DIMENSIONS OF HYBRID CONFLICT AND COORDINATES FOR COUNTERING ITS EFFECTS

Colonel Assoc. Prof. Aurelian RAȚIU, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

The fields of war have changed in time, which has caused transformations, both in the approach to confrontation and in the physiognomy and typology of actions. The military conflict has been characterised by irregularity: traditional and non-traditional actors acting directly or indirectly, with their own forces or through intermediaries (proxy forces), creating their own conventional or paramilitary military structures, and carrying out conventional actions concurrently with terrorist activities specific to insurgency or organised crime.

The solutions for countering the hybrid conflict must be understood in terms of summing up the known (conventional) and the less known characteristics of the conflict, as well as of developing new, unexpected, surprising (irregular) ones, determined by the evolution in the operational field.

Keywords: hybrid conflict; operational environment; hybrid threats; combating the effects of hybrid conflicts; area of responsibility;

INTRODUCTION

Given the interdependence within the relations between states regarding the sectors of economics, security, proliferation of risks and irregular threats (terrorist attacks, attacks with biological agents, with vectors carrying CBRN substances, informational aggressions, cyber or geophysical attacks, organised crime, illegal migration) and of the globalisation of the field of confrontation between the multitude of actors, it becomes obvious that the *hybrid war/conflict*, in the current sense, can be considered an actual, dynamic and very complex concept.

The issue is relevant from the perspective of both the effects of hybrid threats that spread in all confrontation environments and the permanent adaptation of military structures and the development of complementary capabilities in order to be able to meet these challenges in a pertinent and effective manner.

HYBRID OPERATIONAL ENVIRONMENT AND HYBRID CONFLICT DIMENSIONS

In the light of the existence of threats, *aggressions* and *hybrid operations*, the following question arises: where are these carried out? Therefore, the environment in which they take place is characterised by a wide range of components: the actors, the physical space (land, air, naval, cosmic) of the actions, information, technology, cultural environment, risk factors, threats, etc.; basically, a mix of elements whose combination leads to something complex and new, to a *hybrid environment*.

The operational environment in the current context can be understood as a range of conditions, circumstances and actions created by the multitude of actors that interact in a certain area pursuing their own interests and that influence the decisions regarding the employment of the military and non-military capabilities at their disposal, in order to achieve the expected goals. The hybrid operational environment, in another perspective, represents *"the framework for the manifestation of hybrid threats, and it implies the complex and combined configuration of the chessboard of actors, means, actions that converge in a concentrated manner and most often in secret, towards fulfilling the pursued goals"* (Ganea, 2016, p. 65).

In general, the most important constituents of the hybrid operational environment could be the following: *Physical environment/domain (land, air,*

sea); Actors that produce threats and dangers; Civilian/local population; Agencies and organisations; Independent actors; Unknown actors; Information and cyber environment.

Physical Domain/Environment (land, air, sea)

The physical domain is the land, air, sea and *space environment* in which/on which the forces/capabilities of the parties will confront each other in order to achieve their interests/objectives. Thus, this scientific approach refers to some less studied aspects of the dimensions of the hybrid conflict, such as: *aerial* and *maritime*, in comparison with the others, terrestrial and informational ones.

The land domain is the terrestrial/dry geographical environment (the surface of the lithosphere) including all its natural elements, as well as those created by the human hand, which, one way or another, influence the organisation, preparation and conduct of conventional or unconventional actions. The forces will act in a variety of areas, both in the classic ones: planes, hills, plateaus or mountain-forested land, and in other regions, such as the Arctic, the coastal (seaside), jungle, desert or urban areas. Campaigns often involve a *combination of such environments*.

The physical domain for *the maritime component* (sea and river forces) is represented by *oceans, seas, rivers, sunken lands* and *inland waterways*. The maritime environment – the surface of the oceans, seas, rivers and their depth (the underwater space) is the place where the actions of the naval component take place and represents two thirds of the planet's surface. The maritime environment allows forces to have access to the coast, to have mobility, projection and logistic autonomy. The maritime activities are influenced by the meteorological, oceanographic and geographical conditions of the marine environment: the size of the waves, the force of the wind, the speed of the currents, the temperature of the air and the water, the transparency of the water, the tides, the salinity and the density of the water, the characteristics of the bottom of the waters (sea, canals and rivers) – factors that also influence the ability of ships to navigate and use the weapon systems.

The air force, which operates mainly in the air and space environment, essentially changed the conflict paradigm. *The air domain* is *"that continuous environment that surrounds the entire planet, being delimited only by the land surface and the sea surface. This feature facilitates certain differentiated advantages compared to the terrestrial, maritime and underwater environment, generated by a certain freedom of action, constrained only by the performance of the aircraft at the geophysical*

borders and the abilities of the crews" (Roman, 2017, p. 20). The emergence of hybrid threats in the airspace complicated the intervention of the elements of air force in the conflict equation, through the prism of the air force capabilities and their role in relation to a hybrid adversary.

Actors Producing Hybrid Threats

Threats can occur in different forms, coming from groups such as (Rațiu, 2020, p. 46):

- conventional military forces, easily identifiable on the basis of uniform and the weapons *"worn in plain sight"*, acting conventionally/traditionally;
- unconventional/irregular forces, difficult to identify, acting through a combination of violence and subversion: proxy forces, terrorist networks, guerrilla groups, organised crime cartels, ideological groups capable of building paramilitary structures or transnational terrorist networks, hackers or groups of hackers, organizations specialised in laundering and recycling dirty money, mafia associations, pressure and destabilisation groups, etc.

In some cases, opposing forces can produce *hybrid risks* or *threats*. In such cases, a grouping may combine the conventional forces/actions and the unconventional forces/actions in a complementary manner. In other cases, a single force can in itself adopt a combination of actions with conventional and unconventional characteristics.

A) *On the ground*, some potential adversaries may use advanced weapon systems in irregular/guerrilla tactics or change irregular and conventional tactics, depending on the situation. Generally, the proxy, guerrilla military forces use conventional weapons against security structures, but in different tactics, of hybrid type, such as: the placement of improvised explosive devices, hastily prepared attacks and ambushes, indirect fires with the help of more or less advanced, perhaps even improvised, systems, acts of terrorism (suicide/kamikaze attacks, assassinations, kidnappings and false imprisonments).

B) *Naval* military confrontations have a predominantly offensive character and imply continuous manoeuvrability. Most of the time, the actions of conventional and unconventional naval forces will start at sea and end on land. To do this, it is operated both with large battleships and with small, fast means, easy to manoeuvre, with good protection of the embarked forces, and also with considerable striking power. International terrorism acts not only *on land but also on the sea* and it represents a real and complex threat. Preventing terrorist attacks on or from the sea, as well as countering the illegal crossing of maritime borders by terrorists,

became a major concern for the states with access to seas and oceans. Terrorism and associated actions had the effect of increasing the number of *maritime piracy* acts. Moreover, the identification of the common interests of the *terrorists* and *pirates* led to the coalition and even the unification of the groups, to the extension of the areas of action and also to qualitative changes in techniques of action and in the used arsenal.

C) *Airspace* capabilities respond to a wide range of threats, threats that are used during both conventional and unconventional operations: multi-role fighter jets, attack helicopters, unmanned aerial vehicles, anti-radiolocation missiles, ballistic missiles, tactical missiles, ISR – Intelligence, Surveillance, Reconnaissance capabilities.

The most relevant threats remain the conventional, traditional ones, consisting of fighter jets and helicopters. However, it is estimated that the use of unmanned aerial vehicles has recently gained ground. In addition to conventional threats, state and non-state actors make extensive use of other hybrid air threats, in particular civil aircraft (use of passenger planes as a weapon during the September 11, 2001 attacks in the United States) – *RENEGATE threats*, small unmanned aerial vehicles (drones) or the use of anti-aircraft missile systems to shoot down civilian aircraft (as in Ukraine and Iran).

Civilian/Local Population

Most actions and campaigns are carried out among or affecting the civilian population and the military and security structures will have permanent contact with the local population. This requires leaders/commanders at all levels to consider, from the time of planning, the effects that security operations will have on civilians, local communities and infrastructure. Approaches in this regard may vary:

- in *conventional confrontations*, the aim is to avoid the production of victims among civilians by evacuating and/or relocating them, arranging refugee camps, etc., and, also, to avoid damaging civilian infrastructure;
- in *hybrid conflicts*, operations focus on protecting the civilian population against attacks and abuses from opposing groups, on combating the effects of their psychological actions, and on support actions (rebuilding/building infrastructure, offering medical and educational services, etc.) so that government and the international coalition/alliance forces gain authority and legitimacy (thus, the neutral civilian population supports the government component).

The civilian population and society as a whole are the centre of gravity in the hybrid war. The attractiveness regarding the use of the population/society derives

from *"the large dimensions, the structural heterogeneity, the ease of producing the desired effects, the existence of possible fault lines between ethnic groups (breaches in the homogeneous character), the involvement of segments of population extremely permissive to certain messages, offering the possibility of manipulation"* (Mihalcea, 2018, p. 18). All the listed elements can represent vulnerabilities and can be speculated by the conflicting entities.

Agencies and Organisations

Relevant institutions/agencies and organisations can be represented by local and international government departments/institutions, host nation security forces, coalition military forces, non-governmental organisations (NGOs), private security organisations and even independent businessmen.

In the current operational environment, national and coalition military/security forces, following the model of the hybrid approach, are no longer at the forefront, as in war, but have a well-defined role by getting involved in supporting the actions of other governmental and non-governmental agencies and organisations to reach various objectives: political, economic, social, military, cultural, etc.). Moreover, in order to generate the necessary conditions for government institutions and civilian bodies to achieve lasting effects on the political, economic, social, etc. level, the military instrument is directly involved in conducting actions extremely necessary to create a climate of security and stability.

Unknown and Independent Actors

Some actors in the operational environment will be considered *unknown* in terms of the support (given or not) of the campaign/forces pursuing security. Indigenous actors will support the campaign if they believe that the final goals and objectives, as well as the methods/means of achieving them, are legitimate or support their own interests. Their perception of legitimacy will depend on their culture and social expectations. Thus, the perceptions and interests of these actors need to be understood in order to act in their support and to protect them for the benefit of the campaign. Some actors will act completely independently *(independent actors)* from legitimate government forces, even if their ultimate goals are the same as those of the campaign. Such groups will avoid interaction with military forces, pursuing their own goals. The decision-makers need to be aware of the presence of such organisations in the area of responsibility and especially of the effects of their actions, and how they can affect the fulfilment of the assigned objectives (NATO Chiefs of Staff, 2016, pp. 1-5).

Information and Cyber Environment

The information environment represents the cognitive, virtual and physical domain for all the actions and processes that involve gathering, processing and using information. The information environment is composed of *"individuals, organizations and systems that collect, process, disseminate or act on information"* (US Department of Defense, 2016, p. 2).

The information is the link between the physical environment and the other areas that the actors involved use the integrating element of all the actions taken to reach the set objectives.

The decision, in any field, but especially in the field of conflict management, requires timely, accurate and rigorous information, and prediction regarding the need for information plays a particularly important role in the context of ambiguous situations specific to hybrid confrontations.

Currently, the whole company is connected in a *"network"* (Internet network, GSM communication systems, social networks, etc.), which allows both state and non-state actors to use the techniques and means specific to the information environment to reach their goals. They use a variety of means to exploit, disrupt or disable decision-making systems, to misinform and promote propaganda products, to strengthen internal resistance, to recruit supporters, to solicit funding and to promote the legitimacy of their actions, simultaneously with discrediting the actions of other actors, these actions and activities taking place in the information environment.

A significant component of the information environment is the *cyber space*, which overlaps the physical and information dimensions. It is essential that the analysis of the information environment also include actions in the cyber space and the identification of key individuals and groups influencing decisions and the native civilian population through *cyber space*. The *cyber space* represents *the virtual environment, generated by cyber infrastructures, including the processed, stored or transmitted information content, as well as the actions carried out by the users in it* (Guvernului României, 2013, p. 7).

The power offered by the information technology and the means within the cyber space is part of the hybrid war as a strategy for state or non-state actors to achieve their objectives.

The maximum benefit of any form of attack realized in the cyber space increases when this form is integrated with the other methods and means of attack, becoming a complementary element and leading to the *hybridisation* of the confrontation. The use of hybrid elements provided by the cyber domain (cyber attacks, propaganda through the virtual environment, social networks, etc.) can be a factor of force multiplication.

IMPERATIVES IN COMBATING THE EFFECTS OF HYBRID CONFLICTS

For a better understanding of the operational context of hybrid confrontations, of the nature of these types of threats, it is necessary to identify the imperatives and then the directions of action to limit or eliminate the specific risks.

The imperatives in the hybrid confrontations are represented by the context of the changes in the operational environment and by the available means used in the combat strategies.

The cognitive imperative. It refers to the cognitive-psychological component of hybrid warfare and implies a good understanding of the operational environment in the area of responsibility, so as to identify the best methods and tools through which a certain perception of the adversary is generated, so that the opponent, involuntarily, decide and act to his disadvantage. This idea is included in the concept of reflexive control, a concept from the Eastern region, which involves *"the action of providing an adversary with specially prepared information that will lead him to a voluntary decision that benefits the initiator of the action"* (Georgescu, 2016, p.79).

This nonlinear approach is, in fact, an atypical way of thinking, which creates the conditions for implementing power/influence in areas of interest, the simultaneous use of an extremely varied range of non-military methods and means aiming at concealing real geopolitical, military, economic etc. intentions and influencing the adoption of predictable decisions by competitors. The main purpose of these actions is to create a direct, rapid and significant impact on the efficiency of the military and non-military measures that the adversary takes.

In this regard, the operational approach must be able to ensure the most effective counteracting of the cognitive aspect of hybrid threats, through articulated actions that can be carried out at all levels, by employing the most appropriate capabilities. These actions must be carried out in such a way as to have the effect of effectively counteracting the threats and creating the necessary conditions for further action.

The imperative of a comprehensive approach. In the context of opponents using hybrid threats, the imperative of the comprehensive approach refers to the creation of opportunities for tactical, punctual/domain-based operations, and also actions aimed at generating strategic and chain effects with implications in many areas. It is about combining efforts to understand the phenomenon of hybrid warfare and to develop mechanisms for early identification of the threat and responding effectively to hybrid aggression. Fighting hybrid threats is a very complex activity, and the measures taken to limit their effects go beyond the scope and responsibility

of a single actor/institution, involving a *comprehensive approach* – combining/integrating in time and space the efforts of all power instruments, actors/parties involved, both internally and especially internationally.

Pattern imperative – involves avoiding organisation, planning and linear, uniform development of actions/measures in time and space. Based on a good knowledge of the complexity of the operational environment, this aspect is relevant for avoiding surprise, by means of thinking, concepts and measures that circumvent the doctrinal approach to operations. While the military regulations require establishing clear and precise procedures, the new operational vision requires from the leader a much more in-depth analysis of the situation and the factors, an approach different from the dogmatic, traditional one being imperative.

The analysis of these imperatives reveals an intrinsic connection between the cognitive field of understanding the complex adaptive systems in the hybrid conflict and the physical field, between the violent and non-violent, military and non-military component and the efforts of the power elements at all levels.

These imperatives are considered to be essential because their understanding facilitates taking the necessary measures for the management of hybrid conflicts at decision level.

CONCLUSIONS

The complexity of the hybrid conflict includes violent and non-violent, politico-diplomatic, informational-propagandistic, commercial-economic with corruption elements, research-diversionist partisanship, energy and critical infrastructure, cyber, CBRN etc. military methods and means.

Thus, the effects of hybrid conflicts are propagated in all the environments in which the conflict takes place, whether we refer to the land, air, maritime, information and cosmic domain, or to other areas of social life: political, economic, diplomatic, cyber, social, cultural, religious etc.

Any response to hybrid threats will require a comprehensive/integrated approach by employing a wide array of military, non-military, governmental and nongovernmental instruments.

Integrated actions (interagency, inter-institutional), placed on a higher level, will not only mean the cooperation or joining of governmental instruments, but also their merger/integration, involving international or non-governmental organisations as well.

BIBLIOGRAPHY:

1. Ganea, I. (2016). *Noul mediu de securitate şi consecinţele sale. Războiul hibrid ca fenomen actual*. Bucureşti: Revista Oștirii Române, no. 1.
2. Georgescu, D. (2016). *Războiul hibrid – cea mai complexă formă de aplicare a artei operative*. Bucureşti: Buletinul Universității Naționale de Apărare *"Carol I"*, no. 2.
3. Mihalcea, V.C. (2018). *Fundamente şi ţinte ale războiului hibrid în acţiunile beligenei contemporane*. Bucureşti: *Infosfera* Review, no. 1.
4. Rațiu, A. (2020). *Conflictul hibrid. Forme de manifestare și modalități de gestionare.* Sibiu: Editura Academiei Forţelor Terestre *"Nicolae Bălcescu"*.
5. Roman, D. (2017). *Riposta antiaeriană a Forţelor Terestre din perspectiva modelelor conceptuale de lucru colaborativ*. Bucureşti: Editura Universităţii Naţionale de Apărare *"Carol I"*.
6. Chiefs of Staff (2016). *AJP-3.2.-Allied Joint Doctrine for Land Operations*, Brussels: NATO Standardization Office.
7. Guvernul României. (2013). *Strategia de securitate cibernetică a României. Monitorul oficial*, no. 296 of 23 May 2013, https://cert.ro/vezi/document/strategia-de-securitate-cibernetica, retrieved on 29 March 2020.
8. US Department of Defense. (2016). *Strategy for Operations in the Information Environment*. Virginia: Department of Defense, SUA, https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf, retrieved on 19 March 2020.