.

3. Noble, D.D. (2017), *The Classroom Arsenal*, Military Research, Information Technology and Public Education, 242 p.

https://doi.org/
10.4324/9780203730317.

4. Keh, H.-C., Wang, K.-M., Wai, S.-S., Huang, J., Hui Lin and Wu, J.-J. (2008), Distance-Learning for Advanced Military Education, *International Journal of Distance Education Technologies*, 6(4), pp. 50–61. https://doi.org/10.4018/jdet.2008100104.

5. Schatz, S., Fautua, D., Stodd, J. and Reitz, E. (2017), The Changing Face of Military Learning, *Journal of Military Learning*, April, pp. 78-91, available at: https://cutt.ly/Aj4jqkQ (accessed 27 January 2017).

6. Fautua, D.T., Schatz, S., Reitz, E. and Bockelman, P. (2014), Institutionalizing blended learning into joint training: A case study and 10 recommendations, *Proceedings of the Interservice Conference: Interservice/Industry Training, Simulation and Education Conference (I/ITSEC)*, available at: https://cutt.ly/gj4jI9O (accessed 27 January 2017).

7. Boyko, O.V. (2006), *Introduction of modern information and communication technologies in the educational and educational process of the educational institution as a tendency of transformation of the Ukrainian Armed Forces*, Lviv Polytechnic National University Institutional Repository, available at: https://cutt.ly/ej6CS4e (accessed 27 January 2017).

8. Jankowiec, A.V. (2005), "*Pidhotovka maybutnikh perekladachiv za dopomohoyu informatsiyno-komunikatsiynykh tekhnolohiy u vyshchykh viys'kovykh navchal'nykh zakladakh*" [*Preparation of future translators by means of information and communication technologies in higher military educational establishments*], Khmelnytskyi, 27 p. available at: https://cutt.ly/bj6CFK8 (accessed 27 January 2017).

9. Stadnik, V.V. (2015), "Innovatsiyni pidkhody do udoskonalennya systemy pidhotovky ofitseriv zapasu dlya Zbroynykh Syl Ukrayiny" [Innovative Approaches to Improvement of the Reserve Officers Training System for the Armed Forces of Ukraine], *Proceedings of the III International Internet Conference: Pedagogical Sciences*, available at: http://surl.li/kciq (accessed 27 January 2017).

10. Honcharenko, I.F. (2014), "Informatsiyno-komunikatsiyni tekhnolohiyi v profesiyniy diyal′nosti naukovo-pedahohichnoho pratsivnyka u sferi viys′kovo-medychnoyi pislyadyplomnoyi osvity" [Information and communication technologies in the professional activity of a scientific-pedagogical employee in the field of military medical postgraduate education], *Information Technology and Learning*, 42(4), pp. 47-55. https://doi.org/10.33407/itlt.v42i4.1098.

11. Zaitsev, I. (2017), The Using of Means of the Information-Communication Technologies in the Educational Process of the Institutions of Higher Education, *Pedagogical Discourse*, (23), pp. 59-61, available at: https://cutt.ly/Tj6Xn8G (accessed 27 January 2017).

12. Fontenot, G., Degen, E.J. and Tohn, D. (2004), *On Point: The United States Army in Operation Iraqi Freedom*, Defense technical

information center, Fort Belvoir, Virginia, available at: https://cutt.ly/Cj6XDab (accessed 27 January 2017).

13. Feickert, A. (2005), *U.S. military operations in the global war on terrorism : Afghanistan, Africa, the Philippines, and Colombia*, available at: https://cutt.ly/Jj6XKqu (accessed 27 January 2017).

14. Roman, N., Wanta, W. and Buniak, I. (2017), Information wars: Eastern Ukraine military conflict coverage in the Russian, Ukrainian and U.S. newscasts, *International Communication Gazette*, 79(4), pp. 357–378. https://doi.org/10.1177/1748048516682138.

15. Jonsson, O. and Seely, R. (2015), Russian Full-Spectrum Conflict: An Appraisal After Ukraine, *The Journal of Slavic Military Studies*, 28(1), pp. 1–22. https://doi.org/10.1080/13518046.2015.998118.

16. Lyall, J. (2009), Does Indiscriminate Violence Incite Insurgent Attacks? *Journal of Conflict Resolution*, 53(3), pp. 331–362. https://doi.org/10.1177/0022002708330881.

17. Nichol, J. (2008), *Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests*, Defense technical information center, Fort Belvoir, Virginia, available at: https://cutt.ly/xj6X2iM (accessed 27 January 2017).

18. Nichol, J. (2009), *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests*, Defense technical information center, Fort Belvoir, Virginia, available at: https://cutt.ly/Dj6X5Ue (accessed 27 January 2017).

19. Macedonia, M. (2018), *The Future Character of Warfare and Required Capabilities*, available at: https://cutt.ly/7j6CtVQ (accessed 27 January 2019).

20. Prosapas, I. (2018), *The ISTAR Fire Control System: The War Experience of the Chief of Artillery Regiment Azov*, Tsenzornet, available at: https://censor.net.ua/resonance/3046748 (accessed 27 January 2019).

21. Zacharias, G.L., Macmillan, J. and Van Hemel, S.B. (2008), *Behavioral modeling and simulation: From individuals to societies*, National Academies Press, Washington, https://doi.org/10.17226/12169.

22. Edebatu, D.C., Ekwonwune, E.N. and Ezeobi, C. (2019), Learning Management System for Improved Service Delivery in Tertiary Institution, *International Journal of Communications, Network and System Sciences*, 12(03), pp. 37–48. https://doi.org/10.4236/ijcns.2019.123004.

23. Holland, C. and Muilenburg, L. (2011), Supporting Student Collaboration: Edmodo in the Classroom, *Society for Information Technology & Teacher Education International Conference*, Publisher: Association for the Advancement of Computing in Education, Chesapeake.

24. Surepin, S. (2018), "*V Ukraine sozdali messendzher dlya voyennykh*" [*A messenger for the military was created in Ukraine*], available at: https://cutt.ly/Lj6C2Hv (accessed 27 January 2019).

Dmytro Muzychenko
PhD, Associate Professor
Head of the Army Department of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-6470-1402

Vasyl Shvaliuchynskyi
PhD, Associate Professor
Deputy Head of the Army Department of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-2775-4422

Yuri Syromlya
PhD
Instructor of the Foreign Languages Department of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-7297-4259

EXPERIENCE OF COOPERATION BETWEEN THE NATIONAL DEFENCE UNIVERSITY OF UKRAINE NAMED AFTER IVAN CHERNIAKHOVSKYI AND THE LITHUANIA REPUBLIC MILITARY ACADEMY ON THE ARMY OFFICERS TRAINING

The report is devoted to the analysis of the international exercises and classes results held at the university in 2017-2019. The purpose of the report is to identify problematic issues that arose during the training (classes) and possible ways to solve them. Based on the analysis of the results of international cooperation, a number of recommendations are proposed that can be taken into account when planning similar activities in the future.

Keywords: *international cooperation, standards, NATO, international exercise, MDMP.*

Introduction

Problem statement. Ukraine, its Armed Forces (AF) in general, and the National Defence University of Ukraine named after Ivan Cherniakhovskyi (NDUU) in particular are actively working to study and implement a number of standards used in NATO member countries in the educational process and in their daily activities. In order to coordinate joint efforts between the countries of the alliance and our country, many documents have been developed that regulate this process. One such document is the Annual National Program Under the Auspices of the NATO-Ukraine Commission (hereinafter the Annual Program). The Annual Program for 2020 [1] was approved by the Decree of the President of Ukraine of May 26, 2020 No. 203/202. Annex 1 to this Program [2] identifies priority tasks and activities for responsible executors, including the Ministry of Defence of Ukraine (MDU). For MDU the priority tasks are:

– working out of Ukraine with NATO topical special partnership (cooperation) issues;

– study and coverage of Euro-Atlantic security issues;

– holding the International NATO Week in Ukraine (within the walls of the NDUU);

– holding thematic events on Ukraine's cooperation with NATO in military training units of higher education institutions, etc.

Thus, the departments of our university have to solve a number of tasks to study and implement in the educational process new standards for the Armed Forces of Ukraine and the effectiveness of this process is directly related to the level of cooperation of our research and teaching staff (NPP) with colleagues abroad.

The analysis of recent research and publications. An analysis of some of the standards currently adapted for use by national AF shows that these standards do not always correspond to the approaches used in Allies. For example, the Procedure for drawing up operational (combat) documents, approved by the order of the Ukrainian AF General Staff dated 25.04.2018 number 170 “On approval of the Procedure for operational (combat) documents execution”, which was used in the AF

of Ukraine until mid-2020, should streamline the work of servicemen during the development of combat textual and graphic documents, as is done in the AF of NATO member countries. A similar document used in NATO is the APP-6 Standard [3]. But as a result of comparing the content of these documents, a number of significant differences were found, which consist in the content and form of text documents, the order of display (colour, inscriptions, sizes) of graphic symbols (marks), section names and distribution of symbols between sections, etc. In 2020, there was an attempt to eliminate some inconsistencies between the national standard and the NATO standard [3] and in September the Temporary Procedure for Operational (Combat) Documents Design was adopted by the Commander-in-Chief of the Armed Forces of Ukraine. But the new document has many inconsistencies with the NATO standard that took place in the previous national standard.

The APP-6 standard is closely related to other standards and is used in the work of headquarters during the planning of operations, as well as to reflect changes in the situation during military operations. For example, in the U.S. Army, at the tactical level, headquarters use a procedure called the Military Decision Making Process (MDMP) when planning actions. This process is described in detail in many publications, one of which is FM 6-0 [4]. If we study in detail the staff procedure during MDMP, we can conclude that the symbols given in APP-6 are not accidentally divided into appropriate sections and they are often used differently than they are currently used by Ukrainian AF servicemen.

For example, the set of labels listed in Appendix A to Section 8 (Control measure symbols: Mission tasks and mission task verbs) [3] is typically used when displaying the situation on the Decision Support Template (DST), and the verbs that describe these symbols are in the Decision Support Matrix (DSM). Working out of such documents as DST and DSM is not provided by national standards, so staff officers use these symbols when depicting the situation on the graphic part of the plan, work map, etc., which is not correct in relation to the standards used in NATO member countries.

You can find dozens or maybe hundreds of such examples.

Teachers of the Army Department (ARD) believe that the main reasons for the misconception of the Ukrainian AF servicemen regarding the use of NATO standards are:

– the current combat doctrines and guidelines adopted by 2020;

– insufficient number or weak training of teachers (instructors) who can train servicemen of the Armed Forces of Ukraine to use the new standards;

– misunderstanding (translation) of documents developed in NATO (NATO member states) by specialists trying to develop new national standards.

In 2017, the NDUU leadership took one of the first steps to train teachers and students in the MDMP using during planning the operations of tactical-level military formations. Since then, new approaches to planning operations are gradually replacing the old ones and this is reflected in the work programs of academic disciplines, course programs, the content of training sessions, and so on. But there are also a number of problematic issues that are still hampering the process of implementing MDMP during the students' completion of all complex tactical exercises.

Purpose of the report is to identify problematic issues that have arisen in the Army Department staff during international cooperation with the Military Academy of Lithuania (MAL) representatives and possible ways to solve them.

Main part

During the first international command and staff exercise with representatives of the MAL Command and Staff Course (CSC) in 2017, a number of significant differences were found between the national approaches and those used by Lithuanian colleagues when planning combat operations. NDUU students were guided in their work by national guidelines and the Mechanized and Tank Forces Combat Doctrine [5], and students of MAL CSC were guided by their publication and a number of publications developed in NATO and the United States.

As a result of joint work of "mixed" teams between

participants (both students and teachers) there were misunderstandings in the design and number of combat graphic and textual documents, staff procedures (number and structure of meetings / briefings, structure of officials' reports), etc. But the purpose of the training, which was to develop an operation plan and combat management training, was achieved and it was the first important step in rethinking what needs to be done for Ukrainian AF officers to understand NATO standards.

The challenges of transforming the AF to move closer to NATO standards were not new to Lithuanian colleagues, and they invited the NDUU leadership to continue cooperating in the future, to which they agreed. As a result of the agreements in August-September 2018, three ARD teachers had the opportunity to observe the MDMP teaching methods at the MAL Army CSC named after Great Vytautas (Vilnius), together with Lithuanian colleagues developed the concept of the second international exercise and a set of necessary documents. Representatives of MAL Army CSC visited Kyiv in two stages in October and November.

Previously, two Lithuanian instructors and two NDUU instructors trained in Vilnius conducted a short two-week MDMP (Tutorial) course with Ukrainian officers, which helped to reach a common understanding of how the multinational staff would plan the defensive operations. As a result of international training, teachers of the Army Department, as well as other NDUU departments, gained the knowledge needed to train Ukrainian officers to make decisions in accordance with the standards used by NATO member states, and students gained knowledge and experience currently used in training their subordinates, during the introduction of new standards in subordinate military units and subdivisions. At the end of 2018, the ARD teachers published a textbook in Ukrainian [6], developed on the basis of the Lithuanian publication, which is used in the university educational process.

In February 2019, three more officers of the Army Department visited the Army CSC in Vilnius, learned from the Lithuanian colleagues' experience, worked out the concept of the

third international exercise, as well as the concept of a comprehensive tactical task No. 12, which from September 2019 is carried out in accordance with MDMP procedures. The Ukrainian students' preparation course (Tutorial) for the third international exercise has already been conducted by teachers of our university without the help of Lithuanian instructors. The joint training was held at a high enough level, our teachers consolidated their knowledge and skills, some took part in such an event for the first time, and the next change of students received a lot of knowledge and practical skills to work according to new standards.

The NDUU has launched the Army Tactical Level Command and Staff Course (L-2) since January 2020, the program of which was developed on the basis of the Lithuanian CSC. Currently, there are significant differences between the domestic and Lithuanian courses, which are related to the current guidelines (doctrines, instructions, etc.). In 2020, it was not possible to implement in the course program all the staff work principles laid down in the MDMP, and this was clearly noticed by the commission representatives who took part in the educational programs audit. Currently, a new program has been developed, which is fully adapted to the approaches laid down in foreign [3; 4] and some domestic publications [6] and from January 2021 our teachers will train brigades (battalions, divisions) staff officers to work according to standards, used in NATO. It is planned to involve NDUU's students and NATO member states representatives in the training, but these issues need to be agreed at a higher level.

Conclusions

Thus, summarizing the above, we can make the following conclusions:

The joint work of NDUU's teachers with foreign military educational institutions representatives makes it possible to resolve the issue of training teachers capable of implementing in the educational process the principles laid down in NATO standards, as well as better develop educational programs (teaching materials), new guidelines (standards).

Involving students in international training (classes under the guidance of foreign instructors) takes students to gain experience working in a multinational team, improving theoretical knowledge and practical skills (including in a foreign language).

The university must train future professionals who will be able to organize work in the subordinate team in accordance with the governing documents. If our educational programs are tuned to NATO standards and troops use old guidelines, or imperfect "hybrids," then university graduates will have no value for their commanders and subordinates. National standards should be developed by qualified professionals who are fluent in English and understand the issues laid down in the relevant standard.

References

1. The official site of President of Ukraine (2020), "*Richna natcional'na programa pid egidoyu komisiyi Ukraina – NATO na 2020 rik*" [*Annual national program under the auspices of the NATO-Ukraine Commission for 2020*], available at: https://cutt.ly/Ykf2HH3 (accessed 26 May 2020).

2. The official site of President of Ukraine (2020), "*Priorytetni zavdannya ta zahody Richnoyi national'noyi programy pid egidoyu komisiyi Ukraina – NATO na 2020 rik. Dodatok 1 do Richnoyi national'noyi programy pid egidoyu komisiyi Ukraina – NATO na 2020 rik*" [*Priorities and activities of the Annual National Program under the auspices of the NATO-Ukraine Commission for 2020. Annex 1 to the Annual National Program under the auspices of the NATO-Ukraine Commission for 2020*], available at: https://cutt.ly/Xkf2BSm (accessed 26 May 2020).

3. Nato Standardization Office (NSO) (2017), APP-6 NATO Joint Military Symbology, 922 p., available at: https://cutt.ly/lj69G62 (accessed 28 January 2021).

4. Headquarters, Department of the Army (2014), *FM 6-0. Commander and Staff Organization and Operations*, 392 p., available at: https://cutt.ly/ej69iqP (accessed 28 January 2021).

5. Armed Forces of Ukraine Army Command (2016), *Combat doctrine of Armed Forces of Ukraine Army Mechanized and Tank Troops. Part II. Battalion, Company*, Kyiv, 320 p.

6. Shvaliuchynskyi, V. and Filunkin, Y. (2018), *Procedures for the Military Decision-Making Process (according to NATO standards)*, in ed. Muzychenko D., NDUU named after Ivan Chernyakhovskyi, Kyiv, 140 p.

Boguslaw Pacek
Doctor of Social Sciences, Professor
Professor of Jagiellonian University
Krakow, Poland
https://orcid.org/0000-0001-8111-1682

Hennadii Pievtsov
Doctor of Technical Sciences, Professor
Deputy Head of Ivan Kozhedub Kharkiv National Air Force University in Science
Kharkiv, Ukraine
https://orcid.org/0000-0002-0426-6768

Oleksandr Turinskyi
Candidate of Technical Sciences
Chief of Ivan Kozhedub Kharkiv National Air Force University
Kharkiv, Ukraine
https://orcid.org/0000-0001-6888-6045

TRAINING OF MILITARY SPECIALISTS IN CONDITIONS OF HYBRID ARMED CONFLICT

The article presents the analysis of the stages, features, methods and technologies of the hybrid armed conflict of the Russian Federation against Ukraine, its main phases are defined. The main hybrid threats in the military sphere and the new challenges posed by society, the state and the Armed Forces of Ukraine in connection with the Russian aggression in the east are given. Changes in the training of military specialists and in the organization, conduct and maintenance of the educational process at Kharkiv National Air Force University are presented.

Keywords: *hybrid war, hybrid armed conflict, training of military specialists.*

Introduction

Problem statement. At the beginning of the 21st century, fundamental changes in the nature of wars and armed conflicts took place in the world, not only their political goals but also the ways and

means radically changed.

In today's conflicts, methods based on the complex application of political, economic, informational and other non-military measures implemented with reliance on military force are increasingly used. The set of these methods implements the concept of hybrid warfare, the leading idea is to achieve political goals with minimal military influence on the enemy through the use of modern information technologies with reliance on "soft power" and "hard power" [1–6].

A prime example of the implementation of the concept of hybrid war is the action of the Russian Federation against Ukraine. At the same time, the "hybrid policy" of the Russian Federation is not limited to Ukraine. Russia's "hybrid policy" also covers Europe, the United States, the EU and NATO. The objectives of the "hybrid policy" are:

– against Ukraine – it is the desire to act aggressively on the minds of the leadership and business elites, as well as various party and social groups, as well as on the general population of Ukraine;

– against Europe and the USA – it is the desire to undermine the feeling of well-being and confidence in the countries of Eastern Europe and the Baltic States about their guaranteed protection by the EU and NATO;

– against European Union – it is prevention the enlargement and the complete collapse of the European Union;

– against NATO – it is prevention the enlargement and complete destruction of the North Atlantic Alliance.

The analysis of recent researches and publications. The characteristic features of the hybrid armed conflict against Ukraine are [1–6]:

– aggression without official announcement of war;

– concealment by the aggressor country of its participation in the conflict;

– active use of asymmetric combat operations and network warfare, warfare, does not have single and explicit war control center;

– widespread use of irregular armed groups (including under cover of civilians) under the slogans and appearance of civil war;

– unofficial involvement of non-state performers by the aggressor state - "polite men", "volunteers" who are essentially mercenaries;

– neglect by the aggressor of the international standards of warfare and current agreements and agreements reached;

– mutual measures of political and economic pressure (with the formal preservation of relations between two countries);

– confrontation in cyberspace;

– no rear and front;

– methods of information fight and terror are widely used;

– instant reaction to changing conditions and management flexibility, with the appearance of its absence (managed chaos).

In the course of the hybrid armed conflict against Ukraine, the military and economic potential is undermined, the cultural and ideological sphere is being destroyed, radical opposition is being maintained, special operations forces are being engaged to conduct sabotage and prepare the necessary forces and means to manipulate the protests of the local population. Military assistance and financial support to terrorist organizations are also hidden. After considerable depletion of the enemy, there is limited use of military force under the guise of liberation slogans to transfer the country to foreign control.

In addition, one of the features of the current hybrid armed conflict of the Russian Federation against Ukraine is the simultaneous use of different methods and technologies of information confrontation, the combination of the use of soft and hard force to weaken and decentralize our state, bringing to power the pro-Russian, Russian-controlled European leadership exchange rate, the return of Ukraine under the control of the Russian Federation

Among the methods and technologies of the hybrid armed conflict of the Russian Federation against Ukraine, the most commonly used are:

– diplomatic pressure;

– energy and economic pressure;

– use of information technologies for organizing protest movements, formation of the "fifth column";

– information, misinformation and propaganda influences;

– terrorist and subversive acts;

– intelligence and counterintelligence activities;

– use of special operations forces;

– support for corruption;

– conducting operations in cyberspace.

The hybrid armed conflict against Ukraine began with information war and popular unrest against the current government.

In the second stage there was a promotion of instigators, provocateurs and saboteurs under the guise of the local population, who were rocking the situation.

In the next phase, the initiative was taken by people recruited by the Russian special services, or even citizens of the Russian Federation.

Further, in the course of the escalation of the conflict and its transition to the armed stage, volunteers and mercenaries, weapons specialists and special forces from the Russian Federation, who acted concealed, under the guise of local militias, or openly, without concealing their Russian citizenship (for example, Cossacks, inter-brigade), joined to the conflict. Their task was to take the situation under complete control, win and consolidate the interests of the Russian Federation in the Ukrainian territory.

Russia's hybrid armed conflict with Ukraine has several phases.

The first phase (from February 27 to the end of March 2014) is the Russian military aggression on the territory of Ukraine, the capture of Crimea and its inclusion in Russia. The actions of the Russian Federation in the Autonomous Republic of Crimea had all the characteristics of information and psychological operation, aimed primarily at the Russian audience and, on the other hand, at the Ukrainian and Western audiences prepared and thought out for the

purposes, forms, methods, measures and consequences.

The second phase (April – August 2014) is the concealed Russian military aggression and "militia" in the territory of the south-east (Luhansk and Donetsk regions) of Ukraine, the beginning of military operations. During this phase, the Russian Federation actively pursued measures to destabilize the eastern and southern regions of Ukraine by organizing mass anti-government protests, occupation of administrative buildings, "legalizing" the so-called Donetsk and Lugansk national republics by holding appropriate "referendums" and "elections" of their "authorities", the comprehensive support of the separatists, including the financing of their activities, the training of militants and their provision of weapons, military equipment and ammunition, and the introduction of Russian troops to the territory of Donetsk and Lugansk national republics.

The third phase (from September 2014 to the present) is almost open Russian aggression on limited scale in the south-east of Ukraine.

There was also an increase in the grouping of the Russian Armed Forces near the Ukrainian border.

Purpose of report is the generalization of the experience of training military specialists in the context of hybrid armed conflict.

Main part

The conflict in eastern Ukraine, according to UN estimates, "is one of the deadliest in Europe since World War II". During six years of the war, more than 13,000 people were killed in the Donbas, about 30,000 were injured, and about 1.8 million people in Donbas and Crimea became internally displaced. It occupied 17 thousand square kilometers of Donetsk and Luhansk regions, together with the Crimea it makes up 43.7 thousand square kilometers – that is 7.2 percent of the territory of Ukraine. 409.7 kilometers of the Ukrainian-Russian border remains uncontrolled. 27 percent of the Donbas industrial potential was illegally transferred to Russia, including the equipment of 33 local industrial giants [7].

Six years of armed aggression of the Russian Federation against Ukraine revealed:

– Russia has planned armed aggression against Ukraine in advance;

– Russian aggression was aimed at destroying Ukraine as independent state;

– armed aggression is only one of the instruments of hybrid war;

– courage of Ukrainians and international solidarity halted the Russian invasion;

– Russian aggression has led to dire humanitarian consequences;

– Minsk agreements are regularly violated by Russia;

– Russia has violated fundamental norms and principles of international law;

– Russia regularly sends personnel and weapons to the Donbass;

– military aggression and hybrid war have already become a common practice in Russia;

Russia's aggression can only be stopped by increasing international pressure on the Russian Federation.

Despite Russia's hybrid war against Ukraine for the sixth year running, a number of hybrid threats since 2014 remain relevant today, creating the danger of destabilizing and weakening our state, violating fundamental rights and freedoms, reducing the standard of living and, in fact, the most peaceful existence of citizens of Ukraine.

According to the analytical research of the Center for Global Studies “Strategy XXI” in the military sphere, such hybrid threats are [8]:

– activities of illegal armed groups on the territory of Ukraine, aimed at destabilizing the internal social and political situation in Ukraine;

– disruption of the functioning of public authorities, local self-government bodies and blocking of important objects of industry and infrastructure;

– creation by the Russian special services and agency in Ukraine of conspiracy illegal armed formations in the form of ultra-nationalist organizations of patriotic direction, which are in wait for the creation of chaos in Ukraine and the preconditions for change of power;

– activity of diversion intelligence groups of the aggressor under the guise of Ukrainian security forces in order to discredit the latter;

– illegal proliferation of arms, which leads to uncontrolled possession of weapons by the population of the country and opportunities for its acquisition;

– activities of mercenaries from among citizens of Ukraine, Russia and other countries for committing terrorist and criminal acts with the use of weapons, explosives and so on;

– threat of taking under military control part of the territory of Ukraine by military formations of the aggressor country under the guise of conducting a pseudo-peacekeeping operation;

– targeted measures to discredit the Armed Forces of Ukraine and other military formations and security forces.

These hybrid threats and the new challenges posed by society, the state, and the Armed Forces of Ukraine due to the aggression of the Russian Federation in the east of the country, other radical changes in the external and internal security environment, the need for further development of the main components of the security and defense sector, compatible with the relevant structures of NATO member states, set the task of reforming the Armed Forces of Ukraine, further development of the military education system and improving the training of military specialists in the light of experience in the use of troops during Joint Forces Operation (JFO).

The University has established systematic work on the analysis, study and implementation in the educational process of the experience of using the Armed Forces of Ukraine in conducting Joint Forces Operation (JFO) (Anti-terrorist Operation (ATO)) in the east of Ukraine. It provides:

– regular updating of operational situation, analytical

materials regarding the experience of the use of troops during the JFO (ATO), press release received at the management meeting and every Monday, Thursday - to all permanent staff and graduates during the briefing;

– inclusion in the individual training plans of the management, faculties, departments, the military college of sergeant staff, training centers for studying the experience of using the Ukrainian Armed Forces during environmental protection JFO (ATO) and other armed conflicts of the countries of the world;

– bringing materials with experience of using the Armed Forces of Ukraine in the system of individual training according to the schedules of classes.

Information is collected and summarized in the following directions:

– summarizing and analytical processing of information coming from the structural units of the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine;

– conducting lectures and practical sessions by representatives of customers to train military specialists with experience in combat operations, with scientific and pedagogical staff and University cadets;

– participation of scientific and pedagogical workers and cadets of the University in joint exercises (training) in the military units, which were removed from the area of JFO for restoration of combat power;

– collecting information from the staff of the University among the scientific and pedagogical staff and researchers who were sent to the area of the JFO;

– direct receipt and analysis of information coming from University graduates who participate in the provision and implementation of JFO.

On the basis of the recommendations of the customers for the training of military specialists, the University developed a reference material for each specialty of training for graduates. Work is ongoing on its refinement and printing for study and dissemination.

In addition, Ukraine has been participating in the NATO Defense Education Enhancement Program (DEEP) since 2012. This program helps partner countries develop and reform their military education system. In this regard, the general directions for improving the educational process were:

– adaptation of educational programs to the modern order of use of troops in the operation of the Allied Forces and NATO Standards of Training;

– priority of the practical component in the training, the complexity of the forms and methods of conducting the training, taking into account the experience of the use of troops in the JFO;

– relevance of scientific research to the requirements and needs of the troops;

– updating of personnel potential of scientific and pedagogical staff;

– improvement and creation of modern logistical base.

At the heart of improving the educational process is competent approach in the training of military specialists with higher education.

Realizing these ways, Kharkiv National Air Force University is changing its system of training specialists, especially in:

– values, goals and results of training and education (from mastering knowledge, skills - to formation of basic competencies of military specialist);

– content of training (from substantive abstract theoretical information, little to do with practice - to the formation of competencies necessary to perform job responsibilities on systematic basis);

– pedagogical activity of scientific and pedagogical worker (from monologic teaching of educational material - to pedagogy of creative cooperation and dialogue of the teacher and the learner);

– learning activity of the learner (from reproductive activity, passive memorization of educational information - to creative activity);

– technological support of the educational process (from

traditional methods - to innovative pedagogical technologies that implement the principles of the joint activity of the teacher and the learner, the unity of cognitive, research and future professional activity), etc.

Changes in the structure of training are based on purposeful and organized process of successive activities of training and education of cadets, aimed at the formation of the required level of knowledge, skills, professional skills, physical and psychological qualities necessary for fulfilling the duties of the post (specialty). both in peacetime and in a special period.

The hybrid war against Ukraine, waged by both regular and irregular (illegal) armed forces and anonymous (private) military units, is characterized by the use of new combat tactics, the use of diversion intelligence groups, the constant spread of misinformation, the use of misinformation, and use of local residents and settlements as a "human shield" and so on. All this requires a number of clarifications, additions and changes to the content of the training, curricula and educational training programs.

Formation of the future military specialist has become impossible without improvement and introduction into the educational process of new, innovative forms and pedagogical technologies such as problem training, conducting war games, distance learning and so on.

With the content, the method of conducting the lessons has also changed. The basis of this method was the individual approach to each cadet, the development of his ability to think creatively and work independently.

Under current conditions, the training of military personnel and future commanders is planned taking into account the ability to accomplish missions in Joint Forces Operation, using NATO experience.

The experience of combat operations in Joint Forces Operation (Anti-terrorist Operation) has confirmed that an important part of officer's professionalism is his leadership qualities.

According to world expert in the field of psychology of

success Brian Tracy “Leadership is not embedded in genes or chromosomes. The leader develops in conditions where leadership qualities are required. A leader becomes that when he has to act as leader” [9].

The main features of the leader that are formed at Kharkiv National Air Force University are:

– patriotism;

– professionalism;

– ability to unite the team;

– willpower;

– respect for the traditions of the University, the type of troops, the branch of Armed Forces.

While studying at the University, our cadets undergo a unique character education, forming their professional, cultural and patriotic outlook.

The education of cadets and students of devotion to the people of Ukraine, a sense of pride in their historical achievements in the development of an independent state, the formation of high moral and psychological qualities of citizen-patriot, personal responsibility for the defense and security of Ukraine lay the foundation for future officer-leader.

For the special services and courage shown in the combat operations of the JFO (ATO), 28 military personnel have been awarded state awards. Two University graduates have been awarded the title of Hero of Ukraine with the Gold Star award (posthumously).

Only a leader can raise a leader. Therefore, the requirements for overhead personnel and scientific and pedagogical staff are significantly increased at the university.

54 Doctors of Sciences and 392 Candidates of Science (Doctors of Philosophy) take part in the educational process of the University.

At present, more than 700 people are the member of hostilities, including 98 people from scientific and teaching staff and more than 30 scientists.

Another crucial aspect is the practical training of cadet. It is necessary component of training in the context of hybrid threats, carried out in order to consolidate the theoretical knowledge acquired, the acquisition and improvement of professional skills.

The practical training of the cadets is carried out in combination with the combat training of the troops.

Testing the cadets' readiness to perform their duties in the context of hybrid armed conflict is tactical-specific exercise during which different tactical techniques are practiced against the general tactical background. Features of their conduct are:

– conducting tactical and special training at the same time as bringing the military units of the Air Force and Army Forces of Ukraine to higher stage of combat readiness and conducting flights on combat aircraft with practical use of weapons;

– practical participation of cadets in tactical exercises with live firing practices, repair and restoration of serviceability of weapons and military equipment at industrial enterprises;

– practical implementation of measures of preparation and intercession on combat duty with conducting the appropriate ritual;

– working out of issues of engineering and fortification equipment in the organization of airfield security and combat positions.

This practical training organization allows most University graduates to receive a 3rd class military specialist class qualification, and pilot graduates can also gain experience in combat aircraft.

An important element of the practical training of cadets is the formation of psychological readiness for combat, especially in the context of hybrid conflict. The effective system of psychological training of cadets has been created at the University. It provides for various trainings, elements of survival courses, overcoming the effects of stressful effects and so on.

The feature of the current hybrid armed conflict is the active use of the media and computer networks to pursue purposeful information and psychological influence, including on the University staff.

Despite the fact that the information component of the hybrid war has caught us almost by surprise, today Ukraine has already gained unique experience of confronting information aggression, which is taken into account in the training of specialists.

To date, the University has a system of counteracting the negative information and psychological influence of the enemy, constantly taking measures to protect staff from negative information and psychological influence. The main measures to protect personnel from negative enemy information and psychological influence are:

– analysis and prediction of information and psychological influence;

– prevention of information and psychological influence;

– disruption of information and psychological influence;

– elimination of consequences of information and psychological influence.

Scientific activity is an integral part of the educational process. It ensures the correspondence of the content of education to the modern achievements of military science and technology, the development of fundamental, applied research in the priority areas of the theory and practice of construction and application of the Armed Forces of Ukraine, increasing their combat capability and ability to conduct combat operations in the conditions of hybrid war, modernization and creation of principles of hybrid and military equipment.

On this subject annually at the University:

– conferences and seminars are held;

– considerable number of research works and operational tasks are performed.

The results of scientific research are reflected in many scientific, educational and methodological works. More than 130 scientific articles in leading professional editions and more than 20 monographs and scientific and methodological editions are devoted to various factors of hybrid armed conflict.

Conclusions

Finally, it should be noted that the restructuring of the educational process of the University is carried out in accordance with the reform of the military education of Ukraine. The outcome of restructuring will be the creation of effective military education system that will operate on the basis of NATO standards. Effective military education system will be able to guarantee the needs of the Armed Forces of Ukraine for military specialists of all levels of the military education and adequately and flexibly respond to military threats to the national security of Ukraine.

References

1. Horbulin, V.P. (2015), "Hibrydna viina" yak kliuchovyi instrument rosiiskoi heostratehii revanshu" ["Hybrid War" as a key tool for Russian geostrategy of revenge], *Stratehichni Priorytety*, No. 4(33), pp. 5-12.

2. Pievtsov, H.V., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2013), "*Informatsiyna bezpeka u voyenniy sferi: problemy, metodolohiya, systema zabezpechennya*" [*Information security in the military sphere: problems, methodology, system of provision*], Digital Printing House No. 1, Kharkiv, 272 p.

3. Pievtsov, H.V., Zalkin, S.V., Sidchenko, S.O. and Khudarkovskyi, K.I. (2015), "Informatsiino-psykholohichni operatsii Rosiiskoi Federatsii v Ukraini: modeli vplyvu ta napriamy protydii" [Russia's information and psychological operations in Ukraine: models of influence and ways to counter them], *Science and Defense*, No. 2, pp. 28-32.

4. Pievtsov, H.V., Zalkin, S.V., Sidchenko, S.O., Khudarkovskyi, K.I., Feklistov, A.O. and Antonov, A.V. (2014), "Osnovni osoblyvosti oznak provedennia informatsiino-psykholohichnoi operatsii Rosiiskoi Federatsii v Avtonomnii Respublitsi Krym" [The main features signs of information and psychological operation of Russia Federation in Crimea], *Science and Technology of the Air Force of Ukraine*, No. 1(14), pp. 37-39.

5. Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017),

"*Informatsiino-psykholohichna borotba u voiennii sferi: monohrafiia*" [*The information and psychological struggle in the military sphere*], Rozhko S.H., Kharkiv, 276 p.

6. Pievtsov, H.V., Zalkin, S.V., Sidchenko, S.O., Khudarkovskyi, K.I. and Hordiienko, A.M. (2014), "Realizatsiia pidkhodiv informatsiinoi viiny Rosiiskoiu Federatsiieiu v suchasnomu informatsiinomu prostori Ukrainy" [Realization of approaches of information war of Russian Federation in the modern information space of Ukraine], *Science and Technology of the Air Force of Ukraine*, No. 2(15), pp. 10-13.

7. President of Ukraine (2019), Vystup Prezydenta Ukrainy na debatakh Heneralnoi Asamblei OON z pytannia: "*Sytuatsiia na tymchasovo okupovanykh terytoriiakh Ukrainy*" [*The situation in the temporarily occupied territories of Ukraine*], available at: https://cutt.ly/dj4mLwR (accessed 27 January 2021).

8. Center for Global Studies "Strategy XXI" (2018), "*Hibrydni zahrozy Ukraini i suspilna bezpeka. Dosvid YeS i skhidnoho partnerstva*" [*Hybrid threats to Ukraine and public safety. Experience of the EU and the Eastern Partnership*], Kyiv, 106 p., available at: https://cutt.ly/Hj4Qw1R (accessed 27 January 2021).

9. Treisi, B. (2003), "*Tsel – absoliutne liderstvo*" [*The goal is absolute leadership*], Inter-ekspert, 391 p., available at: https://www.livelib.ru/book/1000025058/about-tsel-absolyutnoe-liderstvo-brajan-trejsi (accessed 27 January 2021).

Olha Pashkova
Researcher of the Research Centre for Military History
of the National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-6525-4613

RUSSIAN HYBRID IMPACT ON MILITARY-PATRIOTIC EDUCATION IN UKRAINE (2010–2013)

Occupation of part of the territory of Ukraine and the development of armed conflict in certain districts of Donetsk and Luhansk regions were preceded by careful training of the military and political leadership of the Russian Federation, including its ideological component. The hidden influence on the consciousness of the population of Ukraine was especially active in Russia in the period 2010-2013, when the state authorities of Ukraine declared good neighbourly and partnership relations with the northern neighbour. Analysis of the events of 2014-2019 suggests that the activities of certain religious and public organizations in 2010-2013 were aimed at strengthening Russia's presence in the state authorities of Ukraine, promoting Russia's views on the future of our country, including European and Euro-Atlantic aspirations, as well as the formation of a single "Slavic, Orthodox space", where the Russian Federation was given a leading role. A separate area of their work was the "military-patriotic education" of young people and servicemen of the Armed Forces of Ukraine to form views and beliefs loyal to the Russian Federation and its likely actions towards Ukraine.

Keywords: *military-patriotic education, servicemen of the Armed Forces of Ukraine, public organization, religious organization, hybrid impact.*

Introduction

Problem statement. Military-patriotic education as a component of national-patriotic, acquired state significance after the beginning of the armed aggression against our state. At the same time, in order to understand the causes and preconditions of the

conflict, it is important to investigate the impact on the upbringing of Ukrainian youth of representatives of religious and public organizations. One of the forms of hybrid aggression of the Russian Federation against Ukraine was the incorporation into state authorities of persons whose activities were aimed at reducing the combat effectiveness of Ukrainian troops (forces), in particular through the impact on the consciousness of personnel of the Armed Forces of Ukraine.

The analysis of recent researches and publications. Aspects of the negative impact of the Ukrainian Orthodox Church of the Moscow Patriarchate on the personnel of the Navy of the Armed Forces of Ukraine were covered by some domestic researchers [6; 7]. The activities of some public organizations to influence the military-patriotic education of Ukrainian youth, including future officers, have not been properly reflected in special scientific works.

Purpose of the report is to highlight the negative impact of certain pro-Russian religious and public organizations on Ukrainian youth, including future officers of the Armed Forces of Ukraine, on the eve of the armed aggression of the Russian Federation against Ukraine.

Main part

The results of the presidential elections in Ukraine in 2010 led to a turn of state power from Ukraine's Euro-Atlantic course. In particular, the Law of Ukraine “On the Principles of Domestic and Foreign Policy” enshrined Ukraine's non-aligned status while maintaining good neighbourly relations and strategic partnership with the Russian Federation, other Commonwealth of Independent States. There was in-depth cooperation with these states in the humanitarian sphere, which included, in particular, participation in joint events on the occasion of historical dates. Measures to bring the policy of memory of the Commonwealth of Independent States about the events of World War II to a single standard, to develop common views on the role and place of the Soviet Union in World War II, the formation of a common commemorative space testified to the gradual reorientation of

national military-patriotic education in Ukraine on “Eastern” direction.

The continuity of patriotic educational activities in the Armed Forces of Ukraine was ensured by the Military-Patriotic Education Programs for the relevant period. At the same time, the programs included a number of events together with the Armed Forces of the Russian Federation in Moscow: participation in the Commonwealth Warrior International Professional Skills Competition, an Army Patriotic Song Contest “Vivat Victory”, Military Brass Band Festival “Spasska Tower”, and delegation of Ministry of Defence of Ukraine in the work of the military section of the international Christmas readings. Active cooperation with representatives of the armed forces and religious organizations of the Russian Federation was carried out by the Synodal Department for Interaction with the Armed Forces and other military formations of Ukraine of the Ukrainian Orthodox Church [1, p. 36].

At the same time, representatives of the Department participated in the military-patriotic education of servicemen of the Armed Forces of Ukraine, particularly of cadets and lyceum students (meetings due to the religious and state holidays, ceremonial events, prayers and blessings), took part in scientific conferences about problems of patriotic education of the Ukrainian youth [1, p. 32; 2, p. 44]. In particular, in 2012, with the assistance of the Department, a procession was organized and held with the participation of cadets of some higher military educational institutions of Kyiv, which continued in different regions of Ukraine, covering about 120,000 people [3, p. 59; 61].

In the Autonomous Republic of Crimea representatives of the Orthodox Church (Moscow Patriarchate) declared their “uniting” mission in serving for the Naval Forces of the Armed Forces of Ukraine and Russian Black Sea Fleet, not distinguishing them [4, p. 6]. At the same time, since 2010 priests of the Ukrainian Orthodox Church of the Kyiv Patriarchate and the Ukrainian Greek Catholic Church have stopped engaging in pastoral work in the Ukrainian Navy, unlike representatives of the Ukrainian Orthodox Church of Moscow Patriarchate [6, p. 37].

Ambiguity was also observed in the issue of organizing military-professional holidays. In particular, the Decree of the President of Ukraine postponed the celebration of the Day of the Ukrainian Navy to the last Sunday of July, the Day of the Navy of the Russian Federation [5], which weakened the authority of the Navy of the Armed Forces of Ukraine in the Crimean peninsula, made it impossible to carry out their military-patriotic education on the basis of national historical heritage. At the same time, the initiative to assign a name of the naval activist of the Ukrainian People's Republic Rear Admiral M. Ostrohradskyi-Apostol to the Naval Lyceum in 2010 did not find support in the Ministry of Defence of Ukraine [6, p. 40].

The “uniting” role of the Ukrainian Orthodox Church of Moscow Patriarchate became apparent during the events of February-March 2014, when the Russian Federation occupied the Autonomous Republic of Crimea, and its representatives called on servicemen of the Navy to betray Ukraine and to join “Armed Forces of Crimea (Russia)” [7, p. 177]. Thus, the influence of the pro-Russian clergy of Crimea on servicemen of the Armed Forces of Ukraine and local pre-conscription youth was carried out in line with Russian ideology.

Another area of influence was educational sphere. During the study period, Ukraine received from Russia proposals and initiatives to establish joint military educational institutions in the Autonomous Republic of Crimea. In particular, the Department of Military Education and Science of the Ministry of Defence of Ukraine processed the order of the President of Ukraine dated 11.11.2011 № 1-1/2625 on the possibility of establishing a joint Naval boarding school in Sevastopol for children of servicemen of the Navy of the Armed Forces Ukraine and the Black Sea Fleet of the Russian Federation. On December 8-9, 2011, members of the working group held a field meeting in Sevastopol to study this issue. At the same time, the representatives of the Department stated that there was no interest in the creation of such an institution on the part of Russia [8, p. 71–72].

At the same time, in 2012, on behalf of the Minister of Defence of Ukraine D. Salamatin, the Department considered the appeal of the Minister of Defence of the Russian Federation A. Serdyukov to establish a Russian-Ukrainian presidential Nakhimov school in Sevastopol. Members of the working group from the Ministry of Defence of Ukraine concluded that resolving this issue was beyond the competence of the ministry due to lack of funds in the ministry for the location of such an institution, uncertainty about state standards by which the educational process was to be conducted, subordination, teaching language and content [8, p. 69–70]. In general, the receipt of such proposals, with in-depth cooperation in the humanitarian sphere, joint activities testified to an attempt by the Russian Federation to intervene in the process of military-patriotic education of Ukrainian youth, including future military specialists.

At the same time, this period was characterized by the intensification of "military-patriotic" organizations in Ukraine, especially "cossack", which received support at the state level, ensuring their activities by central executive bodies, including the Ministry of Defence of Ukraine. Thus, the resolution of the Cabinet of Ministers of Ukraine in 2011 established the Coordination Council for the Development of the Cossacks in Ukraine, one of the tasks of which was military-patriotic education and pre-conscription training of youth [9]. The Council included officials at the level of deputy ministers, the head of the Synodal Department of the Ukrainian Orthodox Church for Pastoral Care of the Cossacks and Spiritual and Physical Education of Youth, representatives of public "Cossack" organizations from different regions of Ukraine, and the "chief ataman" of the international public organization "Faithful Cossacks" as the secretary of the Council O. Selivanov. The "Chief Ataman" organized marches of "Cossacks", "Orthodox-patriotic" camps for children, and events with the participation of cadets and lyceum students, etc.

In order to implement the resolution, the order of the Minister of Defence of Ukraine dated 22.06.2012 № 424 "On organizational, informational and logistical support of the

Coordination Council for the development of the Cossacks in Ukraine" was issued. In particular, the Department of Social and Humanitarian Policy of the Ministry of Defence of Ukraine was responsible for ensuring the work of the Ministry with the Secretariat of the Coordinating Council, participation in the preparation of the draft work plan of the Coordinating Council for Cossack Development in Ukraine, assisting the Coordinating Council Secretariat in organizing and implementing the annual plan activities, processing the materials of the Coordinating Council meetings and submitting them to the Secretariat of the Cabinet of Ministers of Ukraine, submitting materials to the Department of Press and Mass Media of the Ministry of Defence of Ukraine them on the official website of the Ministry of Defence of Ukraine, providing it with rooms in the Central House of Officers of the Armed Forces of Ukraine for conferences, seminars, meetings and other military-patriotic events, etc.

In particular, in September 2012, the Central House of Officers hosted a meeting of the Coordinating Council with the participation of leaders of Cossack organizations, representatives of the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, which considered the draft Concept of Cossack Development in Ukraine and a round table discussion topic "Military-patriotic education and pre-conscription training of youth, organization of cooperation of Cossack organizations with military commissariats and units in the Armed Forces of Ukraine as important areas of formation of citizens' readiness for military service" was held. In addition, the work plan of the Coordination Council for 2012 provided for the establishment of seven working groups, including patriotic education of youth, spiritual education of youth and children, military-patriotic education and pre-service training of youth. The content of the activities of other working groups was associated with the participation of the Cossacks in public work and provided for the protection of public order, state border, overcoming the consequences of emergencies, which indicates the likely use of "Cossacks" along with representatives of security and defence

forces of Ukraine.

At the same time, the “Faithful Cossacks” was part of the “Union of Cossack Troops of Russia and Abroad” (Russian Federation), one of whose tasks was to create controlled pro-Russian Cossack structures to influence the development of the situation and the authorities, spreading the idea of creating a single Slavic state. The organization was funded through the International Fund for Support of the Cossacks, established in October 2009 at the initiative of the Union of Military Cossack Societies with the support of the Council under the President of the Russian Federation on Cossacks. During the visit of its representatives to Kyiv, an agreement was signed with the leadership of the International public organization “Faithful Cossacks” on cooperation, funding and a program of further joint actions.

Also, the fact that O. Selivanov was appointed acting Ukrainian State Center for Extracurricular Education of the Ministry of Education and Science, Youth and Sports of Ukraine in 2012 deserves attention. In March 2013, he was released by order of D. Tabachnyk, but later that year he became acting director of the Department of Social and Humanitarian Policy of the Ministry of Defence of Ukraine. At the request of the Prosecutor General’s Office of Ukraine, the Ministry of Defence of Ukraine in September 2013 clarified to the Union of Officers of Ukraine that “at this time Oleksiy Serhiyovych Selivanov is not working in the mentioned ... position”.

Further events testified to the direction and purpose of this “Cossack” organization's activity in Ukraine. At the end of 2013, O. Selivanov “carried out activities against Euromaidan supporters, formed Cossack squads to oppose protesters, spread separatist sentiments among the general population of Ukraine, and together with his accomplices provoked and incited Ukrainian citizens to seize government buildings and hold local referendums on the federalization of certain regions of Ukraine”. After the beginning of the armed conflict with the Russian Federation in 2014, he held protest and information rallies aimed at discrediting the Ukrainian authorities, its policy aimed at rapprochement with Western countries, repeatedly expressed his pro-Russian and anti-Ukrainian sentiments, and

recruited mercenaries for terrorist activities.

Some representatives of this organization in the period from April to October 2015 in order to prevent the implementation of partial mobilization and conscription into the Armed Forces of Ukraine and intimidation of the population of Kyiv were preparing to commit a terrorist act. In particular, they organized weekly practical classes on tactical and sabotage training in one of the forests of Kyiv region, created a group and developed a plan for a terrorist act in one of the district military enlistment offices of the city. However, they were detained by officers of the Security Service of Ukraine.

Later, O. Selivanov joined the ranks of illegal armed groups in the Luhansk region [10]. In addition, the head of the public organization “Union of Cossack People of Luhansk Region” (Luhansk region), “Supreme Ataman” of the public organization “Union of Cossacks of Donbas” (Donetsk region), who were also members of the Coordinating Council for Cossack Development in Ukraine, remained on the temporarily occupied districts of Donetsk and Luhansk regions, cooperating with occupation administrations and illegal armed groups.

In late December 2018, a court decision banned the activities of the Faithful Cossacks public organization for actions aimed at forcibly changing the constitutional order, violating Ukraine's sovereignty and territorial integrity, promoting war, violence, inciting interethnic, racial or religious hatred.

Conclusions

In 2010–2013 – on the eve of the armed aggression of the Russian Federation against Ukraine – there was an intensification of public organizations that declared patriotic orientation, but in practice carried out anti-Ukrainian activities, which testified to the deliberate hidden influence of the Russian Federation on the military-patriotic education in the Armed Forces of Ukraine. This state of affairs was conditioned by inconsistent activities of state authorities and military authorities, which led to the exile of pro-Russian individuals to reduce the level of combat capability of troops (forces) of the Armed Forces of Ukraine and motivate them to repel external aggression.

References

1. Valihurskyi, Yu. (2013), “Naivazhlyvishe z zhyttia Synodalnoho viiskovoho viddilu UPTs za 2012 rik” [The most important thing in the life of the Synodal Military Department of the Ukrainian Orthodox Church in 2012], *Vira i chest*, No. 1, pp. 32–37.

2. Tkachuk, R. (2013), “Dorohoiu do khramu” [On the way to the temple], *Viisko Ukrainy*, No. 04, 64 p.

3. (2013), “Pershyi v novitnii istorii Ukrainy viiskovyi khresnyi hid” [The first military procession in the recent history of Ukraine], *Vira i chest*, No. 1, pp. 58–61.

4. Tkachuk, R. (2013), “Ministr oborony, yakyi buduie khramy” [Minister of Defence, who builds temples], *Vira i chest*, No. 1, pp. 6–11.

5. The Order of the President of Ukraine (2011), *“Pro vidznachennia v Ukraini deiakykh pamiatnykh dat ta profesiinykh sviat No 1209 vid 30.12.2011”* [*On the celebration of some memorable dates and professional holidays in Ukraine*], available at: https://cutt.ly/wkzqoZb (accessed 2 February 2021).

6. Mamchak, M. (2014), *“Aneksiia Krymu. Anatomiia «hibrydnoi» viiny”* [*Annexation of Crimea. Anatomy of "hybrid" war*], Sevastopol, Ukraine, 522 p.

7. Sokoliuk, S.M. (2019), “Diialnist ukrainskoi tserkvy z vykhovannia osobovoho skladu VMS ZS Ukrainy (1992–2014)” [Activities of the Ukrainian Church on the education of personnel of the Navy of the Armed Forces of Ukraine], Ukrainian army: modernity and historical retrospective, *Proceedings of the All-Ukrainian scientific-practical conference*, Kyiv, 29 November, pp. 155–156.

8. *Reports to the Minister of Defence of Ukraine and his deputies for 2007–2013 from 18.05.2007 to 23.05.2013.*, Fund 6829. Inventory 1P. File 3. Kyiv: Sectoral state archive of the Ministry of Defence of Ukraine.

9. The Resolution of the Cabinet of Ministers of Ukraine (2011), *“Pro utvorennia Koordynatsiinoi rady z pytan rozvytku kozatstva v Ukraini No 885 vid 01.08.2011 r.”* [*On the establishment of the Coordinating Council for the Cossacks in Ukraine*], available at: https://cutt.ly/ekzqvTI (accessed 2 February 2021).

10. The official site of Center for Research of Signs of Crimes against the National Security of Ukraine, Peace, Humanity, and the International Law (2021), *Selivanov Aleksej Sergeevich*, available at: https://cutt.ly/4kzqQm8 (accessed 2 February 2021).

Anatolii Pavlikovskyi
PhD (Military Sciences), Associate Professor
Chief of the Centre for Military Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-0637-368X

Oleksandr Dublian
PhD (Military Sciences)
Leading Scientific Research Fellow of the Central Research Institute of the Armed Forces of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0001-5129-3913

Volodymyr Bohdanovych
Doctor of Technical Sciences, Professor
Principal Scientific Research Fellow of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-0481-9454

ANALYSIS TRAINING CONCEPT FOR THE SECURITY AND DEFENCE SECTOR OF UKRAINE

The concept of analysists training for the security and defence sector is presented, which defines the main provisions and recommendations for the implementation of a comprehensive multileveled continuous educational process of their training on the basis of Ivan Cherniakhovskyi NDU and its structural units. The main functions of analysists for the needs of the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, as well as for the needs of the SDS management bodies have been determined by the methods of expert survey and generalization. The basic requirements to the lists of knowledge and skills of analysists are defined. It is recommended to build the information component in the structure of informational and analytical support of a certain level of military security at the national level.

It is proposed to introduce in the educational process the

training of analysists on the basis of higher education with a two-year term of study at the NDU or in its structural units after accreditation of the specialty and obtaining a license in the prescribed manner.

Keywords: *databases, information and analytical support, the concept of analysists training, training of analysts.*

Introduction

Problem statement. Multifaceted and dynamic changes in the modern world require constant improvement of the existing system of military security of Ukraine. Effective and timely information on the real situation on the state of security and defence sector entities and threats in need of neutralization is required to develop and make decisions on the formation and management of integrated capabilities to counter military threats. Sufficient attention is now being paid to these issues. This is manifested in the development of appropriate concepts of national security in various fields, based on the results of research conducted by government agencies and individual researchers.

The analysis of recent researches and publications. According to the experts [1], the activities of government agencies have not developed an integrated system of information and analytical support for decision-making to ensure a certain level of national (military) security. Existing information and analytical structures of the state are not united into a single information network, use different methods for making calculations and have an insufficient level of automation of the process of managing security and defense actors in crisis situations [2]. There are no specialists for the above tasks and the system for training analysts for the needs of the security and defense sector of Ukraine has not been developed.

Purpose of the report is to outline the concept of training analysts for the Ukrainian security and defense sector.

Main part

Depending on the existence of national security (NS) threats, the nature of the information required for government authorities to

make decisions in order to maintain the necessary level of national (military) security of the state changes rapidly, and the array requiring processing and analysis can be limited. All of this requires the creation of a national system of information and analytical support and automation of the process of managing the integrated capacity to counteract threats to the national security and military nature [3].

This approach will expand the capabilities of Ukraine's military security system to maintain stability in the face of a wider range of threats, not only of a military nature. Precise calculations, simulating the situation and forecasting its further development will make it possible to make balanced decisions to eliminate a threat of a military nature primarily through non-military measures and, if they are ineffective, to neutralize them using military-political, military-technical, military-economic, informational and other measures [4].

Proceeding from the essence of information-analytical support as one of the types of information support, the system of information-analytical support to be created should be a single contour of cooperating structures that will provide information-analytical support to decision-making [5].

The functions of such a system are determined primarily by such existing capabilities of information technology:

– reliable storage and prompt access to large volumes of documentary and reference information;

– automated support of information processing procedures (analysis, modeling, forecasting and expert evaluation);

– external and internal communications, as well as support for access to remote information sources and funds;

– automated support of technological procedures for paperwork (registration, sorting, reproduction, editing, printing, design, and publication.)

– support of individual and collective work with information [6].

The purpose of the system should be to identify in advance the causes, conditions and signs of military and hybrid threats and to inform the decision-maker for timely introduction of adequate

military and non-military countermeasures [7].

Overall, there are currently two levels of information and analytical support. Information and analytical support that is now used to determine the level of military security is primarily an information and reference support, not an information and analytical support. The state and military administration bodies are mainly engaged in finding and implementing operational solutions to current military security problems. There are no long-term forecasts of the situation development, and medium-term forecasts are descriptive; there are no scenarios of the situation development in specific areas of national security and their impact on the military sphere based on valid benchmarks and indicators.

This is primarily due to the principal theoretical difficulties caused by the low level of training of analysts and the lack of objective models and methods, which with a high level of reliability and adequacy would allow to describe and study complex processes under conditions of incomplete, unreliable, and inaccurate information (data.) Furthermore, the information and analytical structures of government agencies employ specialists who do not have practical experience and knowledge or skills in analytical work under military threats [8].

At the same time, the potential of the existing situation centers is not fully utilized, and the capacity of modern technical means of data processing and transmission in a single format for the benefit of all actors in the security and defense sector is insufficient.

In view of this, there is a need to develop recommendations for the implementation of full and adequate information and analytical support for the process of managing the integrated capacity to counter threats of military nature.

Analysis of the information component of support in the structure of information and analytical support to maintain a certain level of military security has shown the need to build it at the national level. Therefore, work at this level (filling of databases) should be organized including not only the capabilities of public authorities, individual actors in the security and defense sector, but also society as

a whole and personal intellectual resources of individual citizens.

However, in the common database and databases of the system elements it is proposed to have information units, which are grouped according to the national security threat passports and are used to form and manage the integrated potential for counteracting the threat that has arisen. Within the framework of a unified automated information system of database formation is possible in the following areas:

– military-political;
– military-strategic;
– military-economic;
– military-technical;
– military-cybernetic;
– informational and psychological impact and others [8].

The mentioned directions of database formation should correspond to the list of threats to the national security of Ukraine and corresponding priorities of the state policy in the spheres of national security and defense, which are defined in the National Security Strategy of Ukraine [9], the Military Security Strategy of Ukraine, the Cyber Security Strategy of Ukraine, other documents on national security and defense in the medium- and long-term perspective.

The analytical component of information and analytical support for the management of the integrated capability to counter military threats is also important:

– soundness of decisions due to application of effective methods of information processing and analysis, including unclear ones;

– efficiency of tasks of analysis, assessment and forecasting of any situations [10].

For this purpose, in the structure of the analytical level of the system of information-analytical support and automation of integrated potential management in the conditions of military and hybrid threats, it is proposed to have a set of interconnected models, namely:

the military-political model of the state;

a model of threats to the state's military security (model of data identified at different times and predicted threats of military nature, each of which is described by the characteristics of a typical threat passport);

a model of a system for monitoring threats to the state's military security (a procedure for identifying threats to which the military security system should respond effectively);

the model for evaluation of the level of military danger and capabilities in terms of its de-escalation (the model allows quantitatively, within the limits of 0 to 1, to evaluate the level of military danger on the basis of a set of revealed threats both for a certain period of time and for a selected perspective);

a model for evaluating the required capabilities of force and non-forceful forces and means (makes it possible to determine the required capabilities of the military security system to neutralize a certain (predicted) level of military danger. By solving the reverse task, the model makes it possible to determine the necessary forces and means (potential is needed) to ensure the formation of the required capabilities, which, in turn, depend on many factors, of which the military and political model of a state is a determining factor).

a model of forming a set of variants of integrated potential (the model allows not only to form several variants, but also to rank them by certain indicators, for example, by efficiency of de-escalation of the revealed level of military danger, by duration of carrying out, by number of involved persons, etc.).

Thus, the current state of information-analytical support and automation of management of the integrated potential for counteracting military threats does not allow to ensure the full realization of the potential of the security and defence sector to neutralize military threats. That is why it is necessary to organize systematic training of analysts and relevant analytical structures for individual actors in the security and defence sector [11].

Training, retraining and advanced training of analysts for the needs of the SDSU, government agencies and local governments

requires the implementation of a *comprehensive* multi-level continuous educational process on the basis of the National Defence University named after Ivan Cherniakhovskyi and its structural units [12].

Analysts should be prepared to perform the following key functions (tasks):

for the needs of the MoD of Ukraine and GS of AF of Ukraine:

– to conduct and generalize the results of the monitoring of the impact on military security of the processes taking place in various spheres of life, religious environment and interethnic relations, to forecast trends of changes taking place in them and potential threats to military (national) security;

– to evaluate the effectiveness of measures to ensure military security and predict their destructive impact on national security in its determinant areas;

– to substantiate the projects of managerial decisions to ensure information security of command and control systems of troops and weapons, to protect the information space, information and information resources of the military sphere, to counteract destructive information and psychological effects on the personnel of the Ukrainian Armed Forces, population, society and state;

for the needs of SSU management bodies:

– to conduct and summarize the results of monitoring the impact on national and military security of the processes occurring in the sphere in which the governing body of the SDSU subject operates, to forecast the trends of changes occurring in this sphere and potential threats of both military and hybrid nature;

– to evaluate the effectiveness of measures to ensure national security in the sphere in which the SDSU subject operates, and predict their impact on ensuring a certain level of military security of the state;

– to substantiate the projects of managerial decisions to ensure national security in the sphere where the SDSU subject operates [13].

Analysts need to know:

– system analysis, modeling and forecasting methods;

– theoretical basics of construction, functioning and

efficiency evaluation of complex systems;

– operations research and optimization methods;

– methods of research, design and evaluation of the effectiveness of management activities;

– information processing methods;

– methods of detecting threats to national security, assessing their level, scale and possible losses in case of implementation.

Analysts have to be able to:

– process, structure and analyze large amounts of information;

– formalize, algorithmize, model and program complex processes;

– substantiate projects of management measures to counter the identified threats and predict their possible destructive impact on ensuring national security;

– concisely and reasonably formulate the results and conclusions obtained [13; 14].

The educational process should be aimed at:

– training of analysts (1-2 study groups based on higher education with a two-year study period at NDU or in its structural divisions after accreditation of the specialty and obtaining a license in the prescribed manner)

– retraining and advanced training of analysts (separate groups on the basis of existing training courses of NDU with a training period of 1-2 months).

The selection of trainees for training should be carried out individually according to specially developed methods. Training programs are developed in accordance with the established procedure and are agreed with the relevant customer of the sector of security and defence of Ukraine.

In the educational process, preference is given to active forms of learning, practical and independent work of students.

Analysts' master's theses must be independently peer reviewed.

To ensure the high quality of teaching academic disciplines

to scientific and pedagogical workers involved in the preparation, retraining and advanced training of analysts, by order of the commandant of NDU, an individual classroom teaching load is established for each academic year.

Conclusions

Thus, the presented concept defines the main provisions and recommendations for the implementation of an integrated, multi-level and continuous educational process for training analysts for the Ministry of Defence of Ukraine and the security and defence sector of Ukraine on the basis of NDU named after Ivan Cherniakhovskyi and its structural units.

The main functions of analysts have been determined for the needs of the Ministry of Defence and the General Staff of the Armed Forces of Ukraine, as well as for the needs of the control bodies of the sector of security and defence of Ukraine. The basic requirements for the lists of knowledge and skills of analysts are determined.

It was recommended to build the information component in the structure of information and analytical support for maintaining a certain level of military security at the national level.

References

1. Bohdanovych, V.Y., Svyda, I.Y. and Vysidalko, A.L. (2013), "Analiz mozhlyvostei systemy zabezpechennia natsionalnoi bezpeky Ukraiiny shchodo vsebichnoi pidtrymky bezpekovoho suprovodu realizatsii natsionalnykh interesiv" [Analysis of the possibilities of the ensuring system of the national security of Ukraine regarding the comprehensive support of security support for the realization of national interests], *Science and technology of the Air Force of Ukraine*, No. 3(12), pp. 5-12. https://doi.org/10.30748/nitps.2013.12.01.

2. Bohdanovych, V.Y., Romanchenko, I.S., Svyda, I.Y. and Syrotenko, A.M. (2019), "*Metodolohiia kompleksnoho vykorystannia viiskovykh i neviyskovykh syl i zasobiv sektora bezpeky i oborony dlia protydii suchasnym zahrozam voiennii bezpetsi Ukrainy: monohrafiia*" [*Methodology of integrated use of military and non-military forces and means of the security and defense sector for countering contemporary*

threats to Ukraine's military security: monograph], National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, 268 p.

3. Bohdanovych, V.Y., Svyda, I.Y. and Skulish, Ye.D. (2012), "*Teoretyko-metodolohichni osnovy zabezpechennia natsionalnoi bezpeky Ukrainy: monohrafiia u 7 t. T. 1. Teoretychni osnovy, metody y tekhnolohii zabezpechennia natsionalnoi bezpeky*" [*Theoretical and methodological bases of ensuring national security of Ukraine: monograph: 7 t. - Vol. 1: Theoretical foundations, methods and technologies of ensuring national security of Ukraine*], Scientific Publishing House of the National Academy of the Security Service of Ukraine, Kyiv, 548 p.

4. Ustimenko, O.V. (2019), "Pidvishchennya efektivnosti sistemi derzhavnogo upravlinnya pri privedenni u vishchi stupeni bojovoyi gotovnosti sil oboroni za rahunok rezervnogo konturu opovishchennya" [The increase of the efficiency of the state management system when the defense forces are brought to a higher level of combat readiness due to the reserve contour of alerting], *Collection of scientific works "The Efficiency of State Management. The efficiency of public administration" of the Lviv Regional Institute of Public Administration of the National Academy of Public Administration under the President of Ukraine*, No. 58. pp. 100–111.

5. Saganjuk, F.V., Lobko, M.M., Ustimenko, O.V. and Penkovsky, V.I. (2015), "*Sektor bezpeki i oboroni Ukraïni: zbirka naukovih materialiv*" [*Sector of Security and Defense of Ukraine: Collection of Scientific Materials*], Mayster Books, Kyiv, 174 p.

6. Podberyozkin, A.I. (2015), "Voenno-politicheskaya obstanovka blizhajshih desyatiletij: scenarii i strategii" [Military-Political Situation of the Next Decades: Scenarios and Strategies], *Development and Economy Almanac*, No. 12, 128 p.

7. Sahanyuk, F.V., Frolov, V.S., Pavlenko, V.I. and others (2018), "*Sektor bezpeki i oboroni Ukraïni: strategichne kerivnictvo ta vijs'kove upravlinnya: monografiya*" [*Sector of Security and Defense of Ukraine: Strategic Leadership and Military Management: Monograph*], CP of the Defense Ministry and the General Staff of the Ukrainian Armed Forces of Ukraine, Kyiv, 230 p.

8. Saganjuk, F.V., Frolov, V.S., Ustimenko, O.V., Lobko, M.M. and others (2017), "*Sektor bezpeki i oboroni Ukraïni: teoriya, strategiya, praktika*" [*Sector of Security and Defense of Ukraine: Theory, Strategy, Practice*], Akadempras, Kyiv, 180 p.

9. Low of Ukraine (2018), "Pro nacionaljnu bezpeku Ukrajiny No. 2469-VIII vid June 21, 2018" [On National Security of Ukraine dated

June 21, 2018], *Voice of Ukraine*, No. 122 (6877), Kyiv, 31 p.

10. Arzumanyan, R.V. (2015), *"Strategiya irregulyarnoy voyny: teoriya i praktika primeneniya. Teoreticheskiye i strategicheskiye problemy kontseptualizatsii, religioznyye i voyenno-politicheskiye otnosheniya v operatsionnoy srede irregulyarnykh voyennykh deystviy"* [*Strategy of irregular war: theory and practice of application. Theoretical and strategic problems of conceptualization, religious and military-political relations in the operational environment of irregular military operations*], Moscow, 334 p.

11. Bartosh, A.A. (2018) "Trenie i znos gibridnoj vojny" [The friction and rancor of hybrid warfare], *Voennaya mysl*, No. 1. pp. 5-13.

12. Ustimenko, O.V., Kaposloz, G.V. and Poltorak, M. (2019), "Retrospektivnij analiz pidgotovki fahivciv dlya Zbrojnih Sil Ukrayni v sistemi vishchoyi vijs'kovoyi osviti kriz' prizmu antiteroristichnoyi operaciyi" [Retrospective analysis of training of officers for the Ukrainian Armed Forces in the system of higher military education through the prism of anti-terrorist operations], *Collection of scientific works "Military Education" of the National University of Defense of Ukraine named after Ivan Cherniakhovskyi*, No. 1(39), pp. 214–226.

13. The official site of NKIBRICS.RU (2012), *"Global'nyye tendentsii 2030: Al'ternativnyye miry"* [*Global Trends 2030: Alternative Worlds*],available at: http://www.dni.gov/nic/globaltrends .

14. Gerasimov, V. (2017), "Mir na granyah vojny" [Peace on the brink of war], *Military-industrial courier*, No. 10, p. 676.

Vita Shkorubska
Postgraduate Student
of the Hetman Petro Sahaidachnyi National Army Academy
Lviv, Ukraine
https://orcid.org/0000-0001-6007-7542

ON THE TRAINING OF MILITARY SPECIALISTS IN THE REPUBLIC OF POLAND: 1989-2020

The article attempts to analyze the experience of training Polish soldiers in 1989-2020. In particular, the main stages and directions of reforming the military education system and its qualitative transformations are considered. The data regarding the collaboration of military educational institutions for the training of officers of the Armed Forces of the Republic of Poland is presented. Options of the officerstraining are highlighted. The main advantages and disadvantages of the Polish military education system are identified.

Keywords: *Military education system, educational institution, personnel in the armed forces, military schools, servicemen.*

Introduction

Problem statement. Ukraine aspires to join the North Atlantic Alliance. That is, to achieve in the army the standards of interoperability with the armed forces of NATO member states. To a large extent, the outcomes of this process depend on the training of personnel in military educational institutions. The system of military education does lay the foundation of competencies of future and servicemen, consequently the further development of the Ukrainian army pivots on them.

The Republic of Poland is considered to have a lot in common with Ukraine, especially in mentality aspects. Despite historical issues, Ukraine has managed to build friendly relations, respectful mutual relations of the two neighboring states for the period of independence.

Moreover, at the turn of the 80s and 90s of the last century, Poland had at least one, but "Soviet" system of military education. In

the process of reformation, the Allies have managed to bring it to a state that ensures proper training of troops and the possibility of their joint action with the military of partner countries. Concurrently, Poland managed to preserve the unique features of the national military school.

Purpose of the report. Studying the Polish experience will allow us to apply it to reform the domestic education system, accelerate this process and, possibly, avoid the mistakes of the neighboring country.

Main part

Inherited from the Polish People's Republic, the Republic of Poland was left with a cumbersome system of military education. Among all educational institutions, of which there were as many as 16, including 5 military academies and 11 higher officer schools. In fact, each army armand service used to have its own officer school. They provided the command staff needed for the functioning of more than 300,000 army. Almost every branch of the armed forces had a corresponding higher military educational institution. There were also 21 ensign schools and 19 NCO schools within the military education.[1].

The existing system of military education at that time had a wide educational base and pedagogical potential, allowed to teach and train much more students than it was needed at that time, more so in the future [2]. The reduction in the number of personnel in the armed forces of the Republic of Poland required a reduction in the number of military educational institutions. Poland's military education system has undergone significant changes since the early 1990.

From 1990 to 2000, we can determine the first stage of changing the system of military training in Poland [2]. It is characterized by sometimes contradictory decisions on the liquidation or merger of military schools. Somewhat a lack of strategy in building a clear system of military education. The number of military schools where servicemen were trained has been almost halved: military academies from 5 to 4, higher officer schools of

cornet officers from 21 to 11, and non-commissioned officer schools of schools, in our opinion, have not significantly improved the quality of training [3–4]. However, this situation cases, in our opinion, did not lead to a significant improvement in the quality of training.

As a result, at the beginning of the XX century it was decided to train military personnel. The essence of the issues of military education reform, which was to reform the system, was reflected in the concept prepared by the specialists of the Department of Military Education and Science of the Ministry of National Defense in 2000 [4]. The main idea of the concept was at first glance simple - the liquidation of all military training institutions for officers and - the University of National Defense, which would include the Department of Strategic Defense and Technical Faculty, as well as specific departments in other cities: ground forces in Poznan, aviation in Deblin and Naval in Gdynia and the Military Medical department in Lodz.

The concept of reorganizing military education had been developed before 2006, but it was never implemented, however calls for such reform are often discussed in the Polish military environment today.

In 2003, the Department of Military Education and Science of the Ministry of National Defense developed the following concept. It comprised of three options for changing the number of military schools. However, it was not executed.

Another fundamental fact in favor toenhance the military education was the adoption in 2005 of the law "On Higher Education". Until now, military educational institutions were governed by a separate law, which established uniform training standards for all higher education institutions. It should be noted that none of the military universities complied with the requirements of the Law on the quality of educational facilities [5]. However, it was approved to maintain the basic higher military educational institutions: the Academy of National Defense in Warsaw, where officers of operational-tactical and operational-strategic levels were

trained, the Academy of the Navy in Gdynia, the Higher Officer School in Wroclaw and the Higher Air Force in Demblen - specific universities for tactical officers and the Military Technical Academy in Warsaw as well as Cornet schools were liquidated in 2004 together with the cornet corps [6].

In our opinion, the positive factor is that the liquidated educational institutions did not disappear completely, but were converted into centers and training centers, of which there are currently 17 assets in the Polish Army.

In 2012, the leadership of the Ministry of Defense presented another draft concept for reforming the military education system. The program stated that the training of officers for the Armed Forces of the Republic of Poland would be carried out in a single military educational institution of national defense, which was planned to be formed on the basis of the following educational institutions: the Academy of National Defense; Military Technical Academy, Academy of Naval Forces, Air Force, part of the Higher Officer School of Land Forces and part of the Military Medical Institute.

The reform of the military education system of the Republic of Poland was not characterized by structural composition, but significantly affected the qualitative changes. Obviously, the main task of Polish universities in the period from 2000 to the present has been to create their own human resources. There was an acute shortage of military scientific and pedagogical workers in higher military educational institutions. In the early 2000s, the percentage of scientific and pedagogical workers in military specialties who had a scientific degree and academic rank ranged from 10 to 20 percent. Subsequently, a quality training process could not be provided [5].

In 2005, with the implementation of the Law on Higher Education, Polish higher military educational institutions became autonomous and public (the owned by the state, not the Ministry of Defense), it became part of the state's higher education system [7]. This fact gave impetus to their own development and increase of scientific and pedagogical potential. Over time, it was possible to increase the percentage of scientific and pedagogical workers in the

areas of training, obtain licenses and expand the areas of training of doctors of philosophy and doctors of sciences, etc. Officer schools in Wroclaw and Demblin were titled with the status of academies, and the National Defense Academy became the Academy of Martial Arts.

There is a clear division into didactic and organizational components in Polish higher military educational institutions. Educational is planned and organized for the school year. The main document on the organization and planning is the Plan of the basic actions for academic year. It is developed by the educational department and approved by the rector. Faculties receive extracts from the Plan of main activities, according to the scope of their activities. Departments receive copies of extracts from the Main Action Plan [8].

It is maximally to release the scientific and teaching staff from paperwork and allows you to focus on the educational process and research.

In addition, from the middle of this decade, higher military educational computer programs in Poland have switched to the use of educational support, which has many opportunities and replaces paper planning of the educational process. For example, the Academy of Land Forces in Wroclaw uses the 'Erepia' system, which was specially developed for higher military educational institutions by an IT company [8]. The system contains all the necessary information to ensure not only training but also the life of cadets - from anthropometric data to accounting for progress and the formation of documents on graduation. The system contains all the necessary information to ensure not only training but also the life of cadets, from anthropometric data to accounting for progress and the formation of documents on graduation.

The symbiosis of military and civilian education in military universities led to the broad economic independence of the latter. Today they have about 4,000 cadets, and the annual needs of the armed forces of the Republic of Poland are about 800 officers. In addition to training military personnel for the needs of the state armed forces, higher military educational institutions train civilians

for the national economy, and a significant share of such specialists is paid, which allows maintaining the financial independence of higher military educational institutions. In the last five years, the percentage of so-called "own earnings" compared to public funding was 75% to 25%, respectively [8].

Education in higher military educational institutions is divided into "academic education" ("basic education") and "vocational training" ("basic military training"). As a rule, theoretical training will be carried out in higher military educational institutions, and the practical component of training of the armed forces of the Republic of Poland.

Training in the system of military education of the Republic of Poland is carried out during the entire period of military service through in-service training in higher military educational institutions, training in courses preceding appointment and obtaining the next military rank:

lieutenant - graduation from military university (training for 5 years, all graduates receive an educational qualification level ("master") or completion of an officer's course (3-12 months) - in the presence of civil education at the "master" level;

– senior lieutenant - qualification course (commander, staff, positions of support units), 2 months;

– captain - in the centers qualification course (commander, staff, positions of support units), 2 months;

– major - postgraduate training of operational and tactical level, 18 months;

– lieutenant colonel - qualification course (commander or staff) 3 months;

– colonel - the highest operational and strategic course, 10 months;

– colonel brigadier general - postgraduate training in defense policy, 10 months.

The preparation of junior officers for the military rank of captain is carried out in military educational institutions of the armed forces officer schools. Training of senior art officers. Appointment to

a higher position and obtaining the next military rank is impossible without training in the relevant course [9].

In addition, much attention is paid to the study of English as the Academy of Military International Communication. All alumni / lieutenants must be able to complete the NATO Standard Speech Level 3232. Language proficiency in the service process is maintained in specialized language courses and postgraduate courses.

A significant qualitative feature of military education in Poland, it is advisable to pay attention to the academic mobility of both cadets and teachers. The internal exchange of cadets is widely used within the framework of receiving the academic component of military education of higher military in both Poland and NATO member countries.

In addition, there is an exchange of faculty between higher military educational institutions, as well as participation in the educational process of higher military educational institutions of scientific and pedagogical employees of civilian educational institutions (both Polish and foreign) on the principle of "visiting professor" or session instructor [8–9].

Conclusions

The system of training military specialists of the Republic of Poland has undergone radical changes for more than 30 years. It has transformed from a closed, diverse military education system to a compact, flexible and mobile one that meets NATO criteria and at the same time part of a national higher education system. According to Polish experts, the existing system of military education in Poland has a number of advantages allows, if necessary, to significant human resources for the armed forces; to meet the needs in the field of training of servicemen for professional military service and improvement of professional training of officers; has significant scientific potential. However, with the change of values, the society changes as well as the potential ones - this is the reason for the changes in the training of future defenders. Threats Military education should not be just a theory supplemented by simulators,

training on ground and practices in military units. And this is important because the modern warfare is changing, although the rules of victory and defeat have remained the same for centuries. Further study of the Polish experience will contribute to the reform of Ukrainian military education.

References

1. Burzyński, T. (2016), „Wojownicy" do szkolenia potrzebni od zaraz, *Polska-zbrojna*, available at: https://cutt.ly/lkzeOz5 (assecced 10 November 2020).
2. Ostolski, P. (2016), *Ewolucja polskiego szkolnictwa wojskowego (część II)*, *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej*, No. 4(20). pp. 28-40.
3. *Koncepcja reorganizacji szkolnictwa wojskowego opracowana w Departamencie Nauki i Szkolnictwa Wojskowego MON jesienią AD 2000*, available at: https://krzysztof.borowiak.pl/reforma.html (assecced 10 November 2020).
4. Kałużny R. (2005), *Wyższe szkoły oficerskie wojsk lądowych w Polsce w latach 1967-1997*, wyd. Uniwersytetu Zielonogórskiego, Zielona Góra, 349 p.
5. Najwyższa Izba Kontroli (2008), *Informacja o wynikach kontroli organizacji i funkcjonowania akademii wojskowych i wyŝszych szkół oficerskich ze szczególnym uwzględnieniem gospodarki finansowej i mienia uczelni oraz struktury zatrudnienia w latach 2005 – 2007*, available at: https://cutt.ly/LkzycQc (assecced 10 November 2020).
6. Serwis Rzeczypospolitej Polskiej (2020), *Szkolnictwo wojskowe*, available at: https://cutt.ly/wkzteWt (assecced 10 November 2020).
7. Kancelaria Senatu. Biuro analiz i dokumentacji (2015), *Wyzwania stojące przed polskim wyższym szkolnictwem wojskowym w XXI w*, available at: https://cutt.ly/7kztSv5 (assecced 10 November 2020).
8. National Army Academy named after Hetman Petro Sahaidachny (2014), *Report on the participation of the delegation of the National Army Academy named after Hetman Petro Sahaidachnyi in the internship of research and teaching staff of higher military educational institutions of the Armed Forces of Ukraine in higher military educational institutions of the Republic of Poland*, 52 p.
9. Wojsko-polskie.pl (2020), *Historia wojskowego szkolnictwa*, available at: https://cutt.ly/kkzpRhw (assecced 10 November 2020).

Vasyl Stasiuk
Doctor of Psychological Sciences, Professor
Professor of the Department of Moral and Psychological Support
of the Activity of the Troops (Forces) of the National Defence
University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-4996-4041

Leonid Oliynyk
Candidate of Pedagogical Sciences, Senior Research
Head of the Scientific and Methodological Department of Analysis
and Forecast of Educational Activities of Methodical and Scientific
Centre of Educational Activity Organization of the National Defence
University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-7375-1281

RESULTS OF EXPERIMENTAL STUDY ON MILITARY AND SOCIAL COMPETENCE DEVELOPMENT OF MASTERS OF MILITARY AND SOCIAL MANAGEMENT

The article considers the stages of arranging and conducting a pedagogical experiment and results of military and special competence development of masters in military and social management by using comprehensive structure-functional technology of military and special subjects teaching. The experimental study was considered and the process of summative and formative assessment on the development of military and special competence of masters of military and social management was laid down. The results of experimental study of military and special competence development in the process of teaching military and special subjects to students of higher military educational institutions were consolidated; military and special competence development levels of masters of military and social management were analyzed. The validity of the results received was proved using Mathematics Statistics methods.

Keywords: *experiment, education, military and special subjects, masters of military management, methodical system, technology, military and special competence.*

Introduction

Problem statement. The current status of the Armed Forces of Ukraine and the XXI century realities witness that in addition to traditional threats of local wars and armed conflicts, terrorism in its all aspects constitute considerable threat to the mankind. This requires fundamentally new approaches to arranging educational process, setting up and implementing educational and training methodological systems, which might ensure comprehensive development of a personality and his/her self-actualization in social as well as in military and professional environment.

The analysis of recent researches and publications. Ukrainian army holds one of the principal places in the social institutes system, where military service facilitates establishment of conditions and activities, aimed at learning and mastering by military personnel of military and special knowledge on moral and psychological support of forces and social experience to establish socially positive value-based landmarks [3, p. 58].

Bearing in mind steady increase of the role of spiritual as well as moral and psychological components in Ukrainian Armed Forces' routine activities, teaching of military and special subjects to highly skilled officers, masters of military and social management, at higher military educational institutions acquires particular importance. Professional activities of such specialists directly contribute to moral of forces and their combat readiness.

One of the priority tasks in teaching military and special subjects to officers, specializing in ""Military and Social Management", is to develop their military and special competence as they are directly responsible for educating and mentoring of military personnel. This conclusion was made on the basis of the content analysis of masters' of military and social management duties and responsibilities. The results of the analysis showed that 80 % of their duties and responsibilities concern personnel management, military and ideological training, moral shaping, studying of moral and business qualities, etc of their subordinates.

Methodological foundations of education, which define target- (objective), content- and procedure-oriented characteristics of military and special subjects in general and military special competence in particular, have been covered by research papers of numerous scholars (O. Boyko, O. Torichnyi, V. Yahupov and others [1; 4–5]).

Purpose of the report is to experimentally confirm the efficiency of task-oriented development of military and special competence of masters of military and social management, subject to introducing the comprehensive structure-functional technology related to teaching of military and special subjects into educational and training process of higher military educational institution.

Main part

Research and experimentation assessment of the efficiency of military and special competence development system of masters of military and social management is principal stage of our study and its main objective is to verify hypothesis, which was put forward. It consists of the assumption that the professional competence of masters of military and social management increases subject to implementation of scientifically based military and special subjects' methodology teaching system and goal-oriented development of military and special competence on the bases of the scientifically based comprehensive structure-functional technology.

Pedagogical experiment within the research became a logic continuation of theoretical research and the main method to confirm its validity, assess efficiency and practical importance for developing military and special competence of masters of military and social management.

Formative assessment was the final stage. The aim of the formative assessment was to define the elements of military and special competence that facilitate development of professional competence of masters of military and social management in higher military educational institutions and to conduct pilot testing of

experimental programme of the military and special competence development of masters of military and social management within the educational and training process.

The aim of formative and comparative stages of the pedagogical experiment was to confirm the efficiency of methodological system that has been developed to teach military and special subjects to masters of military and social management. Formative stage of the pedagogical experiment involved 111 students specializing in "Military and Social Management" from Humanitarian Institute of the National Ivan Chernyakhovskyi Defence University of Ukraine, National Guard of Ukraine National Academy, National Bogdan Kmelnytskyi Border Guard Academy. Shaping experiment included one experimental group (57 students) and one control group (54 students). Education process within the control group was conducted in accordance with traditional methodology of teaching military and special subjects, and within experimental group – on the basis of the comprehensive structure-functional technology to deliver the contents of education.

The following components should be considered to ensure quality assessment of military and special competence development level among Master Degree holders in military and social management.

Motivational and value-based component is characterized by professionally significant requirements of career development, desire to increase his/her proficiency, status and credibility in carrying out managerial functions when dealing with personnel; management motives related to moral and psychological support within unit (formation), established attitude and developed value orientations in relation to management activity; by desire and showing interest to work in structures responsible for morale of military personnel.

Cognitive component includes knowledge and objective perception of peculiarities of a Master Degree holder in military and social management military and professional activities. The other element of this component is the ability to assess problematic situations related to carrying out professional activities.

Operational and activity component is characterized by the ability to use methods, procedures and skills of analysis, fusion, consolidation and comparison of information; possessing military and special skills to arrange moral and psychological support of routine activities within unit; ensuring implementation of commander's (chief's) decisions to educate and train military personnel; leading education and training activities of subordinates; planning and arranging moral and psychological support of training and combat-related activities; using most relevant management style to ensure education and training of military specialists under fast changing conditions.

Personality component of military and special competence is a kind of quintessence of the previous components and it means that a Master of Military and Social Management is totally autonomous in his/her military and professional activities. The personality component includes self-control, flexibility, tranquility, resilience, patience, reliability and firmness in implementing managerial function by Master Degree holders in military and social management related to educational activities in a military unit; it envisages observing ethic principles in taking decisions related to carrying out education of military personnel; the ability to manage the actions which constitute implementation of one's own functions and responsibilities of his/her subordinates in any situation; ability to adjust emotional states, which appear in carrying out managerial activities.

Comparative analysis of the experimental group and control group results at the beginning and the end of the shaping experiment is provided in the table 1.

The comparative stage results within the experimental and control groups allow drawing conclusions regarding the advantages of efficiency indicators of methodological system of teaching military and special subjects, and military and special competence development technology employed for educating students of the experimental group. The results of the pedagogical experiment prove that implementation of the methodology system of military and

special subjects teaching facilitates the development of military and special competence development of masters of military and social management. Hence, the creative and high levels of the military and special competence development within the experimental group increased from 43.8% up to 61.5% (by 17.7%), the number of students having the low level reduced from 15.8% down to 3.5% (by 12.3%). The creative and high levels of the military and special competence development within the control group increased from 46.3% up to 51.9% (by 5.6%), while the number of the students having the sufficient level remained without changes.

Table 1

Comparative analysis of the experimental group and control group results

Groups	Students' military and special competence development levels, %							
	Creative		High		Sufficient		Low	
	At the beginning of the experiment	At the end of the experiment	At the beginning of the experiment	At the end of the experiment	At the beginning of the experiment	At the end of the experiment	At the beginning of the experiment	At the end of the experiment
EG n=57	15,8	26,5	28	35	40,4	35	15,8	3,5
CG n=54	14,8	16,7	31,5	35,2	38,9	38,9	14,8	9,2

The upward trend of the military and special competence development levels was achieved for the masters of military and social management, which proves the efficiency of the proposed by us methodology system for teaching military and special subjects.

Solution of a problem to assess the efficiency of military and

special competence development of masters of military and social management technology can be demonstrated by way of the following algorithm:

1. Calculation of the average score for each of the groups: $y_1 = 76,\ y_2 = 70$. The technology efficiency was assessed on the total score of expert assessment of the military and special competence of Master Degree holders in military and social management development level. The efficiency of the technology to develop military and special competence of Master Degree holders in military and social management was assessed on the total score of students' and the group in general, as a result of the expert assessment by all indicators of their performance when carrying out military and special tasks. Consolidated results of the expert assessment were defined for each student.

2. The average mean for two groups is calculated by the following formula:

$$\overline{y} = \frac{n(\overline{y_1} + \overline{y_2})}{2n} = 73,$$

where n – the size of each sample, 2 – the number of military and special competence development technologies within the process of military and special subjects teaching methodology, employed the process of education.

3. Definition of factorial and residual variances. The size of the article does not allow presenting all data of the check measurement. Its consolidated data are presented as a sum of results of every student of control group and experimental group.

$$\delta_{res}^{-2} = \sum_i \sum_j (y_{ij} - \overline{y}_i)^2 = 17303. \quad (1)$$

Let us formulate the hypotheses (assumptions).

H_0 – increase of the development levels of military and special competence of experimental group students as a result of employment of the military and special subjects efficient methodology teaching system which military and special competence development technology is a part of, shall be accidental;

H_1 – increase of the development levels of military and special competence of experimental group students as a result of employment of the military and special subjects efficient methodology teaching system which military and special competence development technology is a part of, shall be substantial.

The factorial variance is calculated by the following formula:

$$\delta_{fact}^{-2} = \sum_{i}^{2} n_i (\overline{y}_i - \overline{y})^2 = 57 \cdot (76-72)^2 + 54 \cdot (70-73)^2 = 999, \qquad (2)$$

where n_i – the size of certain group.

The residual variance is calculated by:

$$\delta_{res}^{-2} = \sum_{i} \sum_{j} (y_{ij} - \overline{y}_i)^2 = 13307. \qquad (3)$$

The value of empirical statistic criterion is calculated:

$$\delta_{res}^{-2} = 13307; \ \delta_{fact}^{-2} = 999;$$

$$F_{emp} = \frac{\delta_{res}^{-2}}{\delta_{fact}^{-2}} = \frac{13307}{999} = 13,32.$$

F_{crit} is defined in accordance with significance value $\alpha = 0,05$ the number of freedom degrees of numerator 1 and the number of freedom degrees of denominator $n-2=109$.

In accordance with the table – criterion [2] (F – value $p = 5\%$) shall be calculated:

$$F_{crit}(0,05;1;109) = 4,8 \qquad F_{emp} = 13,32 > F_{crit} = 4,8.$$

Consequently, H_0 shall be rejected, H_1 shall be accepted, increase of the development levels of military and special competence of experimental group students as a result of employment of the military and special subjects efficient methodology teaching system which military and special competence development technology is a part of, shall be substantial ($p \le 0,05$).

Conclusions

Thereby, the military and special competence development level is lower in the control group than in the experimental group. This proves the efficiency of the methodology system of teaching military and special subjects, which was developed and the military and special competence development technology of Master Degree holders in military and social management.

References

1. Boyko, O.V. (2005), "*Formuvannya hotovnosti do upravlinskoyi diyalnosti u maybutnikh mahistriv viyskovo-sotsialnoho upravlinnya: dys. … kand. ped. nauk*" [*Formation of readiness for managerial activity in future magistrates of higher social management: dissertation*], Kyiv, 476 p.

2. Kyveryalh, A.A. (1980), "*Metody yssledovanyya v professyonalnoy pedahohyke*" [*Research methods in professional pedagogy*], Valhus, Tallyn, 336 p.

3. Oliynyk, L.V., Rudenko, M.V., Osodlo, V.I. and Bohaychuk, V.Z. (2013), "*Sotsialna viyskova pedahohika:pidruchnyk:u 2 ch. CH. I. Teoretyko-metodolohichni osnovy*" [*Social military pedagogy. Theoretical and methodological foundations*], NUOU, Kyiv, 348 p.

4. Torichnyy, O.V. (2013), "*Teoretyko-metodychni zasady formuvannya viyskovo-spetsial'noyi kompetentnosti maybutnikh ofitseriv-prykordonnykiv u protsesi navchannya: avtoref*" [*Theoretical and methodological principles of formation of higher-special competence of future border guards in the process of training: abstract*], Kyiv, 38 p.

5. Yahupov, V.V. (2002), "*Zahalnodydaktychni osnovy navchannya viyskovosluzhbovtsiv strokovoyi sluzhby Zbroynykh Syl Ukrayiny*: *avtoref.*" [*General didactic bases of training of senior servicemen of the Armed Forces of Ukraine: abstract*], Kyiv, 26 p.

6. Boyko, O.V. (2005), *Formation of readiness for managerial activity in future masters of military and social management: dissertation*, Kyiv, 476 p.

Hryhoriy Tikhonov
Candidate of Military Sciences
Senior Researcher of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-1941-744X

Leonid Kryuchka
Postgraduate Student of the National Defence University
of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-8767-5091

EDUCATIONAL STANDARDS FOR CYBER SECURITY TRAINING AND THE STATE OF THEIR TRAINING IN THIS FIELD

On the basis of the system analysis of process of preparation of experts in cybersecurity the questions of standardization of preparation of the given experts are investigated, actual problems of standardization of education in this sphere at the present stage are revealed, the directions of their specialization are offered. The study aims to improve the system of training cybersecurity professionals to a level that will ensure the ability of cyber units to perform tasks as assigned.

Keywords: *cybersecurity specialist, educational standards, training, educational content, educational programs, IT industry.*

Introduction

Problem statement. The war in eastern Ukraine raised the question of the need for the training of a fundamentally new category of specialists in the protection of the country's cyberspace. Therefore, special attention should be paid to the educational standards of training of cybersecurity professionals and the state of their training.

The use of cyber units in joint operations in the east of the country pointed to a number of shortcomings in the system of training cybersecurity professionals, namely: a number of errors and

miscalculations in the educational activities of Ukrainian educational institutions; imperfection of educational standards for training cybersecurity specialists; imperfection of the system of training specialists in this area.

The analysis of recent researches and publications. An analysis of recent research and publications that address the issue of training cybersecurity professionals in the country shows that while paying tribute to scientific developments in this area, it should be noted that research on cybersecurity training is not yet coordinated and systematic, and developments in this area poorly coordinated between research institutions and researchers.

The lack of generally accepted theoretical developments on this topic and relevant recommendations that would correspond to today's realities reduces the effectiveness of the system of training specialists in cybersecurity.

Given that the formation of modern educational standards, strategies and development of national higher education will increase the effectiveness of the system of training specialists in cybersecurity of the Armed Forces of Ukraine, research on these issues is relevant.

Purpose of the report. The purpose of solving the problem of analysis of educational standards for training of specialists in cybersecurity and educational activities of Ukrainian higher education institutions is to promote the training of these specialists.

Main part

Analysis of the system of training cybersecurity specialists for the Armed Forces of Ukraine indicates a number of shortcomings in the educational standards of training and in the system of educational activities of Ukrainian higher education institutions [1].

Regarding the study of the standardization of training of cybersecurity specialists: the standards of higher education (Law of Ukraine "On Higher Education" (2014)) are not about the content of education, what exactly should be taught, what subjects and topics to include in the curriculum, but about the essence of the higher education institution.

When considering the training of cybersecurity professionals, it is proposed to direct their training with more specific instructions, namely: what and how to teach, for what training time, how to check the quality of training of future professionals [2–4].

Requirements for educational standards are based on the principles of autonomy of higher education institutions. The standards of the previous generation provided for a certain set of disciplines with a certain number of hours devoted to their teaching. The standards of the new generation are focused on learning outcomes, and the content of education should be formed by the higher education institution itself. At the same time, the drafters of the Law of Ukraine "On Higher Education" failed to give everything in the standards of higher education to the educational institutions themselves [5]. This Law leaves to the central executive body in the field of education and science the right to establish standards of higher education for each specialty.

It is proposed to standardize the requirements for the educational program, provided for the requirements of professional standards, to provide and formulate: normative content of student training, list of graduate competencies, the amount of credits for each degree not higher than the number and description of disciplines, but through learning outcomes and requirements for the system of internal quality assurance of education.

When creating standards for the training of cybersecurity specialists for the Armed Forces of Ukraine, higher education institutions should take into account the programs and proposals of military units, on the basis of which job descriptions for cybersecurity specialists are concluded. This will be able to bring the standards of education of these specialists as close as possible to the needs of military structures and make the educational process as effective as possible [6–7].

During the standardization of education for the specialty "cybersecurity" important issues were not addressed, namely: what educational programs should be given priority, in what proportion should be presented the actual theoretical and practical components of the learning process.

In our opinion, the modeling of educational standards in the field of "cybersecurity" should be based on the general concept of understanding that in general the list of disciplines of professional and practical training of higher education seekers in this specialty looks somewhat unsystematic and detached from the needs of practice. It is offered in educational programs of training of experts in cybersecurity to give preference to practice-oriented disciplines and a foreign language, increasing time for formation of practical skills and only then - to general disciplines [8].

It should be noted that the main problem of standardization of training processes in the field of cybersecurity is that today this type of professional activity is outside the clearly defined legal field, such activity is not provided by state standards or clearly defined qualifications approved in the state order levels. Therefore, the modeling of educational standards in the specialty "cybersecurity" should be based on the general concept of understanding this concept in science and law [9–10].

Regarding the state of training of cybersecurity specialists, it should be noted that the effectiveness of training of specialists in the world's leading countries is ensured by constantly updating the content of education in educational institutions in accordance with the needs of the state and its armed forces. Students at U.S. educational institutions have the right to freely choose courses / disciplines to study, but they are required to adhere to certain prerequisites for mastering the program of the previous course of study. When training cybersecurity specialists, 2-3 hours of independent work and practical classes are allocated for 1 classroom hour; the lecture lasts 75 minutes [10].

In the Ukrainian model of education, the lecture lasts 90 minutes, for 1 classroom lesson on independent work is not provided. The institution of higher education offers the student a systematic, consistent approach to the choice of disciplines and programs, and the student can not change the content of education. According to the Law of Ukraine “On Higher Education” (2014), only 25% of disciplines of free choice of specialist are provided. In Ukrainian

educational institutions lectures are mainly dominated, in many disciplines practical classes are not planned at all [11].

Practical training in American and Ukrainian educational institutions is the final stage of all training. In the United States, it is implemented through a combination of university studies and the acquisition of practical skills in the future workplace with a salary. In Ukraine, applicants independently organize the place of practice.

The analysis of the American experience of training specialists in the specialty "cybersecurity" allowed to determine the possibilities of using its progressive ideas in the system of higher education in Ukraine, in particular: providing information support of reference Internet resources; development and improvement of practical training of cybersecurity specialists on the American type, which is carried out on the basis of an integrative combination of university studies and acquisition of practical skills in the future workplace or place of work, use of a wide range of innovative forms and methods of training [12].

The Ministry of Defense of Ukraine is concerned about the scope of practical training of future cybersecurity professionals, as there is a significant gap between the requirements of today and the practical results of educational activities of higher education institutions in Ukraine, namely: lack of skills and knowledge of modern technologies, increasing the period of adaptation of graduates in primary officer positions and reducing the prestige of higher education [13].

Conclusions

Thus, the analysis revealed that there are currently a number of problems in the development of educational standards for this category of higher education; allowed to identify shortcomings in the educational process of training cybersecurity professionals.

The direction of further research is the development of partial methods for assessing the level of personnel selection for cyber units of the Armed Forces of Ukraine, its adaptation and motivation.

References

1. The Law of Ukraine (2014), "*Pro vyshchu osvitu (redaktsiya vid 30.11.2016*" [*On higher education edition of 30.11.2016*], available at: https://cutt.ly/PkDTSHD (accessed 12 February 2021).

2. Hordiychuk, S.V. (2016), "Stvorennya standartiv novoho pokolinnya u zabezpechenni yakosti medychnoyi osvity" [Creation of standards of the new generation in ensuring the quality of medical education], *Continuing professional education: theory and practice. Pedagogical Sciences*, Issue 1-2, pp. 121–126.

3. Zhuravs′ka, N. (2016), "Reforma standartiv vyshchoyi osvity" [Reform of higher education standards], *Youth and Market Journal*, No. 8(79), pp. 27–31.

4. Kysel′ov, N. and Yankova, M. (2013), "Zmist ta zavdannya standartyzatsiyi vyshchoyi osvity" [Content and tasks of standardization of higher education], *Science and Education Journal*, No. 6, pp. 90–95.

5. Strilets′, N.V. (2017), "Standarty profesiynoyi pidhotovky v systemi vyshchoyi osvity: napryamy vdoskonalennya" [Standards of professional training in the system of higher education: directions of improvement], *Native School*, No. 1-2, pp. 17–22.

6. Terepishchiy, D. (2014), "*Standartyzatsiya vyshchoyi osvity*" [*Standardization of higher education*], Kyiv, 197 p.

7. Cabinet of Ministers of Ukraine (2015), "*Pro zatverdzhennya pereliku haluzey znan' ta spetsial'nostey, za yakymy zdiysnyuyet'sya pidhotovka vyshchykh navchal'nykh zakladiv No. 266 vid 29.04.2015 (iz zminamy, vnesenymy zhidno z Postanovoyu Kabinetu Ministriv Ukrayiny No. 674 vid 27.09.2016)*" [*The Resolution On approval of the list of branches of knowledge and specialties for which training of higher education is carried out No. 266 dated 29.04.2015 (as amended in accordance with the Resolution of the Cabinet of Ministers of Ukraine No. 674 dated 27.09.2016)*], available at: https://cutt.ly/dkDY60U (accessed 12 February 2021).

8. Goshovskaya, V., Pashko, L. and Fugel, L. (2013), "*Kadrovyy menedzhment yak skladova upravlinnya lyuds′kymy resursamy v systemi derzhavnoho upravlinnya*" [*Personnel management as a component of human resources management in the system of public administration*], National Academy of Public Administration, 96 p.

9. Diorditsa, N. (2017), "Kvalifikatsiyni vymohy do kompetentnosti fakhivtsiv z kiberbezpeky" [Qualification requirements for

the competence of cybersecurity professionals], *Information Law*, No. 2, pp. 215–219.

10. Diorditsa, N. (2017), "Napryamky pidhotovky ta perepidhotovky fakhivtsiv z kiberbezpeky" [Areas of training and retraining of cybersecurity professionals], *Information Law*, No. 3, pp. 199–202.

11. Diorditsa, N. (2017), "Osvitni standarty dlya pidhotovky fakhivtsiv z kiberbezpeky" [Standards for training cybersecurity professionals], *National Legal Journal: Theory and Practice*, No. (23), pp. 50-53.

12. Dubov, K. (2013), "Stratehichni aspekty kiberbezpeky v Ukrayini" [Strategic aspects of cybersecurity in Ukraine], *Strategic Priorities Journal*, No. 4, pp. 119-127.

13. Karp, L. (2014), "*Dosvid USA u pidhotovtsi maystriv informatsiynykh tekhnolohiy u dystantsiyniy osviti ta mozhlyvist' yiyi vprovadzhennya v Ukrayini, Porivnyal'no-pedahohichni doslidzhennya*" [*US experience in training masters of information technology in distance education and the possibility of its implementation in Ukraine, Comparative and pedagogical studies*], Kyiv, pp. 29-35.

Vitalii Tiurin
Candidate of Military Sciences, Associated Professor
Assistant of the Minister of Defence of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0003-0476-7471

Maksym Kasianenko
Candidate of Military Sciences
Deputy Director of the Department of Military Education
and Science of the Ministry of Defence of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0002-3749-4441

Anatolii Salii
Candidate of Military Sciences, Associated Professor
Head of the Aviation and Air Defence Institute of the National
Defence University named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-3491-9301

Pavlo Openko
Candidate of Technical Sciences
Head of Research Department of the Aviation and Air Defence
Institute of the National Defence University
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0001-7777-5101

Oleksii Martyniuk
Candidate of Technical Sciences
Deputy Head of Aviation Department of the Aviation
and Air Defence Institute of the National Defence University
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0003-2578-0018

PROSPECTIVE MODEL OF THE UKRAINIAN EDUCATION AND TRAINING SYSTEM OF AIR FORCE SPECIALISTS

The paper presents the views of the authors on the formation of a perspective model of higher military education in Ukraine based on

the example of the Air Force specialists training. The proposed model meets the modern and projective needs of the Armed Forces of Ukraine and international quality standards of servicemen training. The purpose of the model is to make the Ukrainian Air Force interoperable with the NATO forces. Here given the peculiarities of the higher education system of Ukraine for the development of a perspective system of education and training of Air Force personnel, it is proposed to use a comprehensive system of education and training of NATO and national educational institutions of NATO member states, containing three functional components: academic education, training and improvement of professional competence. The conducted research made it possible to determine the advantages and disadvantages of the proposed system of education and training, to identify tasks that need to be solved for the successful implementation of the proposed model.

Keywords: *higher military education, quality of education and training, system of military education and training of servicemen of the Ukrainian Air Force.*

Introduction

Problem statement. After publication in 2016 a new strategy of NATO Joint Air Forces "Joint Air Power Following the 2016 Warsaw Summit – Urgent Priorities", one of its key theses is integration of Air Force with other services, to acquire the capabilities to conduct Joint Forces operations, which will take place in several operational environments: land, sea, air, space and cyberspace, there have been significant changes in the education and training system, especially for Air Force [1].

The top leadership of our country has declared the acquisition by the Armed Forces of Ukraine of full interoperability with the NATO armed forces, which means the need to reform the military education and training of servicemen, including the National Defence University of Ukraine named after Ivan Cherniakhovskyi [2].

The analysis of recent researches and publications. The professional publications previously covered topics about possible directions and options for reforming the system of military education and training of servicemen [3–9]. Thus, in [3] there are the

characteristics of the formation of a new paradigm of military education, which meets the needs of the Armed Forces of Ukraine and international quality standards for military training, determines the implementation in the context of military reform: providing its legal framework; identification and elimination of a set of factors that cause problems of improving military education; definition of the purposes, principles and tasks of formation of new system of military education; outlining the structure of training of military specialists, the system of officer training, its scientific and high-tech support; building a quality assurance system for military education.

In [4] military education is presented as an important part of ensuring national interests and national security of the leading world countries, justified its goals, laws, principles defined infrastructure, structure and content of military education, organizational and methodological foundations and major dominance of military experts, general trends in the development of national military educational systems.

The authors of [5] present modern approaches, forms and methods of world's leading countries the security and defense policy, protection of their national interests, armed struggle, showing the role and importance of the Armed Forces of Ukraine, the military education system as important intellectual components of security and defense of the state, substantiating the main directions and ways of further development of the military education system.

In [6–8] higher education, including military education, is considered as a historically formed social institution responsible for the succession, accumulation and reproduction of scientific knowledge, the results of which determine that the preservation of educational, scientific potential and strengthening of basic scientific and pedagogical Schools have a special role, certain tasks that must be solved by scientists of military universities, to create innovative technologies that organically combine in-depth research with the educational process and ensure the development of human capacity in the security and defense sector of Ukraine.

The authors of [9] formulate the purpose of the project and

the basic components, identified the main objectives and stages of implementation of the project of change management for the development of the military education system on the basis of program and project management.

The authors of these articles have made a significant conceptual contribution and laid the theoretical foundations for the future system of military education and training of servicemen. However, as mentioned, the proposed directions and options for reform are more conceptual in nature and can only be partially implemented at present.

That is why the issue of reforming the system of military education and training of servicemen in order for the Air Force of Ukraine to become fully interoperable with the armed forces of NATO member states is relevant.

Purpose of the report is to form a perspective model of the higher military education system of Ukraine in the course of reforming the system of military education and training of servicemen of the Armed Forces of Ukraine.

Main part

Careful study and deep analysis of educational programs of education and training of NATO Air Force education, namely the Rome Defense College [10], the Baltic Defense College [11], the NATO School in Oberammergau [12], Royal military College of Canada [13], the Bundeswehr Academy of Management [14], the Academy of Martial Arts of the Republic of Poland [15], the Joint Staff College of US National Defense University [16] showed that training in NATO schools is somewhat different from training in national schools members of the Alliance.

Thus, training in NATO schools focuses exclusively on professional training, i.e. L-courses. Such training is aimed at the acquisition by officers of exclusively military-professional competencies without being tied to a specific position, ie training is bounded to military ranks. After the finishing of L-2 Air Force officer gets competencies that allow them to work as officers of military

management authority at the Component commands, after the finishing of L-3 – take leadership positions by military control at the Component commands or officers of a military administration body at the level of the Joint Headquarters, after passing the course of L-4 – to take the leader positions of the military administration body at the level of the Joint Headquarters or officers of the military administration at levels of the Supreme Headquarters of Allied Forces (SHAPE).

At the same time, training in Allied educational institutions covers both education and training. In some countries, officers are expected to obtain a master's degree in the military field (USA, Great Britain), in others – a master's degree in the civilian field (Germany, France). Professional training is divided into two subsystems: training and improvement of professional competence. Training has the same structure as in NATO schools, except that in some countries, such as Canada, training is carried out without reference to the Service, in others – with reference (USA, Germany).

Careful study and in-depth analysis of these options has shown that Air Force military training institutions in the United Kingdom, France, and Germany are under the command of training commands, and in the United States Air Force they are integrated into the Air Force University, which is equal to such command. These educational institutions provide professional education to junior and senior officers (except for officers with the rank of colonel), which can be used in command, staff and their equal positions in units and in the headquarters of the Air Force, as well as in the departments of military ministries and departments.

The Joint Military Training Institutions of the Armed Forces are designed to train officers (generals) who will hold senior and responsible positions in the Ministries of Defense, other military institutions, headquarters, and senior command positions.

In the system of officers' higher professional education, it can be distinguishing the training of tactical, operational and strategic levels, each of which in different countries has its own specific features. Tactical level training is for junior officers who have the military rank of captain. This most numerous category of

officers is enrolled in schools, colleges and refresher courses. Graduates hold command and staff positions in the air squadron, serve in the headquarters of units and their respective military organizations. The U.S. Air Force has, for example, a first-degree training school for officers, which graduates about 2,400 people a year, an aviation college in the United Kingdom, a staff school in France, and advanced training courses in Germany.

The operational level training is taking by senior officers in the ranks of lieutenant colonels. It differs in more unified specializations in comparison with the training of the first degree, as its officer training is closely connected with the direct planning and conduct of operations, the organization of interaction with other types of troops, as well as comprehensive support. Therefore, in some countries (the United States and the United Kingdom) there are several operational-level training institutions that belong to the Air Force or are common to all Services. Such educational institutions are: in USA – Air Force College and Command and Staff College; in United Kingdom – Defence Academy of UK (common to all of the armed forces); in France – Higher School of the Air Force; in Germany – Bundeswehr Academy of Management, where training is conducted in joint groups on a service basis. An important place in the educational process of these educational institutions is given to practical training together with students of educational institutions of the Land Forces and Navy. The trainings work out the planning and organization of aviation interaction with the ground forces and naval forces, and study the procedure for the use of military equipment and armaments.

Third degree training applies to senior officers and generals under the age of 50. It is organized: in the United States at the National Military College, Staff College and Industrial College; in the United Kingdom at the Royal College of Defense; in France – the Institute of Higher Studies of National Defense, the Center for Higher Military Studies; in Germany – Bundeswehr Academy of Management. The programs of joint military educational institutions provide the study of: economics and politics of major countries; military strategy; structure and armament of the Air Force and their tasks in operations; ways of

conducting independent aviation combat and in cooperation with Army and Navy; management in wartime of aviation formations; logistical support of troops and other issues. The curriculum in military educational institutions is designed in such manner that students study only the disciplines, the mastering of which will help them to perform their duties in a qualified manner. In addition, in all countries there are a number of retraining and advanced training centers, for example, in Germany: Army has 16 centers, Air Force – 9, Navy – 4, which provides direct training of officers to perform their duties (professional and special competencies).

On the example of the Baltic region countries, consider the structure of the national system of professional military training. Course L-2 is represented by the Air Force Command and Staff Course. The training of officers of the air component headquarters is carried out at the Military Academy of Lithuania for 17 weeks, which includes 600 hours with tutor and 250 hours of self-preparation. Course L-3 is represented by the Joint Command and Staff Course of the General Staff, held at the Baltic Defense College, with a volume of 60 ECTS. At the L-2 course, officers in military ranks are trained as captains for the headquarters of the tactical component, and in the L-3 course, officers in the military rank of lieutenant colonel are trained for appointment to joint headquarters.

In addition, students can obtain a master's degree in “Military Leadership and Security”. According to the Rules of Admission, the student decides to take a master's degree immediately after entering the L-3 course. The master's degree is 90 ECTS and lasts for 3 semesters, of which 2 semesters (60 ECTS) are training in the L-3 course at the Baltic Defense College, and the third semester (30 ECTS in addition), with the writing of the master's thesis, takes place at the Latvian National Defense Academy.

It should be noted that NATO's training and education system includes individual and collective training (Fig. 1). The system is managed by a hierarchy of guidance documents [17–20]. These guidelines are the basis for the organization and conduct of educational activities in both NATO’s Centers of Excellence and NATO Partners.

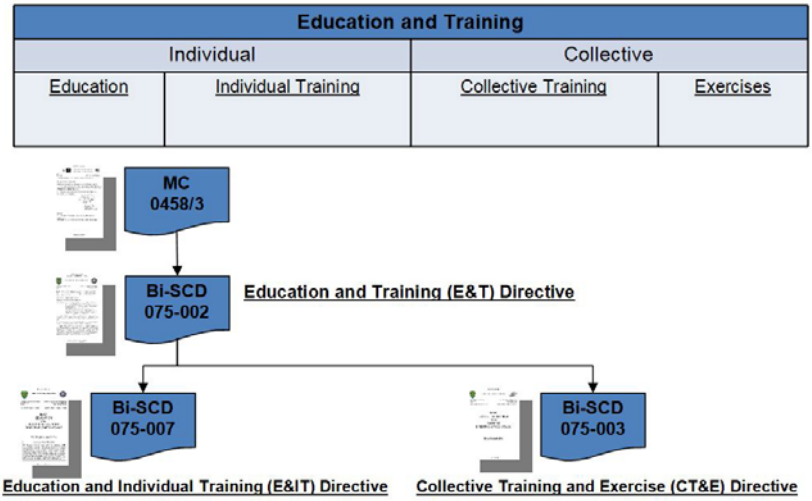

Fig. 1. Block diagram of NATO's education and training systems

At the same time, all educational institutions that train specialists for the Alliance's armed forces must be accredited, which sets certain requirements for compliance with the salary of certain criteria, the algorithm of which is determined by the Directive: Education and Individual Training. In addition, educational and training courses are defined in NATO's guiding instruments are subject to certification according to three categories: "Listed", "Selected" and "Approved" [17].

It should be noted that "Approved" courses are conducted only by NATO-accredited educational institutions, meet NATO needs and meet the requirements of the Education and Individual Training Directive, and courses that are included in the category "Listed" are mainly familiarize with national opportunities and have a wide range of learning objectives.

At the same time, the leadership of Ukraine has made decisions and taken measures to implement the national educational environment to the European one [21]. This process also involves an accreditation process, but unlike NATO's approaches, it is not the educational institution but the educational programs implemented by

the higher education institution. The Ministry of Education and Science of Ukraine approved a number of Standards of Higher Education of the branch of knowledge “Military Sciences, National Security, State Border Security” and the Regulations on Accreditation of Educational Programs [22]. Examination and analysis of these documents have shown that they set a number of requirements that are not identical to those set out in NATO documents.

Thus, when developing a perspective model of the system of higher military education in Ukraine, the above-mentioned superpowers were identified (Fig. 2).

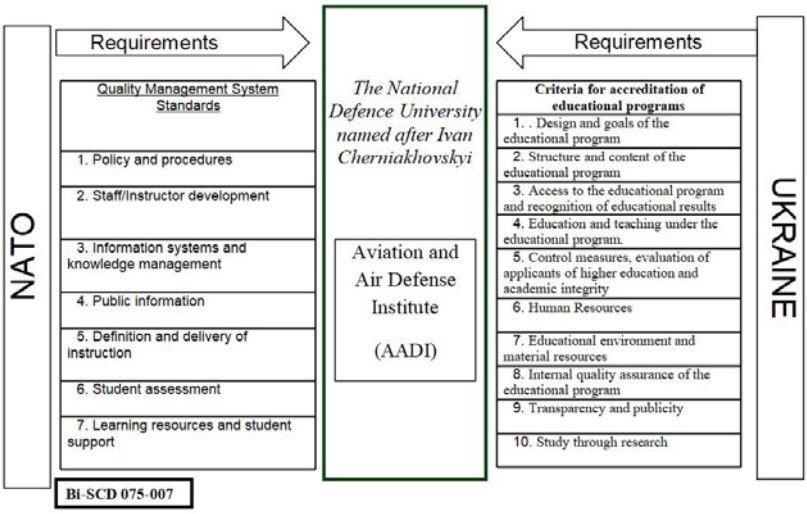

Fig. 2. Requirements for a perspective model of higher military education in Ukraine

In order to be one of the leading higher military educational institutions of Ukraine, as a national institution of higher education, it is necessary to comply with the requirements of national governing documents, and in order to cooperate with NATO institutions and be compatible with them to comply with NATO governing documents.

Based on the above, to develop a perspective system of education and training of Air Force personnel, it is proposed to take as a basis the education and training system in the complex of both NATO and national educational institutions of NATO member states, which is shown in Fig. 3, and consists of three functional components: academic education, training and improvement of professional competence.

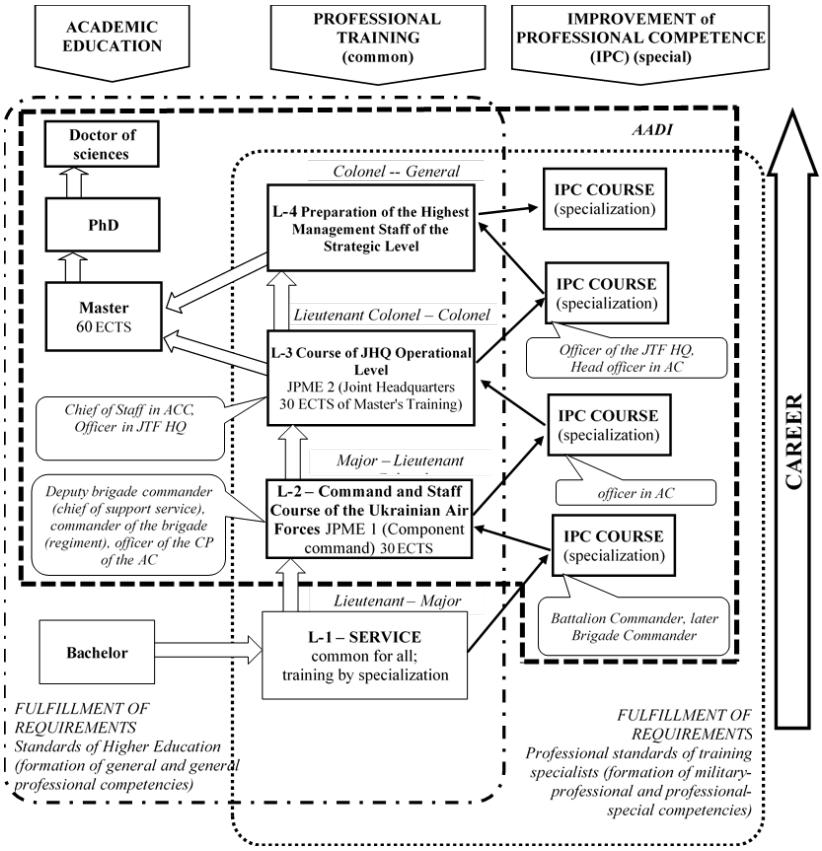

Fig. 3. Perspective model of the system of higher military education of Ukraine (on the example of training of Air Force specialists)

To develop the content of the training on the L-2 course, the composition and functional tasks of the Air Command (AC) and the

Joint Task Forces (JTF) with similar NATO structures were analyzed and compared. Accordingly, it is proposed the course L-2 to train officers of military control authority at the command of the aviation component (AC), and the L-3 – a head of military administration level of air component command or military control authority officer of JTF HQ. At the same time, it is considered expedient to conduct training on the course L-2 by services, and on L-3 and L-4 – joined. However, due to the transitional period of reforming the Air Force, on the course L-2, at present, it is necessary to leave the training of officers at the level of brigade commander, and with the subsequent gradual abandonment of it.

Before the officer arrives at the university to study for the L-2 course, he/she must take courses to improve the professional competence of the battalion commander (brigade chief of staff), and then – the brigade commander, which is proposed to organize on the basis of departments of Aviation and Air Defense Institute of The National Defence University of Ukraine named after Ivan Cherniakhovskyi. Upon completion of the L-2 course, officers will take professional development courses where they will acquire the professional competencies they need to be appointed to certain positions. It is proposed that the departments of all institutes will participate in courses L-3 and L-4.

In addition, it is proposed to indicate in the certificates of completion of the Command and Staff Courses of the Air Force L-2, as well as professional development courses and indicate the amount of study hours in ECTS in order to further take them into account in master's training as educational components that will promote higher education, military-professional and professional-special competencies and achievement of program training results.

Conclusions

The conducted research allowed to determine the advantages and disadvantages of the proposed system of education and training.

Thus, the advantages of this system include:

– adaptation to the education and training system of both

NATO and the European Union member states;

– the system fully meets the requirements of the governing documents to ensure the career growth of servicemen;

– allows to recognize documents of NATO educational institutions without additional nostrification;

– the dual system of education, student-centeredness, academic mobility is provided;

– the possibility of certification both according to NATO standards and accreditation according to the requirements of the Ministry of Education and Science of Ukraine is created;

– system flexibility.

The disadvantages of the transition period include:

– inconsistency of the existing state normative documents regulating the system of military education and training with the normative documents of the education system of the countries of Europe and NATO;

– the difficulty of preparing teaching materials due to the lack of new doctrinal documents;

– excessive workload on faculty members during the transition period;

– long term of implementation of the given system (3-5 years);

– lack of nostrified diplomas to ensure academic mobility of research and teaching and research staff.

As tasks for the construction of this system and the elimination of these shortcomings in the transition period were identified:

– urgent amendments to the normative documents regulating the system of military education and training;

– timely implementation of doctrinal documents for the purpose of high-quality preparation of educational and methodical materials;

– high-quality planning of uniform load on faculty members during the transition period;

– obligatory mastering of foreign language by faculty members (at the level not lower than STANAG 6001 Level-3);

– transfer of specific higher military educational institutions for training only bachelors;

– conducting the procedure of nostrification of diplomas to ensure the academic mobility of scientific, pedagogical and research staff according to the standards of the European Union (NATO).

The implementation of this system of education and training will create conditions for the acquisition of professional competence and graduates and take an active part in joint exercises and collective training activities, both the Armed Forces of Ukraine and NATO member countries.

Prospects for further research. The direction of further research is to create a system of internal system for assessing the quality of education and training, further interaction with stakeholders both during the preparation of regulations and during the educational process.

References

1. Joint Air Power Competence Centre (2016), *Joint Air Power Following the 2016 Warsaw Summit. Urgent Priorities*, available at: https://cutt.ly/pksbnug (accessed 28 January 2021).

2. Ministry of Defense of Ukraine (2020), "*Viziia Heneralnoho shtabu ZS Ukrainy shchodo rozvytku Zbroinykh Syl Ukrainy na naiblyzhchi 10 rokiv*" [*Vision of the General Staff of the Armed Forces of Ukraine on the development of the Armed Forces of Ukraine for the next 10 years*], available at: https://cutt.ly/NkevQ2l (accessed 28 January 2021).

3. Shchypanskyi, P.V., Tymoshenko, R.I. and Salkutsan, S.M. (2017), "Formuvannia novoi paradyhmy viiskovoi osvity" [Formation of a new paradigm of military education], *Science and Defense*, No. 2, pp. 37-42.

4. Prykhodko, Yu.I. (2017), "Pidhotovka viiskovykh fakhivtsiv u pryvidnykh krainakh svitu: osnovopolozhni zasady ta tendentsii" [Preparation of military specialists in the leading countries of the world: basic principles and tendencies], *Pedagogical Sciences*: *Theory, history, innovative technologies*, No. 3 (67), pp. 285-299.

5. Telelim, V.M., Tymoshenko, R.I. and Prykhodko, Yu.I. (2013), "Viiskova osvita v systemi bezpeky ta oborony derzhavy" [Military education in the system of security and defense of the state], *Science and Defense*, No. 4, pp. 21-28.

6. Poltorak, S.T. (2018), “Transformatsiia systemy viiskovoi osvity Ukrainy na shliakhu do dosiahnennia standartiv NATO” [Transformation of the military education system of Ukraine on the way to achieving NATO standards], *Science and Defense*, No. 2. pp. 3-10.

7. Punda, Yu.V. (2018), “Osvita – holovna investytsiia v rozvytok liudskoho kapitalu sektoru bezpeky i oborony Ukrainy” [Education – the main investment in the development of human capital in the security and defense sector of Ukraine], *Science and Defense*, No. 1. pp. 34-40.

8. Syrotenko, A.M., Prykhodko, Yu.I. and Bogunov, S.O. (2018), “Innovatsii v systemi pidhotovky viiskovykh fakhivtsiv z vyshchoiu osvitoiu: poniattia, sutnist, spriamovanist” [Innovations in the system of training military specialists with higher education: concept, essence, direction], *Science and Defense*, No. 3. pp. 38-46.

9. Artamoschenko, V.S. and Favorskaya, O.Yu. (2019), “Upravlinnia zminamy shchodo rozvytku systemy viiskovoi osvity na zasadakh prohramno-proektnoho menedzhmentu” [Management of changes in the development of the system of military education on the basis of program and project management], *Science and Defense*, No. 3. pp. 40-44.

10. *NATO Defense Colledge*, available at: http://www.ndc.nato.int (accessed 28 January 2021).

11. *Baltic Defense College*, available at: http://www.baltdefcol.org (accessed 28 January 2021).

12. *NATO School Oberammergau*, available at: https://www.natoschool.nato.int (accessed 28 January 2021).

13. *Royal Military College of Canada*, available at: http://www.rmc.ca/index-eng.asp (accessed 28 January 2021).

14. *Führungsakademie der Bundeswehr*, available at: http://www.fueakbw.de (accessed 28 January 2021).

15. *Akademia Sztuki Wojennej*, available at: https://www.akademia.mil.pl (accessed 28 January 2021).

16. *Joint Forces Staff College*, available at: http://www.au.af.mil/au/awc (accessed 28 January 2021).

17. NATO (2014), *MC 0458/3 (Final) NATO Education, Training, Exercise and Evaluation (ETEE) Policy, dated 03 September 2014*, available at: https://cutt.ly/xkopJ0V (accessed 28 January 2021).

18. NATO (2016), *BI-SC Education and Training Directive (E&TD) 075-002, dated 09 September 2016*, available at: https://cutt.ly/1kec24O (accessed 28 January 2021).

19. NATO (2015), *BI-Strategic Command Education and Individual Training Directive (E & ITD) 075-007, dated 10 September 2015*, available at: https://cutt.ly/9kecHVa (accessed 28 January 2021).

20. NATO (2013), *BI-SC Collective Training and Exercise Directive (CT&ED) 075 -003, dated 02 October 2013*, available at: https://cutt.ly/JkecWfb (accessed 28 January 2021).

21. National Agency for Quality Assurance in Higher Education (2019), "*Stratehiia Natsionalnoho ahentstva iz zabezpechennia yakosti vyshchoi osvity do 2022 roku*" [*Strategy of the National Agency for Quality Assurance in Higher Education until 2022*], available at: https://cutt.ly/aj5Okrt (accessed 28 January 2021).

22. The Ministry of Education and Science of Ukraine (2019), "*Polozhennia pro akredytatsiiu osvitnikh prohram, za yakymy zdiisniuietsia pidhotovka zdobuvachiv vyshchoi osvity*: nakaz Ministerstva osvity i nauky Ukrainy vid 11 lypnia 2019 roku #977" [*Regulations on accreditation of educational programs, which are used to prepare applicants for higher education*: order of the Ministry of Education and Science of Ukraine of July 11, 2019 No. 977], available at: https://zakon.rada.gov.ua/laws/show/z0880-19 (accessed 28 January 2021).

Stepan Yakymiak
Candidate of Military Sciences, Associate Professor
Chief of the Naval Forces Department of the National Defence University of Ukraine named after Ivan Cherniakhovskyi
Kyiv, Ukraine
https://orcid.org/0000-0002-1530-271X

HYBRID WARFARE IN THE BLACK SEA: LESSONS LEARNED AND TRAINING IMPROVEMENT

The analysis of the hybrid warfare in the Black Sea region certifies that Russia is expanding the scope of hybrid actions at sea and uses interagency task forces. In order to counteract such operations it is necessary to plan and conduct specific maritime operations with the involvement of forces from various ministries and agencies. It requires improved interagency training and expansion of competencies for conducting information, diplomatic, political, economic, cyber, military measures to counteract hybrid influence.

Keywords: *hybrid warfare at sea, lessons learned, maritime operations, interagency training, competencies.*

Introduction

General Problem Statement. Continuing the armed aggression against Ukraine, Russia is actively using hybrid actions at sea, in particular, constantly carries out activities and actions in various spheres and areas, including political, diplomatic, economic, informational, military and others, united by a single plan to achieve a specific political (military-political) goal without full employment military force.

Under such conditions, an important problem that requires constant response and solution is a systematic analysis of combat experience, identifying lessons and ways to counter the enemy. An important component of the response is to improve the training of specialists taking into account the peculiarities of hybrid action.

Analysis of the Recent Research and Publications. Analysis of domestic and foreign sources shows that the study of the experience of the hybrid warfare and the identification of countermeasures has received considerable attention [1–10]. The recommendations for joint counteraction against Russia in the Black Sea region with the involvement of NATO member states and Black Sea partner states – Ukraine, Georgia are suggested in [7–9]. Ways to counter hybrid influence at sea and situational training are devoted to the work of specialists from the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE, Finland) [10]. However, these works do not address the issue of the main directions and measures to improve the educational programs (of professional military education) for increase the effectiveness of interagency (joint) task forces employment in conditions of hybrid warfare at sea.

Aim of the Research. The purpose of this study is: based on the analysis of the experience of hybrid operations at sea and the proposed ways of counteracting – to identify appropriate areas and measures to improve training, which should promote more effective use of interagency (joint) task forces to counter Russia in Black Sea region.

Main part

Russia's hybrid actions against Ukraine in the Crimea, other coastal regions of Ukraine and at sea have been conducted since 1991 and have become clearest in 2014-2019 in the context of Russia's armed aggression.

In the period from 1991 to 2014, the set of hybrid actions of the Russian Federation in the Crimea, other coastal regions of Ukraine and at sea was as follows [6]:

a large-scale information campaign to discredit Ukraine in the eyes of the leadership of European countries, including EU and NATO member states, discredit the leadership of the Ukrainian state, reduce the moral and psychological condition of servicemen, other military formations and law enforcement officers;

constant economic pressure and manipulation of Ukraine,

starting with the redistribution of the Ukrainian side's interest in the division of the Black Sea Fleet through the so-called "payment of debts for Russian gas supplies" (instead of 50% to 50%, the Russian side offered to transfer only 18% of weapons and other material means, property, arguing that they are in arrears for Russian gas supplies), and at the same time neglecting the issue of Russia's payment for the lease of infrastructure facilities in Ukraine to base the Black Sea Fleet, although this issue was enshrined in the Black Sea Fleet distribution agreements;

constant political pressure, first of all on the political and military-political leadership of Ukraine;

neglect of legal norms, in particular the provisions of international law, especially international maritime and humanitarian law, national legislation of Ukraine during the establishment and operation of the Russian Black Sea Fleet, and, in particular, the use of illegitimate methods of force, including units of so-called "green men"; that is, Russian servicemen who did not belong to the Black Sea Fleet personnel and acted with weapons in their hands (creating a threat of using these weapons) on the territory of the sovereign state of Ukraine; blocking the bases of the Navy of the Armed Forces of Ukraine by naval and various tactical groups of the Black Sea Fleet;

non-fulfillment of diplomatic measures stipulated by international law and bilateral agreements during the beginning of the armed aggression and in the future, first of all in response to the notes of the Ukrainian side, etc.

Thus, the set of measures taken by Russia in various spheres of activity, including the military, created conditions under which the Ukrainian side was unable to respond effectively to threats and actions from the Russian Federation. Russia has partially achieved its strategic goal of destabilizing the situation and creating conditions for Ukraine's return to full political control.

After the beginning of the armed aggression against Ukraine in February 2014, the Russian Federation is constantly expanding the scope and scope of hybrid influence on security, including in the

Azov-Black Sea region. According to the analysis of the views of the Russian military-political leadership, in particular the speeches of the Chief of General Staff of the Russian Armed Forces Gerasimov, the Russian Federation implements the so-called "strategy of limited actions", which is known in the terminology used by NATO and Ukrainian experts "Hybrid actions" [9].

Thus, during 2018, the enemy, using hybrid technology to influence Ukraine, took action to disrupt Ukraine's maritime economic activity and strengthen its own military presence at sea [11].

In September 2018, having let the first detachment of two support vessels of the Ukrainian Navy into the Sea of Azov, the enemy captured three warships of the Ukrainian Armed Forces together with their crews on November 25, 2018, on the approaches to the Kerch Strait [4].

In 2019, the enemy spread hybrid action to the Black Sea. Thus, in August 2019, it simultaneously closed for navigation more than 25% of the area of this sea and significantly complicated the conditions for international navigation and combat activities of the Navy of the Armed Forces of Ukraine [9].

Analysis of Russia's hybrid actions at sea led to the following conclusion: the volume of hybrid actions in the course of measures and actions to ensure national security at sea is constantly growing with increasing conflict, and if the strategic goal of hybrid action is not achieved, the aggressor may move to full-scale hostilities.

The above analysis of the experience of action at sea allowed us to determine the following general conclusions [9]:

the enemy expands the methods and forms of hybrid influence on Ukraine with the use of military force, in particular with the hybrid use of created and deployed groups of forces (troops);

during hybrid operations, the enemy uses specially created interagency (joint) task forces;

by conducting actions at sea, the enemy negatively affects the economic activity of Ukraine, international shipping within the

area of responsibility of Ukraine at sea and, accordingly, tries to worsen the social-political situation in coastal regions, in all territory of state and to worsen Ukraine's image as a reliable guarantor for compliance of international low at national waters.

All this necessitates the urgent development of the basics of the use of interagency (joint) task forces at sea in the conditions of hybrid actions of the enemy.

To perform the tasks of conducting hybrid actions, it is necessary to have the appropriate capabilities. It should be noted that the Maritime Doctrine of Ukraine for the period up to 2035 [12], which was developed by the Department of Naval Forces of the National Defense University of Ukraine, provided for the following measures for the application and development of the Naval Forces:

maintaining the naval potential of Ukraine at a level sufficient to ensure the deterrence and repulsion of external aggression from the sea, guaranteed protection of national interests in certain areas of the oceans;

increase of forces and means of defense of the state from the sea by mobilization, use of non-military vessels and special equipment, berths of sea and river ports;

creation of the necessary military potential in the Sea of Azov in peacetime and special periods, including ships (boats) with missile weapons, multi-purpose small surface platforms, including unmanned;

creation of military-level operational management bodies in two separate operational units - in the Azov and Black Seas, which are responsible for the preparation and management of actions of interservices task forces of the Navy and joint (interagency) task forces.

Directions for the development of naval capabilities were also set out in the Strategy of the Naval Forces of the Armed Forces of Ukraine 2035, presented in November 2018 by the Commander of the Naval Forces of the Armed Forces of Ukraine [13]. The implementation of the above-mentioned conceptual documents has made it possible to take a more systematic approach to defining

strategies and plans for counteraction to hybrid operations at sea.

In order to ensure effective counteraction to the hybrid influence of the enemy at sea, the following proposals were developed and submitted [9].

1. In conditions of constant violations of international law by the enemy, it is necessary to plan measures to monitor the situation, anticipate the enemy and respond to his actions.

2. In order to ensure a forceful response, it is necessary to provide for advance planning and implementation of special measures and actions for the return of production facilities.

3. Each detected action (operation) of the enemy at sea, which has a hybrid effect, must be opposed by both protective and proactive advanced maritime operation.

4. Analysis of the situation in the Black and Azov Seas and adjacent coastal areas, allows to determine the main purpose of anti-hybrid operations at sea - protection of national interests of Ukraine at sea, repulse, stabilization and deterrence of enemy aggression from the sea together with other components of security and defense forces

5. In this strategic anti-hybrid operation, the use of diplomatic, political, information-psychological, economic-sanctions, military-demonstration and other measures and actions of Ukraine together with its strategic foreign partners - NATO, EU, USA will play an important role. Among these measures, ongoing cooperation activities, including international maritime exercises in the Black and Azov Seas, should play an important role. The number of joint exercises with partners at sea should increase, and their areas should be expanded towards the central and eastern part of the Black Sea. It would be appropriate to launch an international operation under the auspices of NATO to control and protect shipping in the Black Sea on the basis of a UN decision.

During maritime anti-hybrid operations it will be appropriate to use the provisions on maritime operations set out in the AJP-3.1 Allied Joint Doctrine for Maritime Operations [14].

One of the important measures of joint (interagency)

counteractions to hybrid threats is the organization, establishment and maintenance of constant interaction on monitoring of hybrid actions (at the international, state, military, scientific and expert levels), in particular [9]:

creation of permanent working groups and algorithms of their work (order, time, response, interaction);

coordination of the procedure for information exchange between coordination centers and control centers;

creation (expansion) of an expert and scientific community;

creation in Ukraine of a center for the study of hybrid actions (for expert assessments, research, consultations, systematic presentations for management, development of strategies, plans).

To improve the joint (interagency) training of staff and their activities, the following proposals have been identified:

more systematic and dynamic (advanced) work on the exchange of experience and current information is needed to provide the teacher and the student;

it is necessary to organize anti-hybrid courses (quality and frequency, updates every 6 months or more);

it is advisable to form joint networks - (so far - experts from different NATO countries and Ukraine are looking for each other - there is no national and international accounting to identify areas of professional interest and development of those groups that lack experts);

provide for mutual rapprochement of groups of analytical, expert, professional research and educational structures and their staff, development, transition to measures to model situations, decisions, their consequences and the formation of the necessary capabilities (each seminar, round table, conference, forum to focus on the full cycle consideration of problems and ways to solve them by brainstorming with the provision of the final product in the form of an action plan and capacity development, provision and project management).

To check if we are going in the right direction, ask yourself the following questions:

Is there a database of experts and a permanent system of their work with deepening and detailing the results?

Are there appropriate structures and training courses in the staff training system, and how often are they updated?

Have we reached the level of joint expert work in the course of scientific activities, at which they result in obtaining a specific planning document to improve the situation (content of measures, their provision, management procedures)?

The above recommendations, in the opinion of the authors, will expand the idea of modern approaches to countering hybrid actions of the enemy at sea, in particular to move away from the classic defensive and offensive operations of troops (forces) and move to modern interagency (interspecies) operations at sea. Implementation of these recommendations will ensure the achievement of strategic goals in the protection of Ukraine's national interests at sea, repulse and deter the enemy from the Black Sea and Azov maritime areas in conditions of hybrid actions of the Russian Federation at sea (from the sea), including jointly with NATO and other partners, and will increase the level of international security in the Black Sea region.

Conclusions

From the analysis of the experience of conducting hybrid actions in the Black Sea region, it is determined that in order to counteract the Russian Federation, it is necessary to timely plan and conduct an interagency (joint) anti-hybrid maritime operation. Given the insufficient capacity of the Black Sea states, in particular Ukraine and Georgia, to counter the aggressive actions of the Russian Federation in the region, it is important to coordinate and organize joint actions with NATO.

At the same time, in order to ensure sufficient effectiveness of joint (coalition) actions in hybrid warfare at sea, it is necessary to create conditions for improving the training of specialists in planning and conducting anti-hybrid actions.

First of all, it is expedient to conduct advanced systematic

work on the exchange of experience and adaptive provision of information to researchers, teachers, students, the creation of joint research networks and centers. In Ukraine, it is necessary to create a center for study of hybrid warfare.

Secondly, anti-hybrid courses should be formed, regularly conducted and systematically updated. In the training of specialists in the security and defense sector, it is necessary to significantly expand the studying of information, diplomatic, international law, political, economic, cyber, military measures to counteract hybrid influence and to provide interagency and international cooperation.

The direction of further research is the development of methods for training specialists who can be involved in the management of interagency (joint) task forces during the planning and conducting of operations in the conditions of hybrid warfare at sea.

References

1. Rusnak, I.S., Bydniy, V.A., Segeda, S.P., Yakymiak, S.V. and etc. (2017), *The White Book of the Anti-terrorist Operation in the East of Ukraine in 2014-2016*, in Rusnak, I.S. (ed.), National Defence University of Ukraine, Kyiv, 162 p., available at: https://cutt.ly/skMqjbu (accessed 10 Octoder 2017).
2. Horbulin, V. (2017), *The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from ukrainian*, Folio, Kharkiv, 158 p. available at: https://cutt.ly/tkMqGG6 (accessed 26 January 2017).
3. Borys, V., Gerasymchuk, S., Kravchenko, V., Shelest, H. and etc. (2019), "*Uroky gibridnogo desyatilittya: scho treba znaty dlya uspishnogo rukhu vpered*" [*Lessons of the hybrid decade: what you need to know to move forward successfully*], in Shelest, H. (ed.), Government Office for Coordination of European and Euro-Atlantic Integration, Kyiv, 69 p., available at: https://cutt.ly/rkMebuT (accessed 22 February 2019).
4. Syrotenko, A., Bogdanovich, V., Semenenko, V., Yakymiak, S. and etc., (2020), "*Voyenni aspekty protidiyi "gibridniy" agresiyi: dosvid Ukrayiny: monografiya*" [*Military aspects of counteracting "hybrid" aggression: experience of Ukraine: monograph*], NDUU named after I. Chernyakhovskiy, Kyiv, 176 p.
5. Stocer, D. and Whiteside, C. (2020), Blurred Lines: Gray-Zone Conflict and Hybrid War – Two Failures of American Strategic Thinking, *Naval War College Review*, Vol. 73: No. 1, Article 4, available at: https://cutt.ly/tkMr16q (accessed 24 January 2020).

6. Yakymiak, S.V. (2014), "Visnovky ta uroky z dosvidu diyalnosty Viyskovo-Morskih Sil Zbroynih Sil Ukrainy pid chas okupatsiyi Krymu ta antiteroristichnoyi operaciyi" [Conclusions and lessons from the experience of the Naval Forces of the Armed Forces of Ukraine during the occupation of Crimea and the anti-terrorist operation], *Military History*, No. 3-4, pp. 76-86.

7. Flanagan, S. and Chindea, I. (2019), Russia, NATO, and Black Sea Security Strategy, *Regional Perspectives from a 2019 Workshop*, 18 p. https://doi.org/10.7249/CF405.

8. Perepelytsia, G. (2016), Current geopolitical trends in the Black Sea region, *UA: Ukraine Analytica*, No. 3(5), pp. 20-28.

9. Yakymiak, S.V. (2020), "Problemny pitannya protidiyi gibridnomy vplivu protivnika na mory ta shlyakhy yikh virishennya" [Problem issues of counteracting the hybrid influence of the enemy at sea and ways to solve them], *Science and Defense*, No. 2, pp. 31-36. https://doi.org/10.33099/2618-1614-2020-11-2-31-36.

10. Lohela, T. and Schatz, V. (eds) (2019), *Hybrid CoE Working Paper 5: Handbook On Maritime Hybrid Threats*], 52 p., available at: https://cutt.ly/3kMiSer (accessed 22 November 2019).

11. Decree of the President of Ukraine (2018), "*Pro rishennya Rady natsionalnoy bezpeky i oborony Ukrainy "Pro nevikladny zahody schodo zakhistu natsionalnyh interesiv na pivdny ta skhody Ukrainy, u Chornomu ta Azovskomu moriyah i Kerchenskiy prototsi No. 320/2018 vid 12.01.2018 r.*" [*About decision of the National Security and Defense Council of Ukraine "About urgent measures to protect national interests in the south and east of Ukraine, in the Black and Azov Seas and the Kerch Strait" No. 320/2018 dated 12.10.2018*], available at: https://cutt.ly/AkMoZY6 (accessed 12 October 2018).

12. The Resolution of the Cabinet Ministers of Ukraine (2018), "*Pro vnesennia zmin do Morskoi docktriny Ukrainy na period do 2035 roku No. 1108 vid 18.12.2018 r.*" [*About changes to Maritime doctrine of Ukraine for the period up to 2035 No. 1108 dated 18.12.2018*], available at: https://cutt.ly/dkMo0ZS (accessed 03 November 2020).

13. Voronchenko, I. (2019), "*Strategiya Viyskovo-Morskih Sil Zbroynih Sil Ukrainy 2035*" [*Strategy of Naval Forces of Armed Forces of Ukraine 2035*], website of Naval Forces of the Armed Forces of Ukraine, available at: https://cutt.ly/wkMp5Zc (accessed 11 January 2019).

14. NATO Standardization Office (NSO) (2016), *Allied Joint Doctrine for Maritime Operations (AJP-3.1, Edition A, Version 1)*, available at: https://cutt.ly/skMknhf (accessed 11 January 2019).

AFTERWORD

The study of the problems of the military specialists training system development for the security and defence sector has a long scientific tradition. The study of the features of specialists training in the face of hybrid threats is a continuation of this tradition. This approach in the study makes it possible to consider the scientific problem in a wide scientific circle of the military education and science representatives involved in educational process.

The monograph, which examines the aspects of military specialists training to counter Russia's hybrid threats in Ukraine, is only a small part of a nationwide study in the context of complex international relations and the new paradigm of military education.

As a result of the study of the monograph problematic, the author's team came to the conclusion that the assessment of the military security conditions, as well as the experience of the security and defence sector units participation in the Anti-Terrorist Operation (Joint Forces Operation) in eastern Ukraine revealed a number of defence forces functioning problems in the conditions of existing and potential threats, which is certainly related to the level of personnel training. In particular, this is reflected in:

lack of a clear division of responsibilities for the formation and use of defence forces, which negatively affects the ability of the state leadership to exercise effective governance in the field of defence;

lack of joint leadership of the defence forces in accordance with the principles and standards adopted by NATO member states;

redundancy and irrelevance of the legal framework in the field of defence;

imperfections of defence planning procedures, insufficient consistency with the budget process, imperfection of mechanisms of defence resources program management;

non-compliance of production capacities with the needs of the defence contract, critical physical and moral wear and tear of fixed assets;

deficient operational (combat, special) capabilities of the defence forces;

the lack of an effective unified logistics system capable of supporting the work of all components of the defence forces;

low efficiency of the defence forces medical support system;

problems of defence forces manning during the partial mobilization, the need to increase the professional level of defence personnel, the need to create a sufficient military reserve;

incomplete transition to the contractual army in compliance with the principles of personnel policy adopted in NATO.

The defence reform should meet the current needs of Ukraine's defence, strengthen the capabilities of the defence forces, increase the readiness to perform their assigned tasks and participate in joint combat operations with NATO forces.

To this aim the monograph offers the materials to find answers to a range of problematic questions, namely:

creation of a defence force management system based on a new division of powers, functions, tasks, duties and responsibilities in the field of defence, which corresponds to the principles;

policy-making, planning and management of state resources are consistent with Euro-Atlantic principles that ensure the creation of adequately trained, equipped and supported defence forces capable of effectively performing the tasks set by the strategic documents of Ukraine's national security, defending Ukraine and participating in international peacekeeping operations by developing the necessary capabilities within the identified resources;

acquisition by the defence forces necessary operational (combat, special) capabilities that provide a reliable deterrence of the armed aggression, allow to respond effectively to national security threats in the military sphere, ensure the defence of Ukraine, protection of its sovereignty and territorial integrity, are corresponding to the necessary standards and criteria’s necessary for NATO membership, ensure the ability of the defence forces to participate in the maintenance of peace and international security;

development of a single efficient logistics system for the

defence forces in accordance with NATO logistics standards and guidelines;

formation of the necessary personnel potential of the Armed Forces of Ukraine and other components of the defence forces by professionally trained servicemen with high moral and business qualities, capable of qualitatively solving complex military-professional tasks in peacetime and special period;

creation and maintenance of the Armed Forces of Ukraine strategic reserve capable of carrying out offensive (counter-offensive) operations, strengthening groups of troops (forces) in threatening areas, ensuring the rotation of troops (forces), their replenishment and replacement in case of loss of combat capability;

rational use of personnel potential, formed at the expense of personnel with combat experience gained during participation in the anti-terrorist operation, as well as professionally trained in military educational institutions of NATO and EU member states;

improving the effectiveness of the application of international logistical assistance, from the United States, NATO and European Union member states, and NATO Trust Funds, established under the provisions of the Charter on a Distinctive Partnership between Ukraine and the North Atlantic Treaty Organization in support of sovereignty, independence and territorial integrity of Ukraine;

implementation of the Alliance's standards in all spheres of military activity and introduction of the best world practices to the military management bodies functioning and the fulfilment of crisis response tasks by troops (forces).

The results of the aspects study, identified in the monograph can be useful in the applied analysis of problems related to the development of military education and science and the analysis of decision-making in response to hybrid crises.

This collection of papers represents the outcomes of the international scientific and practical conference "Current issues of military specialists training in the security and defence sector under conditions of hybrid threats" held on the November, 21, 2020 in the National Defence University of Ukraine named after Ivan Cherniakhovskyi.

The conference materials highlight many critically important aspects related to hybrid threats, the features of the cotemporary military conflicts, and the fundamentals of the integrated use of military and non-military forces and means to counter the hybrid aggression.

The conference participates discussed approaches to transformation of the specialists training in the security and defence sector of Ukraine, relevant NATO states' experiences in training, the main tasks of the reformation of the military education and science system, and the military and scientific aspects of countering the hybrid aggression in Ukraine.

SDirect24
Society, Science, Safety

ISBN 978-83-66676-10-7