DE GRUYTER OPEN

Land Forces Academy Review
Vol. XXII, No 1(85), 2017

SPACE – AN ESSENTIAL FEATURE OF THE HYBRID WAR

Dorin IONIŢĂ
Romanian General Staff, Bucharest, Romania
dionita@mapn.ro

ABSTRACT

Hybrid Warfare is an unofficial intellectual construct to describe the combination or integration of conventional and non-conventional approaches used by adversaries to avoid conventional military strengths, often times occurring below the threshold that would trigger a conventional military.

The word "hybrid" is used more for its descriptive value to aid concept writers and military planners in understanding the intersection, interaction, and amplification of trends and conditions that impact the scale and scope of military actions.

The paper explains the role of space as an essential characteristic of hybrid warfare.

KEYWORDS: hybrid warfare, conventional warfare, irregular warfare, space, technology, infrastructure

1. Introduction

In recent years, the traditional, detailed planning processes have proven to be especially effective at hybrid warfare problem solving, but not always *the right problem*. Innovation and adaptation provide the flexibility that allows us to adjust to the dynamic nature of the hybrid operational environment.

Warfare has changed – no concrete battle lines exist, technology is an ever-changing friend and foe, and globalization brings myriad players into the equation that did not exist even two decades ago. The nature of the global environment – especially the myriad dynamic and competing cultures, the derivative range of actors (both combatants and non-combatants) coupled with technology proliferation – ensures the operational environment subsets will show continuous change over the next 20 years.

2. Hybrid War – Descriptive Values

The history of using the concept of *hybrid war* reveals numerous studies and analysis, often contradictory, which develop or are influenced by ideas sometimes considered futuristic or by some conservative or even by some pragmatic ones. This issue is also reinforced by specialists in the field, such as Paul Latawski (2011), who states that: *"fashionable 'big ideas' may be nothing new in the history of war and neither is their impact so profound as to change its nature or character"*.

Amid the character of interdependence of states and present societies, generator of new vulnerabilities, risks and threats, it becomes evident that the *hybrid war* as meant today may be considered as not being a surprising phenomenon, considering the development

DOI: 10.1515/raft-2017-0001

of complementary capabilities, planned to be used for the accomplishment of the strategic objectives.

Although the phrase *hybrid war* was used for the first time, by Thomas R. Mockaitis, in his work *The British Counterinsurgency in The Post Imperial Era,* published in 1995, Latawski (2011) points out that, *"there is really nothing particularly new about the hybrid nature of war and... indeed, all wars are hybrid and it is only the characteristics of hybridity that change over time"*.

The transformations in the security environment, specific to the last decades reveal that security management can no longer be analyzed by taking into consideration templates, principles and changeless criteria, but it is becoming more and more dependent on a multitude of variables. However, a constant feature, with a decisive role in shaping the hybrid actions is *the space* determined by three coordinates: geographical, virtual and cognitive one.

3. Space – An Essential Feature of Hybrid War

According to *The Explanatory dictionary of the Romanian language,* the space is defined as *"the limits to which an action is carried ou"* (Academia Română, 1998).

Although there are conflicting theories concerning the relationship between the hybrid war and borders, it is certain that one of the goals as well as one of the effects of the hybrid war is to eliminate borders. On one hand, an eloquent example in this respect, the recent conflict in Ukraine, reveals and confirms the influence of the hybrid war over borders. It is recognized the fact that the Russian-Ukrainian common border in Dombas, represents an obstacle to the maneuver forces and military and non-military capabilities, supply materials- in general, to the freedom of movement.

On the other hand, the existence of borders, in the scenario of the hybrid war in which the tendency of employment of its components at great distances without leaving their mark or making themselves visible, has no relevance.

From the perspective of the subject of this article, *the infrastructure* represents the area that limits and is preferred as development space of the hybrid war. According to *The Explanatory dictionary of the Romanian language*, *"infrastructure"*, in this context, is *"the assembly of the elements which constitute the technical-material base of a society"* (Academia Română, 1998).

Conceptually, in the opinion of specialists, infrastructures are divided, as a rule, into three broad categories: *common infrastructures, special infrastructures* and *critical infrastructures* (Alexandrescu and Văduva, 2006). An important feature is that these three types are interconnected, they can move from one category to the other, cyclically, depending on the nature of the safety and security of the systems or processes whose components they are. Thus, the infrastructure becomes critical due to the importance of its destination and the negative effects that it produces, if used in hybrid war tactics and techniques, or simply if it is destroyed.

The history of institutionalizing the concerns regarding the definition and protection of critical infrastructures began with the action of the President of the United States of America, Bill Clinton, to issue, on July 15, 1996, *"The Executive Order 13010 for the Critical Infrastructures Protection"*.

Critical infrastructures, for the purposes of this document, represented those national facilities of vital importance, whose incapacity or partial or total destruction could have serious consequences, particularly on the defense or economic security of the United States. The Executive order includes, as critical structures, the following:

telecommunications, electricity systems, fuel depots and transportation networks, banking/finance, water supply systems, emergency services (medical/ police/fire brigade) and the stability of the Government. Later on, during the Bush administration, following the events of September 11, 2001, a new Executive order was issued, Executive Order *13231 − Critical Infrastructure Protection in the Information Age*, a more comprehensive one in which the critical infrastructure was defined as being *"any physical or virtual system or goods /means, of such importance to the United States that its incapacity or destruction may affect safety, in terms of military and/or economic, public health and the safety of citizens, or any combination of the above"* (The White House, 2001).

Romania was aligned to the European and transatlantic concerns and approved, *"The National Strategy for the Protection of Critical Infrastructures"* (Guvernul României, 2011).

We note therefore that the most important components of critical infrastructures are the following: communications system architecture; the infrastructure that ensures mobility in the three spaces of manifestation; spaces/means of securing resources; spaces which ensure the functioning of institutions with competences in terms of governance of the state and ensure the safety and national security. Particular attention is paid to the computerization today, especially in terms of its global character, identifying the twenty-first century as a period of *cyberspace.*

The cyberspace is recognized by NATO as an operational field of war, alongside with the land, air and sea spaces, its importance being underlined by the NATO Secretary-General, Jens Stoltenberg, in his speech at the *North Atlantic Council meeting at the level of NATO Defence Ministers,* in Brussels, Belgium, in June 2016, saying that *"most crises and conflicts of today have a cyber dimension"* and, *"treating the cyber world as an operational domain, would allow us to better protect our operations and missions".*

Here is therefore a new dimension of the space, of the hybrid war, respectively, *cyberspace*, which brings with it not only the multiplication of risks and threats, but also an increase in their degree of complexity, whether it is political, economic, social or security.

In the current environment of security, no one doubts that the hybrid warfare is a form of fighting the cold war nor the fact that the cyber-attacks is a weapon of the hybrid war. These two realities require the increase of the pace for the implementation of countermeasures.

Another important element of the cyberspace is the *radio spectrum*, part of the electromagnetic spectrum. The radio spectrum, quantified as an important national resource, is one of the areas mostly subject to strict international regulations, through the International Communications Union, which operates under the aegis of the United Nations (UN).

At the NATO level, the space for the engagement of forces, in the event of a hybrid – type crisis, is evaluated according to the pillars used within the concept PMESII (political, military, economic, social, of infrastructure and information) (Air Force Research Laboratory, 2009).

According to some foreign and Romanian military specialists (Paul, 1999), the development spectrum of warfare asymmetric actions, such as the hybrid war, includes: global (planetary) space, for which strategic concepts are elaborated; the space of some areas of the globe, including those located at large distance between them, where political, economic, spiritual interests, etc. are maintained or promoted (by force of arms as well); strategic interest space (an area or a land or sea region in the vicinity of national territory); the national territory.

Therefore, the hybrid war prefigures complex interdependencies of historical, political, social, cultural, economic nature, which generate, to the same extent, both effects and solutions. History helps us, from this point of view, with countless examples out of which the manifestations which started during ancient Rome, when Jews, from the year 66 A.D., Vespasian led legions, took place in old Rome when the Jews' revolt of 66 A.D. against the legions of Vespasian was carried out by motley fighters composed of soldiers, mercenaries, criminals and thieves, who used an uneven variety of methods and combat techniques.

Not even the army of Napoleon was exempted from such actions in the year 1806, in the Iberian Peninsula, on the part of Spanish guerrillas, allied with the Portuguese and British forces.

During the war in Vietnam, the North Vietnamese regular army synchronized its operations with an irregular force, Viet Cong, aiming at succeeding a long-standing engagement with the armies of the United States of America and France. And the examples can continue, depicting the confrontations of the forces waging the war between Israel and Hezbollah.

But the latest and most complex way of applying the hybrid threats is represented by the action of the Russian forces for the occupation and annexation of Crimea. In this context, we consider the statements of the Chief of the General Staff of the Russian Federation, Valery Gerasimov (2013), relevant, referring to the fact that *"the center of gravity of the methods applied in the conflict has changed, towards the widespread use of the political, economic, informational, humanitarian means and other non-military measures, implemented in coordination with the potential protest of the population"*.

4. Conclusions

These historical landmarks, with fingerprints in the genesis of the hybrid phenomenon, become therefore particularly useful in identifying the actors in such a conflict, incorporating the most diverse forces and means, sometimes spontaneously, configured for actions and effects that converge concertedly. The term *hybrid i*s, at the same time, sufficiently vague and complex to mean anything, but for sure *the Trojan horse*, the decisive vector can be represented by an increased flexibility in the taking of decisions, the freedom of action of forces in the field or the technological factor.

REFERENCES

Academia Română. (1998). *DEX: Dicţionarul explicativ al limbii române*. Bucureşti: Univers Enciclopedic.

Air Force Research Laboratory Information Directorate. (2009). *Political, military, economic, social, infrastructure, information (PMESII) effects forecasting for course of action (COA) evaluation*, available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA501499

Alexandrescu, Gr. & Văduva, Gh. (2006). *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie*, Bucureşti: Editura Universităţii Naţionale de Apărare "Carol I", 6.

Clinton, W.J. (1996). *Executive Order 13010 – Critical Infrastructure Protection*, available at: http://www.presidency.ucsb.edu/ws/?pid=53066

Gerasimov, V. (2013). The Value of Science in Prediction, *Military-Industrial Kurier*, *February 27*, available at: https://inmoscows shadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Guvernul României. (2011). *Strategia naţională privind protecţia infrastructurilor critice*, available at: http://www.monitoruljuridic.ro/act/strategia-nationala-din-13-iulie-2011-privind-protectia-infrastructurilor-critice-emitent-guvernul-publicat-n-130567.html

Latawski, P. (2011). The Inherent Tensions in Military Doctrine. *Royal Military Academy Sandhurst Occasional Papers No. 5*, 3.

Paul, V. (1999). *Conflictele secolului XXI. Proiecţii în spaţiul strategic*. Bucureşti: Militară, 39.

Stoltenberg, J. (2016). *Press conference at the North Atlantic Council meeting at the level of NATO Defence Ministers*, available at: http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en

The White House. (2001). *Executive Order 13231 − Critical Infrastructure Protection in the Information Age*, available at: https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf