

HYBRID WAR - THEORY AND PRACTICE

Hatidža Beriša, PhD¹

School of Engineering Management, Belgrade, Serbia

Katarina Jonev Ćiraković, MSc²

Anti-Human Trafficking IBSSA, Belgrade, Serbia

Aleksandar Ćiraković³

Abstract: Academic and military circles of the most powerful countries in the world have considered certain concepts of modern warfare, primarily taking into account their own goals and available capabilities. In that way, a theoretical basis was set for the coordination of all available military and non-military capacities, improvement of existing and development of missing capacities and elaboration of optimal methods of their application depending on defined goals, environmental conditions and opponents.

The aim of this paper is to present the concept, principles and forms of application of hybrid warfare and, at the same time, to emphasize the importance of coordinated use of all available capacities, military and non-military, in order to achieve or protect one's own interests. The modern strategic and security environment is very complex and requires the elaboration of concepts, methods and capacities that are applicable in the present and the near future. The traditional approach, which was characterized exclusively by the use of military means, today has limited use value.

Keywords: military forces, concept, warfare, hybrid, hybrid warfare

INTRODUCTION

Numerous conflicts have marked the history of human civilization. Conflicts were waged for various reasons, but with the same general goal of realizing one's own interests, imposing one's own will on the enemy, and preventing the enemy from achieving their own goals. According to the traditional understanding, "war is a conflict of states, military-political alliances, classes, nations or other social groups, in which violence is massive and organized and armed struggle is waged in all areas of social life, in order to achieve certain political, economic and other goals (Vojni leksikon, 1981:508).



Contrary to this traditional understanding of warfare, states have historically used other forms of warfare to achieve their own goals. In that respect, it is primarily understood as economic, psychological-propaganda, political, and with the transition to the new millennium, information and cyber warfare became more important. Such development makes it difficult, and perhaps impossible, to make a clear distinction between the period of war and peace, and at the same time makes it difficult to recognize the threat in a timely manner and to take appropriate preventive or defensive measures.

Given that hybrid action is most often manifested by non-military forms of security threats, which are difficult to detect in time and prevent surprise, the question arises of ways and possibilities in counteracting such destructive action. How to effectively oppose something that is covert, adaptable, comprehensive, has a synergistic effect, and there is still no approximate harmonization, which complicates the normative regulation of the threat and the legal prescribing of countermeasures.

Domestic authors relied on the views and conclusions of both authors from the West and authors from the Russian Federation when considering the subject terms. At the same time, they based their conclusions on their own experiences and events in the former SFRY, which were largely marked by the active engagement of various global and regional powers and the capacities and activities available to them.

According to domestic authors, at the core of the interpretation of hybrid war is the conflict of classical war theory with emerging theories that seek to describe and explain current conflicts. The results of the process of globalization and the general development of human civilization led to the development of postmodernist theories of warfare, which tried to explain a phenomenon that classical theories of warfare could not. Thus, modern theories have significantly changed the logic in understanding war as a social phenomenon, especially since the end of the Cold War. The basic understanding of modern theories of warfare implies that the goal is “to defeat the enemy without a battle” and that war exists even without armed struggle (Mitrović, Nikolić, 2020: 130).

THE CONCEPT OF HYBRID WARFARE

There is no single and generally accepted definition of hybrid threat or hybrid warfare in the world. The definition should determine the content of the term, concretize the content of the hybrid threat as a phenomenon, i.e. its properties, distinguish it from other phenomena. The question is how to effectively counter a threat that is not clearly and unambiguously defined. A similar problem in terms of conceptual definition exists with terrorism, where the definition of terrorism has been influenced by the historical context of terrorism, because by changing the context of this violent activity, the definition has also changed.

The concept of hybrid warfare is relatively new; it appeared at the beginning of the new millennium in the works of military theorists from the USA. At the time of the concept's development, hybrid warfare was just another in a series of concepts that advocated the thesis that modern warfare deviates significantly from the traditional understanding of war. Frank Hoffman, as one of the greatest proponents of this concept, states that “hybrid wars include various forms of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including random violence and coercion, and crime-induced disorder.” (Hoffman, 2007: 14)

Like the notion of hybrid warfare, the notion of hybrid threat is considered from a different point of view. There is no generally accepted definition of a hybrid threat, and it remains a challenge for various



researchers and theorists. One of the appropriate definitions is: “hybrid threats are potential, complex and multidimensional dangers created by the simultaneous action of state and / or non-state entities that adaptively combine conventional means to achieve common goals.” (Saković, Stojković, 2019: 307-308).

According to the Hoffman, hybrid wars can be waged by states, but also by various non-state actors. The introduction and consideration of the new concept were based on assessments of the future environment, which was presented as complex, and posed new challenges to the armed forces. It was thought that future conflicts would be waged in the urban areas of developing countries, with opponents using different asymmetric capabilities in order to prolong the duration of the conflict and waste resources and undermine the will to fight. (Hoffman, 2007: 15)

It should be borne in mind that the basic assumptions of the concept of hybrid warfare are based on the experiences of the armed forces of the United States and the State of Israel during the war in Iraq, starting in 2003, and the war in Lebanon in 2006. That is why it was pointed out that potential enemies will try to overcome the supremacy of the USA in firepower and intelligence capabilities by applying irregular methods. Potential enemies will not abide by any rules, they will learn from the regular armed forces and will apply modern technology in unique and unexpected ways (Hoffman, 2007: 16) At the same time, it was assumed that potential enemies would largely apply various forms of criminal activities, but also actively engage in the information dimension through social networks for the purpose of psychological propaganda.

In accordance with the stated assessments and conclusions, the notion of a hybrid threat has been defined in the USA. A hybrid threat is a diverse and dynamic combination of regular forces, irregular forces and / or criminal elements united in achieving mutually beneficial effects (TC 7-100, 2010: 2). They are innovative, adaptive, globally connected, networked and hidden in the mass of the local population.

According to the doctrinal documents of the US Armed Forces, the intention of the hybrid threats is to saturate the entire operational environment with effects that support the achievement of its own goals. By acting simultaneously, it is possible to achieve economic instability, undermine trust in local authorities, attack information networks, send propaganda messages, cause technical-technological accidents and physically endanger opponents. Synchronized and synergistic activities of hybrid threats can be manifested in the informational, social, political, infrastructural, economic and military dimensions of the operational environment. (TC 7-100, 2010: 1, 2)

An integral element of hybrid threats are criminal groups that are used in cooperation with regular and irregular forces. Criminal groups have the ability to provide the necessary sources of funding for certain actions and activities, as well as the procurement of weapons and military equipment illegally. In that way, hybrid threats are enabled to master modern technologies, which increases the space in which they can pursue their actions and activities.

For success in hybrid warfare, it is not necessary to achieve any tactical success or victory, but it is necessary not to lose the war (TC 7-100, 2010: 1-2). It is necessary to achieve a stalemate in the political and military sense, and thus disrupt the support of the electorate in order to change the behavior or policy of the United States. Examples of US actions during the occupations of Iraq and Afghanistan are adequate indicators of such doctrinal commitments.

From all of the above, it is obvious that the experiences of the United States, and mainly the experiences gained during the use of their armed forces in the late 1990s and during the first decade of the new millennium, significantly shaped these attitudes. Operation ‘Iraqi Freedom’ and the war in Lebanon in 2006 largely demonstrated the inefficiency of conventional armed forces in a conflict with an adapt-



able (hybrid) adversary capable of independently combining and synchronizing the use of available capabilities in different dimensions.

One of the definitions in its study on combating hybrid warfare was given by the international organization “Multinational Capability Development Campaign (MCDC)”, which defines it as the synchronized use of several different instruments of power that are directed (tailored - designed) to specific - specific vulnerabilities. spectrum of social life and achieve a synergistic effect. Hybrid threats are designed to address the weaknesses (MCDC Countering Hybrid Warfare, 2017) of states in the political, military, economic, social, infrastructural, and information domains.

Panarin also gives a new approach, according to which hybrid war is a set of methods of military, political-diplomatic, financial-economic, information-psychological and information-technical pressure, as well as technology of colored revolutions, terrorism and extremism, activities of special services, formation of special forces, a force for special operations and a structure of public diplomacy, which, according to a single plan, is implemented by state bodies, the military - political bloc or transnational corporations. (Panarin, 2019: 57)

The evolution of the concept (example of Ukraine)

The crucial geopolitical event that drew the attention of the professional public to the concept of hybrid warfare was the crisis in Ukraine in 2014 and the active engagement of the Russian Federation. This event also contributed to the evolution of the concept of hybrid warfare, and it is necessary to consider to some extent the conditions that led to it.

After the violent removal of the legitimately elected president of Ukraine, which was crucially contributed by the United States and the European Union, the Russian Federation used its own armed forces to occupy all important facilities on the Crimean peninsula, after which a referendum was organized on unification of Crimea with the Russian Federation. Based on the results of the referendum, Crimea was annexed to the Russian Federation. This development was a complete strategic surprise, primarily for the United States, because the Russian Federation showed an unexpected level of determination in protecting its own vital interests in the immediate neighborhood. Not only was the action of the Russian Federation characterized by determination, but also a high level of synchronization of the application of available instruments of power was demonstrated in order to achieve the set goals.

As already stated, the traditional interpretation implies that war is characterized by armed struggle, i.e. that there is a clear distinction between the period of peace and war. However, experiences in the USSR during and after the Cold War, events in the SFRY and experiences from the Middle East and North Africa in the conditions of the “Arab Spring” showed that modern war, in its forms and contents, significantly deviates from traditional interpretation. With this in mind, General Gerasimov states that “a perfectly stable state can, within a few months, or even days, become the scene of a fierce armed conflict, a victim of foreign intervention and sink into a net of chaos, humanitarian catastrophe and civil war” (Vasilyevich, 2013 : 2-3).

At the same time, he states that “the role of non-military means in achieving political and strategic goals has increased, which, in many cases, exceed the strength of weapons in terms of their effectiveness.” (Vasilyevich, 2013: 2-3). Considering experiences from different regions of the world, examples of unilateral and reckless behavior of the United States in the form of “humanitarian” interventions and preventive attacks on other countries without the consent of the United Nations Security Council,



as well as numerous “colored” revolutions in space of the former USSR, General Gerasimov concluded that success in modern wars could no longer be based solely on the use of armed forces. In order to achieve the desired goals, it is necessary to apply various non-military measures in coordination with the military forces.

Taking into account the events in Ukraine during the first half of 2014, but also the views of General Gerasimov presented in the mentioned article, academic and military circles in the West concluded that the Russian Federation is waging a hybrid war against Ukraine. Based on such conclusions, there was an evolution of the initial concept of hybrid warfare, but also the appearance of numerous papers that discussed current topics. The report from the Munich Security Conference in 2015 states a model that comprehensively presents a new interpretation of the concept of hybrid warfare, i.e. that hybrid warfare includes a combination of different conventional and unconventional means of warfare, such as diplomacy, economic warfare, information warfare and propaganda, cyber attacks, regular military forces, special forces, irregular forces and support for local unrest.

Taking into account the new interpretation of the term, the Western expert public tried to define certain principles or characteristics of hybrid warfare. Based on the study of events, primarily in Ukraine, the following characteristics of hybrid warfare have been defined (Hybrid Conflicts as an Emerging Security Challenge, 2015):

- Coordinated application of means - within hybrid warfare, various actions and activities are performed simultaneously, which implies the necessity of their coordination in order to achieve the desired effect. The actions and activities performed can be of different levels, from strategic to tactical, and the party that implements them tends to use conventional and unconventional means to achieve its goals.
- Ambiguity - hybrid warfare is usually amorphous and ambiguous, i.e. it includes state and non-state actors and the use of irregular and unconventional forces. Deception and propaganda are characterized by hybrid warfare, which makes it difficult to distinguish peace and war.
- Continuous adaptation - the actors of hybrid warfare constantly adjust their own actions in order to achieve the desired effects. There are no specific rules, patterns or boundaries that can lead to a long-lasting conflict whose intensity and content change over time. The ideal goal is to achieve victory without a fight.
- Lack of rules as a principle - actions and activities are not carried out in accordance with the rules of use of force or the principles of international humanitarian law. Extreme violence can be used for propaganda purposes with the aim of intimidating the opponent or leading the opponent to reckless action.
- Constant technological change - the development of new technologies, such as social networks and the ability to gather intelligence from open sources has led to the evolution of hybrid warfare. It can be expected that future technological advances will also lead to changes in certain characteristics of hybrid warfare.

APPLICATION OF HYBRID WARFARE (EXAMPLES OF SYRIA AND UKRAINE)

A clear recognition of security challenges and threats cannot be expected in the future. Traditional conflicts will continue to be the most dangerous form of social conflict in the future, but future oppo-



nents will most likely combine different ways and forms of warfare. The most significant change in the character of modern warfare is reflected in the unclear nature of the struggle of the opposing sides.

Hybrid warfare combines the lethality of interstate conflicts with the fanaticism and longevity of “irregular warfare”⁴ In such conflicts, non-state actors use access to modern military capabilities, such as encrypted communication systems, portable anti-aircraft missile systems, etc., and use ambushes, improvised explosive devices and liquidations with the long-term use of insurgent actions. Technologically advanced state actors could combine the use of anti-satellite weapons with terrorism and cyber attacks aimed at financial institutions.

The successful implementation of hybrid warfare requires the existence of certain conditions, such as: long-term intolerance, existing or perceived social inequality, general social distrust, weak state institutions or ethnic tensions. If a state wants to use hybrid warfare, it will usually encourage local unrest in the initial phase in order to provoke a reaction from state or local authorities. (Rančić, Beriša, 2018) He will then strive for the internationalization of the problem and the application of various forms of diplomatic and economic pressure. It will most often strive to achieve goals without armed conflict, but armed conflict is the ultimate means of achieving a goal.

For the purposes of this paper, general examples of the application of the content of hybrid warfare will be considered, focusing on the examples of Syria and Ukraine. The contents of hybrid warfare will be grouped according to the connection of their application.

Diplomacy and economic warfare

Economy is one of the basic pillars of every country, i.e. developed economy is the main prerequisite for the development of other national interests, such as: good living standards, meeting the living needs of the population, building and maintaining credible military power, technological development, improving the education and health system, political and economic influence in the region or in the international community and the like.

Diplomacy and forms of economic warfare (economic sanctions, customs, embargoes, fiscal and monetary policy, etc.) belong to the traditional forms of international political and economic relations. Since their inception, states have, depending on their capabilities, applied various forms of diplomatic pressure to achieve political goals. At the same time, various forms of economic warfare sought to develop their own and weaken the opponent's economy. As such, they cannot be independently considered as a special content of hybrid warfare, because in that way it could be concluded that numerous actors in international relations are constantly in some kind of hybrid warfare. The basic goal of the economic war is to realize the interests of the state that started that war, but without the use of armed struggle. The intensity and duration of the use of such economic instruments can crucially affect the ability of the attacked state to resist potential armed aggression. Diplomatic pressures and economic warfare are primarily applied in order to support other contents of hybrid warfare in order to achieve a synergistic effect. Given that these are traditional forms of international relations, in this paper they will not be discussed in more detail.

4 Irregular warfare is defined in US doctrinal documents as “a violent struggle between state and non-state actors for legitimacy and influence over a certain population.”



Support for local unrest

Support for local unrest is an important content of the hybrid war, because it enables easy identification of threats, but also identification of actors interested in a possible escalation of the crisis. Most often, Western countries, led by the United States, provide support for local riots. The United States provided the necessary organizational, financial and media support to numerous “colored” revolutions in the former USSR and the former SFRY, riots in the countries affected by the “Arab Spring”, and in recent years riots in South America, Venezuela and Bolivia. Organizational assistance was reflected in the formation and organization of various democratic movements and non-governmental organizations in countries that were subject to local unrest. Some members of these organizations and movements have been trained in Western countries to express forms of civil disobedience, to organize protests, but also to escalate unrest in case of need. Financial assistance was reflected in the allocation of significant financial resources from various funds intended for the spread of democracy. In this way, primarily the United States, but also some other Western countries, in a number of cases, managed to achieve their own goals and lead to a change of government. At the time of writing, the same method is used in Hong Kong.

On the other hand, the Russian Federation has been passive in this segment for a long time. With the escalation of the crisis in Ukraine, the Russian Federation has also started providing support for local riots in the Donbas area. In the political dimension, the demands of the Russian population on the territory of Donbas were supported, in the media dimension, propaganda activities were carried out with the aim of damaging the reputation and legitimacy of the Ukrainian state authorities. At the same time, the departure of the citizens of the Russian Federation to the area of Donbas to participate in the conflict was not prevented.

Information warfare and propaganda and cyber attacks

Information warfare and propaganda are interrelated and have been used for a long time with the aim of discrediting and damaging the reputation of the opponent, or his authorities, violating the will to fight or resist the opponent, deceiving and influencing the opponent to make wrong or inappropriate decisions and the like. Information is distributed through television, websites and social networks, and sometimes with the use of leaflets. Quantity, not quality, is crucial to the success of information warfare. If the same information from several different sources is distributed to the target groups within the information environment, it is expected that the target groups will accept such information as credible. Based on that, it can be concluded that the synchronization of information warfare and propaganda actions is very important. The necessary level of synchronization can be achieved primarily by state actors, because they have control over various media houses such as CNN, BBC, Fox News, Russia Today and the like. Special topics and messages are formed that are constantly repeated with the aim of their acceptance by the target groups. One of such topics is the notion of “Novorossiysk”, i.e. the area of eastern and southeastern Ukraine, which was pointed out by the President of the Russian Federation in his presentation in 2014. This topic was used to unite different local groups in the Donbas area within one common political goal. (Kofman, 2017: 52).

An example of information and propaganda activities is the issue of weapons of mass destruction in Iraq and Syria. In the context of Iraq, the mentioned topic was used as an occasion for aggression and occupation of Iraq by the USA and the “coalition of the willing”, but in the absence of evidence after the US aggression, their international credibility was damaged. Also, information on the use of chem-



ical weapons by regular Syrian forces against the rebels has been presented on several occasions, all in the context of creating a favorable international environment for potential military intervention by the United States and NATO in Syria. (<https://news.un.org/en/story/2020/04/1061402>)

Information and propaganda activities, since they represent a non-contact form of conflict, are applied continuously. To a large extent, information and propaganda activities are carried out with the aim of supporting the achievement of political goals and interests, and if necessary, the provision of wider international support for military intervention. Although the concept of hybrid warfare and hybrid threats was not discussed in 1999, the “Racak” case, with exceptional media support and information activities, was used by the United States as an occasion for military intervention in the territory of FR Yugoslavia.

Cyber attacks are a relatively modern means of warfare, enabling effective action on certain parts or objects of critical infrastructure or financial institutions. It is very difficult to prove the source of cyber attacks, and certain state actors are usually accused of certain cyber attacks based on assumptions. There is a well-known case of the application of the computer “worm” Stuxnet, which caused mechanical damage to over 1000 centrifuges used in the Iranian uranium enrichment program, and which is presumed to be a product of the USA and Israel. On the other hand, the Russian Federation was accused of several weeks of cyber attacks on Estonia in 2007, in response to the relocation of the monument to Soviet soldiers from the center of Tallinn to a nearby military cemetery (Ottis, 2018: 1). Within the crisis in Ukraine, cyber attacks were recorded in several cases on government websites using the so-called DDoS (Distributed Denial of Service) attacks. In October 2014, the electronic system for recording the election results of the Ukrainian Parliament was disabled, for which a hacker group called CyberBerkut took responsibility (Ottis, 2018: 1).

Regular military forces, special forces and irregular forces

These contents are closely connected, which is why their joint consideration is necessary. In the context of hybrid warfare, irregular (paramilitary, insurgent or terrorist forces) are particularly significant. In most cases, they are primarily used to achieve the desired goals. Depending on the state actors who support them, they can be engaged against the security forces or in cooperation with the security forces. They usually consist of the local population, but in certain cases they can also be composed of foreign nationals. These are usually easily equipped forces, and in a smaller number of cases they have armored and artillery means. They usually carry out insurgent actions or use guerrilla forms of warfare and are not able to perform complex operations with joint tactical formations. With regular material support from abroad, they exhaust regular military and security forces through long-term warfare, constantly inflicting losses on them and undermining the will to fight.

Special forces are usually applied in parallel with irregular forces. They are engaged in the tasks of: gathering intelligence; artillery-missile, air and ship fire; training of local military and irregular forces, and in certain cases being directly involved in combat operations. They are very suitable for performing tasks in low-intensity conflicts, and are therefore most often engaged. Since they are essentially light forces and do not have heavy means of war equipment at their disposal, it is also difficult to identify them on the battlefield.

Regular military forces are very rarely engaged in hybrid warfare. They can be engaged in cases of providing limited military support to local security forces or irregular forces, but also in cases where other contents of hybrid warfare have not led to the achievement of the goal and it is necessary to engage the



armed forces in the conventional sense. Experience to date has shown that regular military forces were used in a conventional sense to a limited extent, i.e. to the extent necessary to achieve the set goals.

Taking into account all the above, the conflicts in Syria and Ukraine are taken as examples of the use of all these forces. It is also important that the examples of the current conflicts in Libya, Yemen and Afghanistan, as well as the crisis in Venezuela and Bolivia, can also look at the ways in which all these forces are used by various actors.

All these forces are represented in Syria. Within the irregular forces on the side of the security forces there are various local militias, Shiite militias from Iraq, Iran and Afghanistan supported by Iran, as well as Hezbollah. On the rebel side there are various rebel, extremist and terrorist forces backed by the US, Turkey and certain Sunni monarchies from the Persian Gulf, as well as Kurdish forces openly backed by the US and the EU. Also, for several years, the forces of the so-called Islamic states, which as a terrorist group had no official support, although in economic terms (crude oil trade) cooperated with Turkey and part of the Sunni monarchies in the Persian Gulf. The special forces were engaged by the United States, the Russian Federation, France and Turkey within the tasks already mentioned, and in cooperation with the forces and movements they supported. Regular military forces were engaged by the United States, the Russian Federation and Turkey, but to a limited extent and heavily in order to support the actions of local forces of operational and strategic importance.

In Ukraine, the mentioned forces were used in a somewhat different form in relation to Syria. On the Ukrainian side, numerous paramilitary forces were used, formed by extremist and right-wing organizations, which were financially supported by certain Ukrainian tycoons. Paramilitary forces were heavily used in combat operations because the morale of the regular armed forces was very low (Cvetković, Kovač, Joksimović: 2019: 329). On the other hand, the rebel forces in Donbas were formed by the local population, but also by a certain number of volunteers from the Russian Federation and other Orthodox countries. The Ukrainian armed forces as a whole have been used in a conventional sense, but rather unsuccessfully as a result of years of neglect, high levels of corruption and very low morale. Several Ukrainian and Western sources have stated that members of the Russian armed forces, and even entire units, are taking part in the fighting on the side of the rebels, but there is no evidence to confirm such allegations. Taking into account the course of combat operations, it can be assumed that certain members of the Russian armed forces were engaged in advisory or command roles, but also in gathering intelligence. The conflict in Ukraine can primarily be characterized as a civil war, because there was no open, or proven, participation of foreign armed forces on either side.

CONCLUSION

Under the cloak of good diplomatic relations, respect for international legal norms, advocacy for peace and good cooperation, there will always be parallel relations permeated with conflicts, tensions, and pressures with the aim of realizing one's own interests. Many sovereign subjects seek, to a greater or lesser extent (depending on the power they possess), to undermine the power of their rivals, even according to official policy and "friendly" countries, thus striving to pursue their interests, even if they violate moral norms.

The hybrid aspect of the term means a combination of previously defined forms of warfare, conventional, irregular, political or informational. The combination of different means in different dimensions of warfare is not new, but originates from the very beginnings of warfare.



From the point of view of the Russian Federation, the approach to warfare, which includes various forms of projection of power, is not new, nor is it a reflection of a new strategy. First of all, this approach shows that, in the Russian Federation, it is correctly understood how modern wars are fought, regardless of who participates in them. Modern wars, in the simplest sense, are fought with the combined application of various instruments of national power. The West, and primarily the United States, has long adhered to this approach, which in the times in which we live is popularly called “smart power”. The concept of hybrid warfare is thoroughly elaborated in contemporary Western military thought, but the problems to which hybrid warfare needs to be answered are not new, but the answers were previously given in the context of considering unconventional and political warfare.

The hybrid war has become a catchphrase describing the use of the instruments of national power of the Russian Federation in the conflict in Ukraine, but it can be concluded that the Western academic and military professional public has been seduced by this term. In an attempt to correct the neglect of the Russian Federation over a long period of time, the West has tried to encompass all the activities of the Russian Federation in one term. Existing tensions over Ukraine, which have led to drastic mistrust between the Russian Federation and its neighbors, condition the perception of fear that the Russian Federation will intervene again in the immediate neighborhood. The crisis in Ukraine is not the first example in which the Russian Federation has demonstrated its determination and ability to apply the instruments of national power in the former USSR. It is necessary to know the capacities of the Russian Federation for the application of the instruments of national power, but it is unlikely that the Russian Federation would apply the approach like the one used in Ukraine once again. The application of the instruments of national power of the Russian Federation in Ukraine must be viewed in terms of intervention in a neighboring state which it considers to endanger Russia's vital national interests. This approach to action is certainly very well known to the United States, given that it has taken such an approach to a number of countries throughout its history.

Future conflicts will not be easily categorized as conventional or unconventional. The nature of the conflict is more complex, because it is difficult to recognize all potential threats, coming from state or non-state actors, but we must not assume that interstate conflicts have gone into oblivion. Interstate conflicts are unlikely, but it is necessary to understand that interstate conflicts do not have to be exclusively conventional or armed conflicts. Different capacities or contents that can be used for the purpose of warfare are available to an increasing number of actors, but also an increasing number of actors show the ability to coordinate the application of different capacities and abilities in order to achieve their own goals.

REFERENCES

1. Beriša Hatidža, Ivan Rančić: Hibridno ratovanje, Vojno delo br 3, Beograd, 2018,
2. Vojni leksikon, Vojnoizdavački zavod, Beograd, 1981.
3. ГЕРАСИМОВ, Валерий Васильевич, Ценност науки в предвидении, Военно-промышленный курьер, 2013, http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.
4. GALEOTTI, Mark, The ‘Gerasimov Doctrine’ and Russian Non-Linear War, Blog: In Moscow's Shadows, 2014, <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>.



5. GAO 2010 Analysis of DoD Military Concept & Briefing Documents & Academic Writings, <https://www.gao.gov/new.items/d101036r.pdf>.
6. Hybrid Conflicts as an Emerging Security Challenge: Policy Considerations for International Security, PfPC Emerging Security Challenges Working Group Policy Paper No.3, јануар 2015, <https://www.pfp-consortium.org/index.php/pfpc-products/policy-papers/item/95-hybrid-conflicts-as-emerging-security-challenge-policy-considerations-for-international-security>.
7. Panarin I.N, Hybrid War: Theory and Practice, Club of Generals and Admirals of Serbia and Association *Milutin Milanković*, Belgrade 2019
8. Milenković M. and Mitrović M., Colored revolutions in the paradigm of hybrid war, *Vojno delo* 6/2019, Belgrade 2019, p. 248 - 263.
9. Mitrović M, Nikolić N: Hybrid war - contribution to defining the concept, content and model of action, Institute for Strategic Research and Media Center *Defense* (in press), Belgrade, 2020
10. MCDC Countering Hybrid Warfare Project, Understanding Hybrid Warfare, January 2017
11. Saković R, Stojković D: Development of the defense system of Republic of Serbia in the conditions of hybrid threats, *Vojno delo* 7/2019, p. 307-308.
12. Cvetković, N, Kovač, M, Joksimović, B : The concept of hybrid war, *Vojno delo*, 7/2019, Belgrade
13. HOFFMAN, Frank G., Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, 2007, http://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
14. HOFFMAN, Frank G., Hybrid Warfare and Challenges, Joint Force Quarterly, Issue 52, 1st Quarter 2009, <http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf>.
15. KOFMAN, Michael et al, Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, САД, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1498/RAND_RR1498.pdf.
16. Munich Security Report 2015, Munich Security Conference, 2015, https://securityconference.org/assets/02_Dokumente/01_Publikationen/MunichSecurityReport_2015.pdf.
17. OTTIS, Rain, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Cooperative Cyber Defence Centre of Excellence, Естонија, 2018, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.
18. THORNTON, Rod, The Changing Nature of Modern Warfare: Responding to Russian Information Warfare, The RUSI Journal, Vol: 160 No: 4, 2015, <http://koziej.pl/wp-content/uploads/2015/09/Responding-to-Russian-informationwarfare.pdf>.
19. TC 7-100, *Hybrid Threat*, Department of the US Army, 2010, https://www.benning.army.mil/mssp/security%20topics/Potential%20Adversaries/content/pdf/tc7_100.pdf.



