NEW OPERATIONAL REQUIREMENTS OF THE INTEGRATED DEFENCE SYSTEM IN THE HIBRID WAR CONDITIONS

Ovidiu MOŞOIU*, Ion BĂLĂCEANU, Marius MOLDOVAN*****

*"Henri Coandă" Air Force Academy, Brasov, Romania (ovidiu_mosoiu@yahoo.com)
**Hyperion University, Bucharest, Romania (balaceanugion@yahoo.com)
*** General Staff, Bucharest, Romania (mmoldovan66@gmail.com)

DOI: 10.19062/1842-9238.2017.15.1.21

Abstract: *The assessment of the operational requirements characteristic of the hybrid war requires the integrated defence system to address new threats specific to the hybrid environment, in which the non-state or state adversary uses concerted and effective political, economic, military, informational or social means, as well as conventional or unconventional methods, procedures and actions, in order to achieve the planned objectives. An important aspect which differentiates the hybrid threats from past military conflicts is that in the current operational environment (hybrid type), the share of unconventional actions, especially those of asymmetric type, is clearly superior. In this article, we highlight the main aspects of the new operational requirements of the integrated defence system under the contemporary conditions imposed by the hybrid war.*

Keywords: *Operational requirements, integrated defence system, hybrid threats, hybrid warfare.*

1. INTRODUCTION

Specialists in the military science domain have analysed the phenomenon of hybrid war and have established that in the contemporary operational environment, complex weapons systems and high IT & C technology are not anymore a sufficient condition to carry out the mission and to achieve success, because the counteraction of a hybrid threat is the result of the action of people (force structures) who think creatively, who have initiative and who apply a wide range of tactics, techniques and battle procedures. Essentially, modern groupings of forces, used in a multinational system, in a complex, fluid and uncertain operational environment, have to carry out various missions in changing situations and circumstances.

When facing the hybrid opponent, the chances of success can increase significantly if all the power tools (political, military, economic, informational and legislative) are used and their vulnerabilities are identified and exploited. Moreover, the threat-type of hybrid war may be used by the belligerent force structure with low military power and this has in view balancing the ratio of forces and achieving major goals with very low losses. Typically, a belligerent who uses hybrid threats has an excellent adaptability capacity, effective combat capabilities; being highly motivated, extremely volatile and flexible.

To exploit the vulnerabilities of the opponent, the hybrid aspect of the war (specific to the contemporary operational environment) can be manifested on several planes. In *the structural plan* of the hybrid war are specified the operationalised forces (combatants, combat support, logistic support, special forces etc.), groups with expertise in psychological and informational operations, mass manipulation, espionage, influencing decisions at the economic, political, legislative level, etc.

The action plan details the following aspects: operating modalities; Individual weapons, fighting techniques and weapons systems; IT & C equipment; specific equipment to operate theatre conditions, etc.

Usually, the hybrid threat is not visible, and the perpetrators of this type of threat cannot be proven too easily to be punished under international law because they use specialized structures (sometimes different intermediaries), endowed with state-of-the-art technological means, they use new training criteria and innovative tactics, techniques and procedures specific to asymmetric warfare. An important feature of the hybrid threat is that this type of action involves a great amount of effort, allowing the unconventional opponent to extend the conflict over time to the limit of the war of wear, as well as combining it with asymmetric measures and asymmetrical operations such as sabotage or ambushes, in order to significantly diminish the combat power of the conventional type.

Essentially, the strategy of opponents who use the hybrid threats in the current operational environment is an efficient one, as it is easy to get asymmetric advantages through combinations of highly trained and highly technological capabilities.

2. NATO's APPROACHES TO OPERATIONAL REQUIREMENTS SPECIFIC TO HYBRID WARFARE

In the last decade, US military specialists have developed the concept of *hybrid war* to emphasise the need for the US military to permanently adapt to the new realities of the modern operational environment. Since 2005, initiators of the development of this concept (Frank G. Hoffman and James N. Mattis of the US Marine Corps) have published the article *„Future Armed Confrontations. The emergence of hybrid wars"* [1] in which they claim that the wars in Iraq and Afghanistan have influenced the whole process of American strategic thinking on how to respond to new threats to the American continent and US interests. In the same context, it is also underlined that the conventional threat will never disappear, and that *„the US Armed Forces must maintain their superiority in this area in order to be ready to carry a major, high-intensity war at any time"*.[2]

In 2008, Russel W. Glenn (renowned US military analyst) published the article *„Evolution and Conflict: Summary of the 2008 Israel Defense Forces"* defining the concept of a hybrid threat as *"an adversary who adaptively and simultaneously uses a combination of political, military, economic, social and informational means, within conventional, irregular, catastrophic, terrorist and disruptive / criminal methods"* [3]. After a year (2009) at the *"Hybrid Threat Seminar War Game"* conference in Santa Monica, Russel W. Glenn, supporting the concept of hybrid confrontation, shows that this concept represents a *complex amalgam of activities without any restriction*. On the other hand, the hybrid threat can be characterised by simultaneous non-military and military activities, decentralised, combined with the traditional asymmetrical ones, terrorist actions with disruptive criminal ones, under the complex operating environment, *"all with the intention of using time and space to make the right decision"* [4]. As a rule, this type of opponent may be a state actor, a non-state actor, or a combination of these.

During the same period, Frank G. Hoffman defined the hybrid threat as *"any adversary who simultaneously and adaptively uses a combination of conventional weapons, irregular tactics, terrorism, and criminal behaviour in the battlefield to achieve its political objectives."* [5] It is noticeable that Hoffman, in his definition, used only terms specific to tactical and operative level actions.

It did not include strategic-level actions or political, social or economic actions. Instead, he appreciates the very close links between asymmetric actions such as organised crime, terrorism, trafficking in human beings and drugs, destabilising actions of undermining local authorities and generating or amplifying the crisis.

In fact, organised crime structures operating on the American continent (with effort in Mexico) and opium production in the Afghanistan area are particularly damaging factors that support its theory.

Later in 2013, the US Army, in its military doctrine, detailed the two concepts (*hybrid threat and hybrid war*) and explicitly used them without creating confusion. Thus, the hybrid threat has been defined as a dynamic combination of heterogeneous, regular and / or irregular, criminal and / or terrorist forces, unified, under the unitary leadership, acting to achieve major effects in the common interest. Moreover, hybrid threats can combine the operations of regular forces (operating under norms, laws of international law and military traditions) with operations carried out by irregular forces (performing operations without precisely established objectives and without restrictions of violence). Unregulated forces include guerrilla troops, terrorists, and criminals who can combine various abilities depending on the situation (use of irregular/ regular weapons and tactics and techniques). These types of skills can generate important hybrid threats that, if used against the vulnerable elements of a conventional opponent, can be extremely effective.

Also, in US military doctrine it was specified that the US military considered the existence of the two main forms of war (irregular and traditional). The war is a duality involving both dimensions in both forms of combat (offensive or defensive). *"The basic forms of war are not in terms of `either one or the other` but in a variety of combinations, depending on the capabilities and strategy of the combatants"* [6]. For these reasons, the formulation of specific operational requirements for hybrid warfare is difficult to highlight. However, international democratic bodies must militate that, in any type of military engagement (including counter-terrorism, cross-border organized crime, etc.), at least the following operational requirements must be respected: to be legitimated, to be legal and based on regulations National and international specificities; to ensure the protection of the forces carrying out actions in compliance with the legal provisions; to adapt easily to the actual situation in order to quickly remove the effects produced; to respect the signs of the sovereignty of states when acting in the multinational environment; to act proactive and proportionate to the size and intensity of the crisis; to fulfil the missions established by the political-military leadership; to avoid creating disproportionate reactions; to ensure the protection of the population, institutions and national patrimony; to avoid and limit the collateral effects.

Under the conditions of the hybrid war, the planning of military actions (in the conditions of the globalization of the terrorist scourge and cross-border crime) has become very delicate in the sense that the limitations of the legal framework of military operations must be strictly known, especially when performing undercover actions, surveillance, information, monitoring, etc. In this respect, the functioning of the integrated national defence system must be properly assessed in order to ensure the coherence and the operational and decision-making efficiency, specific to the prevention and combating of the hybrid threats.

3. THE RUSSIAN FEDERATION'APPROACH REGARDING THE OPERATIONAL REQUIREMENTS SPECIFIC OF HYBRID WAR

In Russian conception there is a different approach regarding to the hybrid war and the hybrid threats, and this practice was applied in Russian-Ukrainian conflict. The fact that the rules of the war are already changed was confirmed by Valery Gherasimov (Chief of General Staff of Russia) in an article entitled *"The value of science in prediction",* where he presents a certain and lucid definition of the concept of hybrid war, affirming that: *"the centre of gravity of the methods applied into the conflict changed in the direction of using a large scale of political, economical, informational, humanitarian and other non-military measures ,applied in coordination with the potential protest of the population".*

Also, he supports that in modern conflicts, the asymmetric operations have a pretty important presence, which would make possible that in the future armed conflicts, the cancellation of some political, economical and military advantages of conventional enemy.

Gherasimov highlights the asymmetric actions generated by the use of forces of the special structures in order to generate and maintain, throughout the opponent's territory, a conflict situation with a permanent character. This scenario can be completed by joining special IT & C. Essentially, in modern contemporary conflict, the separate threats have diminished in intensity, and operational approaches are fundamentally different. The opponents have already been using different forms of action tactics and procedures, more important and effective, being that with a simultaneous character. In the hybrid war, *"the war no longer declares itself, but once it starts, it goes according to an unfamiliar model,"* added Gherasimov, an observation that promotes the effort of planning military operations in the area of irregular threats, which would impose a comprehensive abdication from opponents to facilitate the achievement of the objectives.

It should be noted that there is a big difference between the Russian approach, mainly applied in the Ukraine area and NATO's western approach. This difference is applied because of doctrinal conception of the Russian Army, lacking of the conventional threats, as Gherasimov even stated, in the same article: *"one of the main objectives pursued by the hybrid threats is the destabilization of the governing body and the main institutions of the opponent, Thereby creating chaos and vacuum of power."* This goal can be achieved only if the opponents will avoid using traditional methods if they do not carry out predictable actions and will seek to gain important strategical advantages through violent attacks by surprise that will immediately achieve the goals of the hybrid-specific operation.

The whole physiognomy of the hybrid conflict, supported by the military expert Gherasimov, it was applied perfectly to the Russian-Ukrainian war. At the same time, guerrilla actions have been combined with actions specific to cyber, informational, economical and political conflicts, amid a lot of psychological and media operations which aimed at vulnerable state building and causing chaos and destabilization of public authorities.

The key elements that supported the Russian approach were five, as follows: [7]

1. *Undertaking actions under the law* - creating or simulating a legality issue / moment in order to avoid any possible accountability to international security bodies (for example, the organization by Moscow and the holding of a referendum on the annexation of Crimea without international supervision as a follow-up Of the "will of the local population");

2. *The organization of demonstrations of military force* - important Russian forces and military equipment were deployed at the border with Ukraine for preparing a strong and fast intervention, if the crisis created requires entrance in the neighbouring territory, in order to solve it;

3. *Intervention with special forces* - on the territory of Ukraine, the Russian Army used insignificant force structures (the Vostok battalion) as "local security forces" to facilitate Russian intervention in the area and to protect the Russian population, atypical operation that has not attracted any political accountability to international democratic bodies;

4. *Creating a firewall to justify force intervention* - against the backdrop of the protection and support of dissatisfied Russian minorities, Russia launched military action on the territory of Ukraine, taking advantage of the local militias and the tensions maintained by the pro-Russian population;

5. *Expanding the media war through hostile and laborious propaganda* - aware of the importance of the media during the hybrid war, Russia has deployed massive mass-manipulation and disinformation campaigns, turning information into an effective weapon. At both global and regional level, they have promoted systematic disinformation, credible denial, humanitarian coverage, invoking historical arguments, etc.

The involving of Russia, using specifical procedures of the hybrid war, in different areas of the world became a method at the beginning of this millennium.

General Philip Breedlove, demonstrated in a meeting of the USA Senate on february 2016 that Russia used Syrian refugees for creating a weakness in the European continent, destabilizing the local economic goals and creates a major social anxiety. Also, in the same month Jussi Niinistö (Finnish Minister of Defence), declared, in a meeting of the defence ministers part of the NATO, that Finland has information that Russia would open another front, in the nord of the European continent, at the russo-finnish border for about 1 million migrants, for which they would facilitate the crossing of the border so they would reach west of the Europe. A declaration regarding the new front of the migration, round the Baltic Sea, was made by Ilkka Kanerva, president of the Parliamentary Commission of National Defence (ex external business minister of Finland). [8] Also, there is more and more information that support the interference of Russia into internal USA problems, on the 2016 elections, into the Russia-European Union relationship, as well as some accusations of destabilizing and intimidating the EU states, by extending the cybernetic war by the Federation of Russia.

An example, typical for our subject, is the Islamic state (of Iraq and Levant/ISIL) a non-statal actor which continues to use hybrid techniques and tactics against conventional forces of Irak army. ISIL has set goals that it wants to achieve using regular, irregular tactics and terrorism [9]. The Iraq State, in response, has adopted hybrid tactics, seeking to use international and non-state actors to counteract ISIL's intentions. Thus, the Syrian-Iraq hybrid war has become a conflict between groups of non-state and state actors, which have overlapping goals in the responsibility area of a weak state with divergent interests. [10]

To combat hybrid threats the people who are in charge must focus the efforts to win the trust of the population, choosing for long-term strategies and comprehensive approaches to counteracting hybrid threats, as well as for non-military tools, including intelligence operations.

CONCLUSIONS

Operational requirements specific to hybrid conflicts need to be adapted to the contemporary operations planning system (to combat the terrorist phenomenon, illicit acts specific to cross-border organized crime, internal corruption, etc.). Giving the existence of limitations and constraints, it is very important to know the restrictions of the war in order not to overcome the legal framework of military actions. This issue becomes even more sensitive if we look at the situation where undercover, surveillance, information, monitoring or even irregular combat actions are taking place, involving non-militarized structures, terrorist groups and criminal networks. Therefore, in the hybrid operation planning algorithm, the function of the integrated defence system should be assessed permanently to detect, eliminate or reconsider some malfunctions, to ensure policy coherence and efficiency, prevent, sanction, and combat hybrid threats.

In the hybrid operational environment, the borderline between the actions of state or non-state actors (terrorists, insurgents or criminal groups) is highlighted quite hard, because there is also the possibility of confronting opponents who can use unconventional means. This may favour the emergence of hybrid threats stimulated by unconventional, incidental or uncoordinated actors, used simultaneously and unitarily by identified opponents who can use hybrid threats to exploit operational vulnerabilities, generate military challenges, and trigger hybrid conflicts, in violation of the legal, ethical and democratic framework. Even if we are discussing about the new operational requirements of the hybrid war, the design and operation of the defence system under the conditions of hybrid threats is only a part of the integrated national security system that manages the whole set of actions and operations in different environments (diplomatic, political, democratic, economic, moral-spiritual, cultural, ecological, criminal, legal, humanitarian and military) by all public authorities, as well as by state powers, at peace and war.

Under these conditions, with the scientific implementation of an algorithm of the operationalization activities on the integrated combat system, following the model established by the NATO structures can efficiently approach the operational requirements in planning of military operations under the conditions of the hybrid war.

REFERENCES

[1] Frank G Hoffman, James N. Mattis, *Future Warfare: The Rise of Hybrid Wars*, Proceedings Magazine, vol. 132/II/1,233, US Naval Institute, nov 2005, http://milnewstbay.pbworks. com/f/ MattisFour BlockWar USNI Nov2005.pdf, accessed in 02.05.2017;

[2] V. Cruceru, „*Despre conceptul de război hibrid în gândirea militară americană*", Buletinul UNAp, septembrie 2014;

[3] Russell W. Glenn, *"Evolution and Conflict: Summary of the 2008 Israel Defense Forces"* article presented in 2009 at the *"Hybrid Threat Seminar War Game"* held in Santa Monica. This document was not available to the general public. The term "catastrophic" implies the events defined in JP 1-02, „*Department of Defense Dictionary of Military and Associated Terms*", Washington, D.C., 12 april 2001 (adjusted in 17 october 2008), p. 79 like *"any Natural or Challenged Incident Including terrorism, which causes a large number of victims, damage or destruction, or which seriously affects the population, infrastructure, the environment, the economy, the morale and / or the functioning of the government."*;

[4] P. Duţu, *Ameninţări asimetrice sau ameninţări hibride: delimitări conceptuale pentru fundamentarea securităţii şi apărării naţionale*, Editura UNAp. „Carol I", p. 46,Bucureşti 2013;

[5] F. G. Hoffman, Hybrid vs. compound war, Armed Forces Journal, 1 octombrie 2009, pe http: //www.armedforcesjournal.com/hybrid-vs-compound-war/, accesat pe 02.05.2017;

[6] JP 1, *Doctrine for the Armed Forces of the United States*, 25 martie, p. I-4, 2013;

[7] Rebecca Blum, The future of NATO in the face of hybrid conflict, Bernard El Ghoul, International Relations, Academic year 2014/2015;

[8] *"UE suspectează Agenda rusă în domeniul migrației, schimbând calea arctică"* . New York Times, 2016-04-02;

[9] J. Scott; M. Scott (2014-12-02). *"Statul islamic este o amenințare hibridă: de ce contează asta?"* . *Jurnalul războaielor mici* . *Fundația războaielor mici.Adus 2015-08-05;*

[10] Schroefl, Joseph; Kaufman, Stuart. "*Actori hibrizi, soiuri tactice: regândirea războiului asimetric și hibrid"*. *Studii în conflicte și terorism* . 37 (10): 863.

[11] *** Strategia națională de apărare a țării pentru perioada 2015-2019;

[12] Berger Alois şi Weident Medana, *Lupta pentru piticul economic Ucraina*, Deutsche Welle, 2014. http://www.dw.de/lupta-pentru-piticul-economic-ucraina/a-17541536;

[13] I. Bălăceanu,. & I. Martin, & V. Dragomirescu, *Interacţiunea sterategiilor în conflictele armate moderne*. *Editura Universităţii Naţionale de Apărare* „Carol I", Bucureşti, 2010;

[14] Bostan Radu, *Ucraina, la confluenţa intereselor marilor puteri. De ce este importantă Ucraina*?, Ziarul Financiar, 2014, http://www.zf.ro /business-international/ucraina-la-confluenta-intereselor-marilor-puteri-de-ce-este-importanta-ucraina-12179700;

[15] T. Frunzeti, & V. Zodian, *Lumea 2015 - Enciclopedie Politică şi Militară (Studii strategice şi de securitate)*. Editura CTEA. Bucureşti, 2015;

[16] A. Grumaz, *Al treilea război mondial,* Editura RAO. Bucureşti, 2013;

[17] Katz Nina Judith, *The True Interests of the US and Russia in Ukraine*, Daily Kos, 2014, http://www.dailykos.com/story/2014/05/04/1296752/-The-True-Interests-of-the-US-and-Russia-in-Ukraine;

[18] I. Martin, *Raționament și argumentare în planificarea operațiilor*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2015;

[19] D. Miron, *Aspects on the Operationalization and the use of Military Power in Multinational Operations* - Review of the Air Force Academy Vol XIII, No 1(28)/2015;

[20] O. Moșoiu, *„Risks, vulnerabilities and possible threats of the european security environment*" in Review of the Air Force Academy, nr.2(15)/2009, Braşov: Air Force Academy Publishing House;

[21] O. Moșoiu, I. Martin, „*Riscuri și amenințări cu impact asupra mediului de securitate euroatalntic, generate de climatul de instabilitate din spațiul est european și zona extinsă a Mării Negre"*, Buletinul UNAp, nr. 2/2015, editura UNAp, București;

[22] Mediafax, *Juncker a anuntat un ajutor suplimentar de 1,8 miliarde de euro pentru Ucraina*, business24.ro, 09 Ianuarie 2015; in: http://www.business24.ro/international/stiri-international/juncker-a-anuntat-un-ajutor-suplimentar-de-1-8-miliarde-de-euro-pentru-ucraina-1553277;

[23] Mediafax, Soros: Europa este sub atacul Rusiei. Ucraina are nevoie de până la 50 de miliarde de dolari, business24.ro, 2015. http://www.business24.ro/international/stiri-international/soros –europa-este-sub-atacul-rusiei-ucraina-are-nevoie-de-pana-la-50-de-miliarde-de-dolari-1553282.