DE GRUYTER OPEN
International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXIII No 1 2017

# THE HYBRID WARFARE IN THE 21ST CENTURY: AN OLD CONCEPT WITH A NEW FACE

**Ionut Alin CÎRDEI**

**"Nicolae Bălcescu" Land Forces Academy Sibiu, Romania**
**cirdei_alin@yahoo.com**

***Abstract:*** *In the last years the focus of the military specialists changed from the asymmetrical threats to the hybrid threats, seen as one of the main challenge for the security in the 21st century. The increased attention paid to hybrid threats is due to the events that took place in Ukraine, Syria and other confrontation areas and which highlighted the vulnerability of the modern societies and modern armies toward this type of actions. The use of hybrid type tactics can ensure the achievement of the main objectives of an international actor, with a low effort, usually without using the force, and can deny to the target/victim the possibility to take any defensive actions. The hybrid warfare can represent the war of the 21st century, a new type of direct or indirect confrontation, with effects on short and medium term, impossible to be anticipated.*

**Keywords: hybrid, threat, confrontation, international actors**

## 1. Introduction

The term of hybrid conflict is not new, and its origin is lost in the darkness of time. This concept appears again in the world's attention now that the nature of the war has changed completely and the mix of conventional actions with unconventional, asymmetrical, irregular ones has become a reality. Moreover, the delimitation between peace and conflict has become very difficult to accomplish, hostile actions may take place long before a conflict breaks out officially and long before the victim realizes it.

In the twentieth century the world has become accustomed to seeing things in black and white, in terms of peace or war, and the cold war has been officially recognized as a state of tension between the main political and military blocs. At that time, things began to get shades of gray, and the techniques specific to the hybrid war were reinvented. In the 21st century gray is the new dominant color in the international environment, and the hybrid confrontation is an expression of this change of perspective.

Starting from the idea that a war begins long before the weapons are used and that international actors use a wide range of means to reach their goals, we can say that the hybrid threat is more and more present and that it becomes omnipresent in all current confrontations, all the more so as society is more vulnerable in the era of globalization, technology and informatisation.

With the increase in the speed of information transmission, with the increase in the amount of information available at all times, all states, all institutions and all individuals have become increasingly vulnerable, and the promoters of the hybrid war are doing nothing but exploiting these vulnerabilities.

## 2. The revival of the concept of hybrid war in the 21st century

The international security environment behaves as a living and adapting organism

DOI: 10.1515/kbo-2017-0011

that constantly seeks steady state and is now subject to huge pressures that may destabilize it, pressures that may come from both legitimate and illegitimate actors, by using legal or illegal, traditional or hybrid means [1]. In this context, in order to avoid direct confrontations between states, confrontations that may have immense costs, effects that can be difficult to predict, there is an increasing preference for using asymmetric and hybrid means for weakening the opponent, due to the smaller costs, huge potential and the difficulty of identifying the real attacker, especially in the conditions of using the informational and cybernetic environment. Also, the use of hybrid war offers hopeless states or terrorist organizations the hope of winning a conflict, even in the face of a strong asymmetry, which turns this type of conflict into the conflict of the 21st century.

The very famous Chinese general, Sub Tzi, has highlighted the importance of using hybrids tactics to win a victory against any opponent over two thousand years ago, arguing that the most effective victory is to subdue the enemy, reduce his strength without calling to the force of the weapons. In other words, all the non-military means available to exploit the weaknesses of the adversary must be used, in the economical, social, political, diplomatic field, and, we add, we can do this without the opponent being aware of this action. Kneeling the opponent, influencing it, directing its actions or determining it for action or inaction can be done by using in a modern conception the procedures specific to hybrid war.

It is not about inventing new processes, actions, the revolution of strategic thinking, but only about using the modern means to achieve the goals, by timely using, from the perspective of time and space, the methods that exploit the ever more numerous vulnerabilities of any system and interdependencies between systems and system elements.

The hybrid conflict came to public attention after Russia's annexation of the Crimean peninsula and its involvement in the perpetuation of the conflict in the East of Ukraine. Public opinion and military specialists were surprised by the effectiveness of these methods due to the surprise effect and the impossibility of combating them.

As a result of the analyzes carried out by specialists, by taking into account the different levels of intensity of the threats and the intent of the actors involved, several elements can be distinguished, such as: hybrid threat, hybrid conflict, seen as a situation in which the parties involved refrain from openly using the armed forces, instead using a combination of classical, irregular and hybrid means, and hybrid warfare, in which the armed forces are used openly, simultaneously with the use of an ensemble of economic, political, diplomatic means, etc. [2].

The hybrid war in the 21st century exploits internal weaknesses by using non-military, political, informational, economic means, but also by using manipulation, intimidation, misinformation, and it does not exclude, and is often supported by, the use or threat of using conventional military means [3], as was the case with recent Russian actions in Ukraine, finalized with the annexation of Crimea, the creation of a separatist conflict in eastern Ukraine, which will most likely turn into a frozen conflict and by removing Ukraine from the process strengthening the ties with NATO and the EU.

The new hybrid conflict is not reserved for states, and can be run by any kind of state or non-state actor who does not obey or circumvent international law.

The specialists in the field of hybrid conflict and threats believe that the basis of the hybrid war is represented by the use of subversive techniques and focuses on four main stages: demoralization and successive or simultaneous destabilization of the target, creation of the premises for the

outbreak of a crisis in the target society and taking control over the target society by using internal forces acting in concert with the attacker [4].
Once again, we can say that it is about the reinvention of techniques, of old strategies, in line with the evolution of technology and computerization, which allow the intensive use of cybernetic space to hide both the real face of the threats and their initiators.
Hybrid threats are nowadays the same as they were in the past, in the whole spectrum of confrontations, with the indication that they make evident their presence either as hybrid threats in the gray area or as open hybrid threats [5], the first category being much harder to identify and counteract. Unlike the hybrid threats that have occurred in the past, the current ones have to be analyzed in line with the unprecedented development of the security environment with the integration of new dimensions such as cosmic and informational ones.
Currently, hybrid conflict can be a way to achieve the objectives for certain actors in the security environment and can be seen also as an expression of the effect-based approach. Due to the many facets that this kind of conflict can have and due to the multitude the means of putting into practice, we can say that the implementation of this concept is limited only by the imagination of those who carry it.

## 3. The future of hybrid warfare

Due to the expansion of the phenomenon of globalization, the world becomes more vulnerable because of the interconnections and interdependencies between countries and between regions, and the exploitation of these vulnerabilities becomes an objective of actors aimed at destabilizing the system or its parts. The practitioners of the hybrid war, understanding how profoundly interconnected is the world of today, seek to impose their own will on the opponent by weakening the society as a whole, targeting the key points that ensure his normal functioning [6]. By striking key points, tactical or even strategic gains are sought with minimal effort and with the greatest possible media and moral impact, as society is not yet ready to face this challenge, and individual and organizational resilience, as well as the ability to react and understand is limited.
In the future, we believe that the hybrid conflict will develop, will gain new followers and new forms of manifestation will emerge, because society is vulnerable, both in the physical environment and especially in the cybernetic environment. Protective measures adopted by states or by organizations and individuals can temporarily limit the effects of hybrid attacks but will certainly cause initiators of attacks to discover new methods and new means of action.
Important to this type of conflict is that it can take place in all phases of a crisis, without the target being clearly aware of being attacked. Hybrid aggression methods can be used in peacetime when they are often hidden under the guise of regular activities such as funding of certain organizations, parties, and people, in order to promote interests, ideas or to prevent certain activities being carried out. Here, we can provide as example the support for non-governmental organizations that appear to be disinterested in promoting or limiting certain activities, supporting publications or television stations that focus on a particular direction, promoting messages with a clear target, supporting political parties or candidates for various positions in the state so that they can then be used in the interests of certain actors or launching campaigns to influence public opinion, online and offline, by posting messages, attempting to influence the public by commenting on specific issues and topics etc.
In times of crisis, hybrids means used will become more aggressive and will multiply, targeting the most important points on the opponent's territory, without the initiator of the attack being clearly identified and without being easily counteracted, because

the target's efforts will be aimed at limiting the effects and identifying suitable protection and control measures.

When it comes to deciding to open a conflict, hybrid methods of aggression will become more visible and can be linked with the attacker, and these will be doubled by the use of military means. In this case, the hybrid war is only a mean of weakening the opponent, so that its military power cannot cope with aggression and ease the success of the aggressor.

The hybrid war is even more important for some states, since the use of its specific methods cannot be considered as an aggression, and when a state finds that the specific techniques against its institutions have been used, whether it is military, economic, financial, etc., can only identify the source of the attack and, as far as possible, try to punish the person or group that carried out the attack by resorting to domestic or international legislative provisions. At least in peacetime, but also in time of conflict, it will be almost impossible to prove the involvement of a state in such attacks, even if traces go in that direction, because the state will deny any involvement, as was the case with Russia in the first phases of the conflict in Ukraine and as it seems to be the case of the official and non official involvement of Russia in the US campaign for presidency.

## 4. Conclusions

The logic of using the hybrid war is found in the very essence of the war, because the ultimate goal of all those who participate in the war is to win, and most of the time the purpose excused the means. Moreover, some specialists believe that the goal of the opponent is to create a breach in the dialectics of the war and not to be drawn into a form of struggle that he knows will not win [7].

Hybrid war is not a new type of war, but in conditions specific to the 21st century, due to the expansion of the globalization phenomenon, the growing interdependencies and vulnerabilities of all states, it discovers new ways of manifestation and offers solutions to the weaker actors on the international scene which now see the possibility of achieving the goals and even of winning against powerful opponents with high potential both from a military and economic point of view. The effects of a hybrid attack on a computer network, an energy distribution system, a financial target, can be felt for a long time, and eliminating them and implementing protection measures can be very expensive and time consuming, and this attack, doubled or supported by other means of pressure, can prepare the ways for achieving the higher aim.

Combating hybrid threats becomes, in the new operational context, a particularly complex and difficult task, and the measures taken to combat them or to limit the effects go beyond the scope of one actor, involving a conjugation of efforts in time and space, and a comprehensive approach. Any answers to hybrid threats will require comprehensive approaches by engaging a wide array of military, non-military, governmental and non-governmental instruments. Integrated (interagency) actions, situated at a superior level, will not only mean joining governmental instruments, but also merging/integrating them, involving international and non-governmental organizations as well [8]. A better management of hybrid threats requires a close cooperation between all stakeholders, both internally and internationally. It is about combining efforts to understand this phenomenon, to develop mechanisms for identifying as early as possible hybrid actions, sharing real-time information between states and between specialized agencies, developing cyber defense capabilities, both active and passive and making operational effective tools to punish those who support, promote, or even directly use hybrid methods of aggression, be it people, organizations or states. As the

use of hybrid means of aggression is limited in real terms only by the imagination of the attacker, the means of counter-attack must be as diverse, flexible and easy to apply. Once the hostile hybrid type action has been identified, it must be combated with all its forces, both to limit its effects and to discourage any future use.

## References


[1] Ionuț Alin CÎRDEI, *Rolul securității energetice în asigurarea securității naționale și colective,* Editura Techno Media, p. 32, Sibiu, 2015.

[2] Patryk PAWLAK, *Understanding hybrid threats*, At a glance, June 2015, European Parliamentary Research Service, available on http://www.europarl.europa.eu/thinktank, accessed on 9 April 2017.

[3] JM CALHA, , *Hybrid warfare: NATO's new strategic challenge?*, NATO, 7 April 2015,available on http://www.nato-pa.int/Default.asp?CAT2=3924&CAT1=16&CAT0=2&COM=4018&MOD=0&SMD=0&SSMD=0&STA=0&ID=0&PAR=0&LNG=0, accessed on 6 April 2017.

[4] *Hybrid Warfare: A New Phenomenon in Europe's Security Environment*, Updated and extended 2nd edition Published by Jagello 2000 for NATO Information Centre in Prague. Praha – Ostrava 2016.

[5] John CHAMBERS , *Countering gray-zone hybrid threats*, *An Analysis of Russia's New Generation Warfare and Implications for the US Army,* Modern War Institute*,* p. 14, October 18, 2016.

[6] Marius PRICOPI, *Studiu privind efectele războiului hibrid asupra infrastructurilor critice*, publicat în: Ghiță Bârsan (coord.), Anca Dinicu (coord.), Dorel Badea (coord.), „Analiza și modelarea conceptuală a situațiilor complexe", Editura Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, pp. 56-69, 2016.

[7] LTC Bertrand BOYER*, Countering Hybrid Threats in Cyberspace*, February 15, 2017, The Cyber Defense Review, available on http://www.cyberdefensereview.org, accessed on 06 April 2017**.**

[8] Aurelian RAȚIU**,** *Countering Hybrid Threats by Integrating Civilian-Military Capabilities,* published at the 22-th International Scientific Conference „The Knowledge Based Organization", Sibiu, June, 2016,"Nicolae Bălcescu" Land Forces Academy, pp. 109- 115, 2016.