DOI: https://doi.org/10.36719/2663-4619/101/121-125

Azer Haziyev
Wroclaw, Poland
azar.haziyev@gmail.com

HYBRID WARFARE: HOW TO DEFINE AND COUNTER?

Abstract

The main aim of this paper is to analyze hybrid warfare, its characteristics and components, and the challenges that states face in their struggles with it. The paper also proposes several ways to counter hybrid warfare. Throughout the paper, the concept of hybrid warfare is mainly investigated based on the Crimean conflict. In the context of security issues in international relations, the analysis of the hybrid warfare concept carries paramount importance taking into account the increasing attention to it. The investigation of hybrid warfare and its tools can assist the countries to define potential hybrid threats and to design proper strategy to struggle with them.

Keywords: *Hybrid Warfare, Russia, Ukraine, Crimea, war*

Azər Həziyev
Vrotslav, Polşa
azar.haziyev@gmail.com

Hibrid müharibə: necə təyin etmək və ona qarşı necə mübarizə aparmaq?

Xülasə

Bu yazının əsas məqsədi hibrid müharibə, onun xüsusiyyətlərini və komponentlərini və dövlətlərin hibrid müharibələr zamanı qarşılaşdıqları problemləri təhlil etməkdir. Eyni zamanda, məqalə hibrid müharibəyə qarşı mübarizənin bir neçə yolunu təklif edir. Məqalə boyu hibrid müharibə anlayışı əsasən Krım münaqişəsi əsasında araşdırılır. Beynəlxalq münasibətlərdə təhlükəsizlik məsələləri kontekstində hibrid müharibə konsepsiyasının təhlili ona artan diqqəti nəzərə alaraq mühüm əhəmiyyət kəsb edir. Hibrid müharibənin və onun alətlərinin tədqiqi ölkələrə potensial hibrid təhlükələri müəyyən etməyə və onlarla mübarizə üçün düzgün strategiya hazırlamağa kömək edə bilər.

Açar sözlər: *Hybrid Warfare, Rusiya, Ukrayna, Krım, müharibə*

Introduction

What is hybrid warfare?

The term of Hybrid Warfare was in use after the Hezbollah-Israel war in 2006, but became popular after the annexation of the Crimean Peninsula by the Russian Federation in 2014 in political, military, and academic circles. Despite being mainly explained by Russia's actions in Crimea, the hybrid warfare phenomenon had been used from the early 2000s. While the concept grabbed the attention of the large audience, the lack of clarity of the definition remained problematic. Reichborn and Cullen note that the term was being used with reference to different wars by different authors and this can simply show the analytical confusions over the use of hybrid warfare term. While it was used to describe a new type of warfare conducted by non-state actors in the early 2000s, later it referred to the actions of states, particularly Russia in the mid-2010s. Discussions over the topic of whether the hybrid warfare phenomenon is new or not is another sign of the inaccuracy regarding the conceptualization (Reichborn, Cullen, 2016: 1). Although there were many different explanations with regard to it, generally it was being defined as a mixed-use of regular and irregular forces against the enemy in conflicts.

Though there is no unanimously accepted definition of hybrid warfare among analysts, there are generally observed features through which it is possible to formulate a common definition. These

features are difficulty in differentiating between the state of war and peace, blurring warfare modes by simultaneously merging conventional and unconventional, regular and irregular, linear and non-linear, covert and overt methods of conducting war by states and non-state actors, being dynamic, flexible, unpredictable, subversive, complex and multidimensional (Rusnakova, 2017: 346; 3). Referring to these key features, Hoffman described contemporary hybrid threats as following:

"Hybrid threats incorporate a full range of modes of warfare, including conventional capabilities, irregular tactics, and formations, terrorist acts that include indiscriminate violence and coercion, and criminal disorder. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of the conflict" (Baezner, Robin, 2018; Sliwa, Veebel, Lebrun, 2018).

The definition suggested by European Parliamentary Research Service describes hybrid warfare as "…a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat". Another definition of hybrid warfare provided by NATO in the Wales Summit of 2014 consisting of "…wide range of overt and covert military, paramilitary, and civilian measures employed in a highly integrated design" (Rusnakova, 2017: 346)

Although many analysts commented on the topic, there is not a fixed definition to describe hybrid warfare. What is more important on that point is to clearly describe the key components of hybrid warfare to better understand the concept. Therefore, I will be talking about the components of hybrid warfare in the second part (The Ukraine conflict, economicâ"military power balances and economic sanctions, 2016).

Components of hybrid warfare.

The components of hybrid warfare are various and diverge. While discussing the component of hybrid warfare, analysts mainly focus on Russia's hybrid war in Crimea. Research conducted by Caliskan and Cramers shows that approximately half of the authors mention the Russia-Ukraine conflict as a relevant example of hybrid warfare. Other examples such as "Russia's recent activities against the West or NATO" have also close ties with the Russia-Ukraine conflict (Caliskan, Cramers, 2019: 12). The analysis of data indicates that the authors mainly see the Russia-Ukraine conflict as hybrid war. The given case is a unique one that can help us clearly understand the full spectrum of the hybrid war. Therefore, this article also focuses on the Russia-Ukraine conflict and listed the components based on the Crimean case. These components are following:

1. Information warfare
2. Cyber Warfare
3. Psychological operations
4. Intelligence means
5. Proxies
6. Economic tools

Information warfare: is the conflict between two or more groups in the information environment (Porche, Paul, York, Serena, Sollinger, Axelband, Held, 2013: 14). While there is no unanimously accepted definition of information warfare, analysts mainly define it as a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations (Deshpande, 2021). Russia has effectively used information warfare within the broader hybrid warfare perspective during the Crimean conflict as well as during the war in Georgia and East Ukraine. The main goal of information warfare is to influence the internal and external politics of the targeted state.

Cyberwarfare: In comparison with information warfare, cyber warfare has a more technical and specific meaning refers to the attacks aim to disrupt the computer and cyber system of the target. Generally, cyber warfare is referred together with information warfare due to their close relation (Chivvis, 2017: 5). Beyond stealing essential information, the goal of cyber attacks might be to influence and manipulate the population in favor of the attacker (Chivvis, 2017: 3).

Psychological operations: Such operations are conducted to transmit selected ideas and information to the target with the aim to affect the emotions, actions, behavior, policy as well as objective reasoning of the target. The target of psychological operations may vary from individual to certain groups, organizations, and states (Caliskan, Cramers, 2018: 5; Hunter, Pernik, 2015). As an example, throughout the actions in the Crimean Peninsula Russian side spread the myth claiming that the Ukrainian government is based on fascist ideology and it poses an existential threat to the civilian population in Crimea (Rusnakova, 2017: 362).

Intelligence means: Intelligence and special service organs actively participate in hybrid warfare. As a part of the modernization process of the military, Russia additionally strengthened its SOF (Special Operation Forces). These units have been involved in a broad range of activities including directly leaking other states (Chivvis, 2017: 4).

Proxies: are certain groups with sympathy to the side that conducts hybrid warfare and serve its interests. Night Wolves, a club of bikers known as an anti-American and nationalist group can be shown as a good example to the proxies. Generally, this group does not have certain goals, though it is being used to implement different tasks within hybrid warfare (Caliskan, Cramers, 2018: 4).

Economic tools: are also defined as a part of wider hybrid warfare. Davis emphasized that economic warfare (including specific economic sanctions) is intended mainly to influence economic, technology, and military power balances to the advantage of the country/alliance conducting it (Davis, 2016: 170). Blocking bank accounts, imposing restrictions on bilateral and multilateral trade, banning companies, and limiting free movement are examples of economic tools employed during hybrid warfare (Rusnakova, 2017: 350). In the context of the Crimean conflict, energy tools were used as a part of wider economic warfare to change the balance of powers in favor of Russia. By using the energy dependency of many European states, Russia still manages to influence the politics of these states (Caliskan, Cramers, 2018: 4).

Countering hybrid warfare.

After clarifying the meaning of hybrid warfare, as well as its components, the next milestone is to define how to counter hybrid warfare. In this context, it should be emphasized that it is expected to observe the increase of hybrid threats in near future. There are several reasons that lead us to come to this conclusion:

1. The changing balance of powers and competition over the sphere of influence will lead the actors to actively participate in confrontation and defy the current status quo;
2. In the context of rising cooperation among states, the actors of the system will be more vulnerable to hybrid threats as the interdependence among them increases;
3. Futuristic developments in the field of technology will enable more actors to actively involve in the power struggle and compete over the spheres of influence.

Considering the aforementioned factors, we can predict a rising use of hybrid tools in future conflicts. Therefore, defining a proper strategy to counter hybrid threats is quite essential with regard to the changing security environment (Cullen, Wegge, 2019: 17). Monaghan mentions three respective stages of countering hybrid threats. These are as following:

1. Detecting hybrid threats
2. Deterring hybrid threats
3. Responding to hybrid threats.

Detecting hybrid threats is based on two main principles: Firstly, building close cooperation among the bodies within the state. Secondly, cooperating with partners and allies. States can use two methods to detect the hybrid threats. These are the use of special intelligence and analysis of data from technical and physical assets across the state (Monaghan, 2019: 90). Austria has developed a method for detecting hybrid threats which is based on intelligence and data analysis. The Austrian model suggests us to define national vulnerabilities and link them to the capacity and goals of the adversary through hypotheses. The next phase is to produce a plan to counter the threats (Cullen, Wegge, 2019: 28; Robinson, Jones, Janicke, 2015).

Deterring the hybrid threats is considered the most essential stage of countering hybrid warfare. Deterrence of hybrid threats has two ways: Deterrence by denial intends to avoid the capacity of an adversary to conduct hybrid warfare; and, deterrence by punishment intends to convince the adversary that any hybrid attack will bear serious consequences for the side who conducts it (Cullen, Wegge, 2019: 35-36).

The next stage of countering hybrid warfare provided by Monaghan is responding to hybrid threats. In case the adversary continues to pose a threat after deterrence, states may apply to the responding measures in order to counter hybrid threats (Cullen, Wegge, 2019: 51). However, the side which plans to respond to hybrid threats should carefully take into consideration the risk of counterescalation which may further jeopardize its security (Monaghan, 2019: 91; 16).

Conclusion

This paper investigated the phenomenon of hybrid warfare which is popular among political and military analysts especially after the annexation of Crimea. In the first part, I tried to answer the question of "What is hybrid warfare" based on different definitions provided by analysts. The second part assessed the characteristics and components of hybrid warfare. In order to clearly define the components of hybrid warfare, I used the Crimean case study as a complementary supplement. The third part of the paper was dedicated to how to counter hybrid warfare. In this part, the paper analyzed the reasons why it is essential to counter hybrid threats and the possible ways of countering them.

The analysis of hybrid warfare showed that there are still unclear points on what is hybrid warfare and how to counter it. Current political and legal tools to address the issue lacks and this further motivates the adversaries to employ hybrid warfare tools effectively. Therefore, there is still a need to rethink the political and legal sides of the issue to counter actual threats and to define a feasible strategy to respond to them. In this context, multilateral cooperation among the countries is essential to achieve the mentioned goals.

References

1. Reichborn-Kjennerud, Cullen, E.P. (2016). What is Hybrid Warfare? https://core.ac.uk/download/pdf/52131503.pdf
2. Rusnakova, S.N. (2017). Russian New Art of Hybrid Warfare in Ukraine. Slovak Journal of Political Sciences, 17(3-4), pp.343-380. https://doi.org/10.1515/sjps-2017-0014
3. Countering Hybrid Warfare: So What for the Future Joint Force? (2018). https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf
4. Baezner, M., Robin, P. (2018). Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict. https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict
5. Sliwa, Z., Veebel, V., Lebrun, M. (2018). Russian ambitions and hybrid modes of warfare. https://www.baltdefcol.org/files/files/publications/HybridModes.pdf
6. The Ukraine conflict, economicâ"military power balances and economic sanctions. (2016). Taylor & Francis. https://www.tandfonline.com/doi/full/10.1080/14631377.2016.1139301
7. Caliskan, M., Cramers, P.A. (2019). What Do You Mean by "Hybrid Warfare"? A Content Analysis on the Media Coverage of Hybrid Warfare Concept. DIAL.Pr - BOREAL. https://dial.uclouvain.be/pr/boreal/object/boreal:208939
8. Porche, I., Paul, C., York, M., Serena, C., Sollinger, J., Axelband, E., Held, B. (2013). Redefining Information Warfare Boundaries for an Army in a Wireless World. RAND Corporation. Retrieved February 1, 2021, from http://www.jstor.org/stable/10.7249/j.ctt3fh1qp Congressional Research Service, Defense Primer: Information Operations, 2020.
9. Deshpande, V. (2021). Hybrid Warfare: The Changing Character of Conflict. Raj Publication.

10. Chivvis, S. (2017). Understanding Russian "Hybrid Warfare": And What Can Be Done About It. https://www.rand.org/pubs/testimonies/CT468.html.
11. Hunter, E., Pernik, P. (2015). The Challenges of Hybrid Warfare. https://icds.ee/wp-content/uploads/2013/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf
12. Davis, C.M. (2016). The Ukraine conflict, economic–military power balances and economic sanctions. Post-Communist Economies, 28(2), pp.167-198. https://doi.org/10.1080/14631377.2016.1139301
13. Cullen, P., Wegge, N. (2019). MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf
14. Robinson, M., Jones, K., Janicke, H. (2015). Cyber Warfare: Issues and Challenges, www.researchgate.net. https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges
15. Monaghan, A. (2016). Putins Way of War. Www.Academia.Edu. https://www.academia.edu/24314231/Putins_Way_of_War
16. What Do You Mean by “Hybrid Warfare”? A Content Analysis on the Media Coverage of Hybrid Warfare Concept. (2018). https://www.researchgate.net/publication/329782285_What_Do_You_Mean_by_Hybrid_Warfare_A_Content_Analysis_on_the_Media_Coverage_of_Hybrid_Warfare_Concept

Received: 05.02.2024 Accepted: 25.04.2024