A HYBRID SECURITY THREAT

Cătălina- Gabriela CUREA

National University of Political Studies and Public Administration, Bucharest, Romania
(belgiu_catalina@yahoo.com)

DOI: 10.19062/2247-3173.2023.24.9

Abstract: *According with NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats and EU Joint Framework to Counter Hybrid Threats, approved a new Military Strategy that will help set out NATO's military priorities and approach to current and future challenges, including cyber and hybrid threats, instability across the Middle East and North Africa, and a more assertive Russia.[1]Hybrid conflict is defined as a dynamic interaction between elements of hard power (consolidation of military forces, deployment of military forces and capabilities in conflict zones, financing of separatist movements, activities to destabilize and undermine the security of a state or regions) and soft power (maintaining an economic or energy dependence, applying economic sanctions, conducting propaganda, disinformation and influence campaigns, conducting cyber attacks, etc.)[2]. Hybrid warfare encompasses a vast area of hostile actions in which military force is only a small part of a flexible strategy with long-term objectives, complemented by political, economic and informational methods.*

Keynotes: *hard power, soft power, hybrid war, hybrid threats*

1. INTRODUCTION

Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies. [3] Features of Hybrid War can be multidimensional and on the multilateral parts on society:

- exploits national vulnerabilities in political, military, economic, social, informational and infrastructural terms;
- can be initiated and carried out by both states and non-state structures;
- may use means of organized crime (corruption, blackmail, etc.) and terrorist actions, assassinations, crimes, other acts committed for the purpose of serious disturbance of public order;
- uses less visible attacks to be difficult to detect and often relies on digital information dissemination technology [4].

Hybrid threats present certain characteristics such as: "complexity, low vulnerability, difficulty to counter them, adaptability, increased lethality, use of nuclear, biological and chemical means, development of cybernetic war capabilities and damage to command and control systems through the use of anti-satellite programs".[5]

2. THE CONCEPT OF THREAT

The threat defines the totality of hostile actions, facts, intentions or strategies aimed at intimidation, potentially endangering the interests, values and national and international security objectives, affecting the normal activity of the institutions of the security structures, as well as those in the civil field. In the military literature, the threat is seen as the restriction and analysis of all information related to potential activities that may endanger state security. There are different approaches to the concept of threat, starting from a wide range of techniques and procedures of persuasion and manipulation, it can have references to the action of disadvantage and coercion, even reaching a psychic action carried out with the aim of influencing the victim to fulfill the established wishes of the aggressor.[6]

Military aggression of the Russian Federation on Ukraine led to the fact that in 2014 the system of international and regional security as well as the system was distorted international law. Virtually all international security guarantees of Ukraine (including the one in the Budapest Memorandum) can be considered unreal, given that the main aggressor pronounces himself as main guarantor – Russian Federation. "Hybrid war", from a structural and functional point of view, is unique: in form it is "hybrid", and as "asymmetrical" content. The character of the new hybrid war can be seen in the process of annexation in the spring of 2014 by The Russian Federation of Crimea, and later also in supporting separatist elements in the east Ukraine. Thus, analyzing each element of "hybrid warfare", is worth noting the fact that some elements have been used and in the classic wars of the past. The innovative character of this phenomenon resides in element correlation, dynamics and ability of their use, as well as increasing the role of the informational factor. Thus, the informational factor in some cases becomes independently, no less important as the military one. Although many researchers and polemicists point to the "hybrid" character of this war, however the conceptualization of this phenomenon remains incomplete.

Hybrid warfare "incorporates a wide range of means used in warfare, including conventional capabilities, irregular tactics and formations, terrorist acts, undifferentiated violence and coercion, as well as legislative confusions (gaps). These multimodal activities can be carried out by separate units or even by the same unit, but are generally operationally and tactically directed and coordinated in the central battle space to achieve synergistic effects".[7]

"Hybrid warfare" includes a wide spectrum of actions, in which the military component has an insignificant role. The main means of attacking the opponent are the political ones, informational, psychological and economic. These methods make it possible to achieve the necessary results - they cause political, economic and territorial damage to the opponent, disorder of the state and administrative system, demoralize society.[8]

Building the definition of hybrid warfare and hybrid threats firstly we can point out that they coexist with the conventional warfare. Actually, they are the sum of conventional and unconventional strategies as a whole, which will be explained further on this dissertation, and on a parallel line it is the mixed combination of all the types of warfare together. [9]

On the new paradigm of war Frank van Kappen states: “Hybrid warfare is a fusion of classical warfare with the use of new elements. The state that leads a "hybrid war", concludes agreements with non-state executors - fighters, groups of the local population, organizations, with which the connection is totally denied. These executors can perform actions that he himself the state would not allow them.

All actions non-state formations execute them dirty. Thus, the Russian Federation, through classic scenarios of maintaining frozen conflicts such as the Transnistrian one in the Republic of Moldova, Ossetian and Abkhaz in Georgia currently also uses energy resources as elements of "hybrid warfare"[1].

3. CYBER SECURITY - COMPONENT OF THE SECURITY ENVIRONMENT AND PART OF THE HYBRID WAR

Security is a state, as researchers in the field would say, it is influenced by the environment in which we live, the influences of international actors on it and the level of protection attributed to it, the security environment represents the totality of the influences of the system of international relations the evolutions of these relations, the changes in the balance of power, the strategic trends, the reaffirmation of certain states and all the registered changes that can affect the balance. 'Cyber-conflict' and 'cyber-war' serve as examples of the use of new technologies within the scope of hybrid threats. Cyber-war basically refers to a sustained computer-based cyber-attack by a state (or NSA) against the IT infrastructure of a target state. [10],[11]

The evolution of the technological field and technology is the main factor that allows us to use the virtual environment, along with its evolution, vulnerabilities and threats to it have also developed, and its security has become a priority both for the state and public institutions, as well as for organizations international organizations that outlined the protection of cyberspace as a priority, this priority gradually developing into a responsibility of the entire society and becoming an aspect of strategic importance. Opportunities to develop and implement interconnectivity in this environment offer new possibilities for economic, social, cultural growth and can develop a stable and strong security environment, but this can only be achieved if the level of protection is high and attention is given increased that is needed.[12]

The first step of defense against an asymmetric threat is the use of information, an advanced detection of threats is connected with the need to test the vulnerabilities of systems and remediate deficiencies, relevant training in real situations, development and enforcement of security policies are as critical as the level of development of technology. While standard defense technologies are always needed against standard hackers, avoiding an asymmetric attack requires advanced intelligence and analytics to effectively identify and address attacks.[13]

4. ASYMMETRY CONCEPT IN HYBRID THREAT WAR

Asymmetry "consists in refusing the rules of combat imposed by opponent, thus doing any unpredictable operations". [14] The asymmetric threat can be defined as "the wide range and unpredictability of military, paramilitary and information operations, led by nations, bodies, individuals or indigenous forces or by placing under their command, which specifically targets weaknesses and vulnerabilities in an enemy government or armed force"[15]. As a rule, conventional forces engage in war symmetrically, because asymmetric threats do not allow them to demonstrate the ability to destroy a relative, invisible enemy.

[1] The original publication of the interview with Frank van Kappen, 26 April 2014, in Russian, is available at http://svoboda.org/content/article/ 25362031.html/, accesed on 30.04.2023 on https://www.svoboda.org/content/article/

In the plus, asymmetric actors choose places like the jungle as their battlefield, the mountains and even the urban environment, where they attack and disappear, diminishing the advantage of the powerful, of the security and military forces of the states. In addition, asymmetric actors use the power of psychology to a cover the material inconveniences against the belligerents strong. In this regard, for example, device attacks improvised explosive devices or suicide bombings heighten the feelings fear of the adversary's military, but also of the population.

Asymmetric threats can be grouped into three broad categories: intelligence operations, weapons of mass destruction and unconventional operations. [16]

- attacks against infrastructures (for example: attacks against computer networks, electronic warfare, physical destruction);
- deception (for example: propaganda operations in the media of public communication, dissemination of false information, etc.);
- psychological operations (for example, taking hostages or distributing pamphlets, broadcasting radio or television shows or using other media to sow fear and discouragement).

Forms such as:

- the use of new tactics and terrain: the use of tactics unorthodox or unconventional terrain (eg urban space) by an asymmetric adversary can facilitate a direct attack on military materiel or operations, maximize the physical and psychological impact of an attack, and complicate possible military or police responses. An armed response in populated areas raises special problems, as the large number of civilians may prevent the attackers from being identified. In addition, a counterattack could further increase the number of civilian casualties;
- civil disobedience: an asymmetric opponent can generate a threats through strikes and riots, demonstrations, the illegal occupation of important points in a locality (communication centers, for example) and the initiation of boycotts in order to destabilize and discredit his opponents or cause them damage.
- This type of unconventional action is increasingly used in failed states (like Somalia) or countries that do not exercise political control over the territory. It should be mentioned that such unconventional actions do not only target the armed forces, but also the civilians in the attack area.
- the use of terror; actions such as intentional targeting a civilian populations in regions far from the main scene a conflict, hostage taking, kidnappings, mutilations, crimes and others criminal activities can lead to the appearance of terror in the heart of the population without the asymmetric attacker exposing himself to high risks.

Hybrid threats are the product of a wide variety of adverse circumstances and existing actions, such as terrorism, migration, piracy, corruption, ethnic conflict and more. Hybrid threats are not exclusively a tool of asymmetrical or non-state actors, but can be applied by state and non-state actors equally. [17]

5. CONCLUSIONS

In conclusion, a state or non-state actor that resorts to hybrid actions can create instability in the internal affairs of another state. Hybrid threats have a direct impact on defense and national security. This is for a number of reasons. First, they are usually generated by non-state actors such as:

- militias, mutant guerrillas, hybrid entities populated by terrorists, fanatics, "patriot bandits" and military deserters;
- orders of dissident generals, seniors of the war, or pure and simple bandits;
- unknown or imperceptible entities, capable of mutations and frightening alliance changes;
- groups with different orientations (religious, ethnic, ideological, political) that ignore international laws and including those that reveal humanitarian respect;
- different illegal organizations living in symbiosis with the economy criminal, in the triangle narcotics - weapons of war - oil. Then, hybrid threats combine, in a relatively random way, conventional and unconventional, symmetric and asymmetric methods and means of action to achieve the objectives established.

"Hybridization" can be found in the entire spectrum of combat actions and profoundly changes the conduct of modern warfare. This makes it very difficult to pinpoint when it started. Additionally, it increases the possibility that an actor using hybrid actions will deal significant damage to their opponent before they can respond or even detect a hybrid attack.

From this point of view, the states that bear the effects of hybrid actions must first of all understand the aggressor's strategy and identify, mitigate and possibly overcome the operational and strategic dilemmas associated with the operational environment.

Given that a "hybrid war" campaign means the conduct and direction of political, conventional, unconventional, asymmetric and cyber warfare, both directly and indirectly, on objectives in all domains and instruments of national power, the aware state that will be affected must prepare countermeasures and effective methods of their implementation.

REFERENCES

[1] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf, accessed on 30.04.2023;
[2] https://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/, accesed on 30.04.2023;
[3] https://www.nato.int/cps/en/natohq/topics_156338.htm, accesed on 30.04.2023;
[4] Ș. Oprea, *Lumea sub efectele acțiunilor hibride*, Monitorul Apărării și securității, 2018, accesed on https://monitorulapararii.ro/lumea-sub-efectele-actiunilor-hibride-1-2520;
[5] http://www.aos.ro/wp-content/anale/R-S-M-Vol-15-Nr1Full.pdf accesat la 10.04.2023;
[6] G. Alexandrescu, *Amenințări la adresa securității*, Editura Universității Naționale de Apărare, București, 2004;
[7] F.G. Hoffman, Conflict in the 21st Century: The rise of Hybrid Wars – Potomac institute For Policy Studies Arlington, Virginia, December, 2007;
[8] K. Ioannou, *Hybrid Warfare: Theory, Case studies and Countermeasures*, University of Pireus, 2022;
[9] Mattis & Hoffman, Future Warefare, The rise of hybrid war, 2005, p. 1-2;
[10] D. Roman, C. Nicolaescu, *Mediul de securitate actual – realități și perspective*, Buletinul Universității Naționale de Apărare „Carol I”, Decembrie 2017, disponibil la https://revista.unap.ro/ index.php/ revista/article/ download/378/355/, accesed on 30.04.2023;
[11] J. Döge, Cyber warfare: Challenges for the applicability of the traditional laws of war regime, Archiv des Völkerrechts 48. 2010. 486;
[12] ***, *Strategia de Securitate Cibernetică a României 2.0 (2021-20126),* pp. 3-5, disponibil la http://sgglegis.gov.ro/legislativ/docs/2021/08/sr2dvm1746zwhc0fby5n.pdf, accesed on 30.04.2023;
[13] C. Mark, *Asymmetrical threats in Cybersecurity*, disponibil la https://cybersecurity.att.com/blogs/ security-essentials/asymmetrical-threats-in-cybersecurity, accesed on 30.04.2023;
[14] T. Poulin, Les guerres asymétriques: conflits d'hier et d'aujourd'hui, terrorisme et nouvelles menaces», http://www.grotius.fr /guerres-asymetriques/;
[15] M. Kolodzie, *Commentary the Asymmetric Threat*, accesed on http://www.almc.army.mil/ alog/issues/JulAug01/MS628.html;
[16] P. Henrichon, *Protéger les forces canadiennes contre les menaces asymétriques*, http://www.journal.forces.gc.ca/vo3/no4/doc/9-14- fra.pdf ;

[17] G. Anghel, *Particularităţi ale conflictelor viitoare. Ameninţările hibride. Război/conflict hibrid*, http://www.mapn.ro/publicatii/1_2011 , pdf;
[18] http://sgglegis.gov.ro/legislativ/docs/2021/08/sr2dvm1746zwhc0fby5n.pdf.