

A Strategic Means of Hybrid Warfare

Milica Ćurčić, Slavko Dimović, Ivan Lazović

Abstract—The modern security environment is undergoing a profound transformation. This transformation has been shaped by the emergence of new patterns of conflict and cooperation among state and non-state actors as well as the spread of globalization and new technologies. Also, the development of a new breed occurred, characterized by a combination of warfare methods and usage of different means of warfare. In the constellation of new wars, a hybrid wars stand out as a war that combines different strategies of warfare to achieve synergistic effects. The aim of the article is to analyze and describe characteristic of both non-state and state hybrid warfare, as well as the key elements that constitute strategic means of hybrid warfare. The usage of information weapons, cyber sphere and psychological means, in combination with conventional weapons of war, become main features of modern conflict. Modern technologies are the main factor that influenced and transformed warfare and their usage permeates every activity in hybrid war.

Index Terms — Hybrid warfare, war, means of warfare, security, strategy, new technologies

I. INTRODUCTION

Clausewitz's observation that war is "a merely continuation of policy by other means" [1] has become an incontestable maxim among security experts. During history, war occurred among centralized, hierarchically ordered, territorialized states in which big armies confronted each other on the battlefield, using similar strategies, tactics, and weapons. The war is still present in international relations, but with different forms and characteristics.

The nature of warfare is changing and as Williams noticed, there are three issues important to discuss: how useful is the concept of 'total war' for thinking about developments in warfare? What is the relationship between war and globalization; specifically, has globalization given rise to a 'new' type of warfare? What changes can be identified in the way advanced industrialized democracies in the West are waging war today compared to earlier historical periods? [2]

The post-cold war period is characterized by the emergence of non-state actors, new threats that are combined with globalization factors and the usage of sophisticated technology. In order to find a new analytical framework for

Milica Ćurčić – Department of Physical Chemistry, "Vinca" Institute of Nuclear Sciences - National Institute of Republic of Serbia, University of Belgrade, Belgrade, Serbia (e-mail: milica.curcic@vin.bg.ac.rs).

Slavko Dimović – Department of Radiation and Environmental Protection "Vinca" Institute of Nuclear Sciences - National Institute of Republic of Serbia, University of Belgrade, Belgrade, Serbia (e-mail: sdimovic@vin.bg.ac.rs).

Ivan Lazović – "Vinca" Institute of Nuclear Sciences - National Institute of Republic of Serbia, University of Belgrade, Belgrade, Serbia (e-mail: ivan.lazovic@vin.bg.ac.rs).

understanding the nature of modern wars, new paradigms had been constructed. Those concepts are seeking to understand an ambiguous border between war and peace because from the perspective of modern wars, wartime, peacetime and crisis do not exist as separate phases [3]. In a more practical way, the main dilemma arises from questions of how it is possible for a weaker actor to win a war against a significantly stronger and more powerful enemy and how a stronger actor should oppose to a weaker one in an asymmetric conflict.

One of the basic characteristics of modern wars is the use of new means of warfare that avoid predictability and linear military operations. Technological progress has conditioned changes in all spheres of life, including conflict, wars and military operations. The new technologies allow the possibility to achieve strategic goals by unconventional and cognitive effects (technologies of social influence and manipulation, cyber sphere, information weapon, possibilities of significant damage of control system of a state) [4]. Those technologies appear to be increasingly adaptive and sophisticated, able to outpace state-based militaries in the dialectic and competitive learning cycle inherent to wars [5]. Technological advancements have furthered weapons and platform development, but also introduced new capabilities and vulnerabilities in the security arena, that additionally increase the complexities of contemporary conflicts.

II. HYBRID WAR AS A NEW FORM OF WARFARE

The security architecture of the modern world focuses on threats such as terrorism and radicalization, nonproliferation of WMD, securitization of migration, cyber and ecological threats etc. Most of these threats are dominantly posed by different non-state actors. Also security agendas introduce new types of wars that cannot be defined as conventional, traditional or classical wars. In order to clarify the different types of war in a contemporary security environment, as well as their basic characteristics, a number of scholars have attempted to define new types of war. In the literature we can find terms Unconventional war [6-8], Irregular war [5, 9], Fourth Generation of War [10-11], Unrestricted War [12] Compound War [13] and Asymmetric War [14-16]. All this approaches of modern war in different ways are pointing at the blurring of subjects, objects and dynamics in contemporary conflicts.

The following variables are most commonly used to determine the characteristics of modern wars: the main protagonists and units of analysis of war - states or non-state actors; the primary motives of actors (ideology, territorial secession, religion etc.); the spatial ranges: interstate, regional, or global; the technological means of violence – weapons and strategies of war; the social, material, and human impact of conflict, including patterns of human victimization and forced

human displacement; the influence of the political, economic and social structure on conflict [17].

The „hybrid war” emerged as the newest kind of war during the first decade of the 21st century by key scholars who focused on “the blending or blurring character of conflict” [18]. This term was first used in 2006 to describe the strategy that Hezbollah used in the Lebanon war. Mixing an organized political movement with decentralized armed cells employing adaptive tactics in ungoverned zones, Hezbollah affirms an emerging trend. Highly disciplined, well-trained, distributed cells can contest modern conventional forces with an admixture of guerrilla tactics and technology in densely packed urban centers [19]. In this conflict Hezbollah conducted several technological surprises on Israeli forces. Hezbollah’s fighters bypassed the complex surveillance system used by Israel to monitor its border with Lebanon led to the kidnapping of two Israeli soldiers and the killing of eight. The firing of a Noor anti-ship cruise missile (an Iranian version of the Chinese C-802) resulted in the loss of four Israeli sailors and the crippling of an Israeli missile ship. Two Merkava IV tanks were destroyed and their crews killed or wounded, probably by a combination of Raad anti-tank missiles (the Iranian version of the Russian Sagger AT-3) and advanced improvised explosive devices (IEDs) [20].

This case demonstrated the ability of a non-state actor to deconstruct the vulnerability of not only a powerful state, but Western-style militaries [21]. The increased number of actors, who innovatively combine different models of war, capacities and weapons in order to achieve strategic goals, has created fertile ground for the introduction of concept which explains characteristics of modern warfare. In that manner, hybrid war is becoming the dominant discourse in discussions of modern warfare as well as accepted and promoted by politicians, military experts and theorists as the basic concept of modern military strategies [22].

The term ‘hybrid warfare’ was introduced in theory by Frank Hoffman, a former US Marine officer, to influence on ingrained and outdated beliefs in the US military about the utility of military force in the post-Cold War environment. In Hoffman’s view, hybrid warfare was a suitable analytical construct to explain the success of a relatively weak opponent, such as the Taliban, Al Qaeda, or Hezbollah, against the vastly technologically and numerically superior militaries both in Afghanistan and Iraq and in the 2006 Lebanon war against Iraq and Israeli forces [23]. Hoffman define hybrid war as a type of war that “incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion and criminal disorder. Hybrid war can be conducted by both states and variety of non-state actors” [18].

What makes a war “hybrid” and differs from other modern war is coordinated fusion of different modes of warfare, both military (use of force) and non-military (violence, irregular tactics, criminal disorder, terrorist acts), to achieve synergistic effects in the physical and psychological dimensions of conflict within the main battle space [18].

The evolution of hybrid warfare has two phases so far. The first phase is called non-state hybrid war, as it involves the

action of non-state actors that combines conventional forces, whose actions are regulated by the rules and norms of law and traditional military custom, with unconventional forces that conduct operations of guerrilla warfare, terrorist activities and criminal activities. Characteristics of this phase of hybrid war are: non-state exhibit increased levels of military sophistication as they successfully develop modern weapons systems (such as anti-ship missiles, UAVs), new technologies (cyber, secure communication, sophisticated command and control), and tactics (combined arms) that are traditionally considered to be outside range of such actors. Non-state actors expanded the battlefield beyond the purely military realm and show the growing importance of non-military tools by including elements of information warfare (e.g. controlling the battle of the narrative and online propaganda, recruitment and ideological mobilization [24].

The second phase of the evolution of the term hybrid war called state hybrid war begins with the Ukrainian crisis and the Russian annexation of Crimea in 2014. Russian operations demonstrate that hybrid warfare can be conducted with great success by state actors. The main characteristics of Russian operation in Crimea as a prototype of the second phase of hybrid warfare are:

- non-declaration of the state of war;
 - non-contact clashes between highly maneuverable interspecific fighting groups;
 - annihilation of the enemy’s military and economic power by short-time precise strikes in the strategic military and civilian infrastructure;
 - massive use of high-precision weapons and special operations, robotics, and weapons that use new physical principles (direct-energy weapons – lasers, shortwave radiation, etc);
 - use of armed civilians;
 - simultaneous strike on the enemy’s units and facilities in all of the territory;
 - simultaneous battle on land, air, sea, and in the informational space.
 - use of asymmetric and indirect methods;
 - management of troops in a unified informational sphere [25].
- Usage of non-military means, especially the use of information surprised Ukraine and represented significant factors for the realization of Russian plans in Crimea and announced future trends in warfare.

This transformation of used means surprised even Hoffman, whose definition of hybrid warfare is limited to a combination of tactics related to violence and irregular way of warfare between state and non-state actors. His definition did not recognize non-violent and non-military instruments like diplomatic, economic and financial activities, subversive political acts such as the creation or secret use of trade unions and non-governmental organizations as a front of actions, or information and propaganda operations through the use of fake websites and newspaper articles [22].

As Figure 1 shows hybrid warfare differs from other types of war in their initiation and prosecution, involve various sphere of social action, employ different strategies and means. Hybrid warfare is directed towards the whole society with the aim of destabilization and polarization. In this type of

war, not only the military weaknesses are essential but also those that only society can generate: ethnic tensions, weak and corrupt institutions, economic or energy dependence. Based on these weaknesses, hybrid war applies on the full spectrum of activities ranging from media propaganda to terrorism through irregular and unassumed warfare [26].

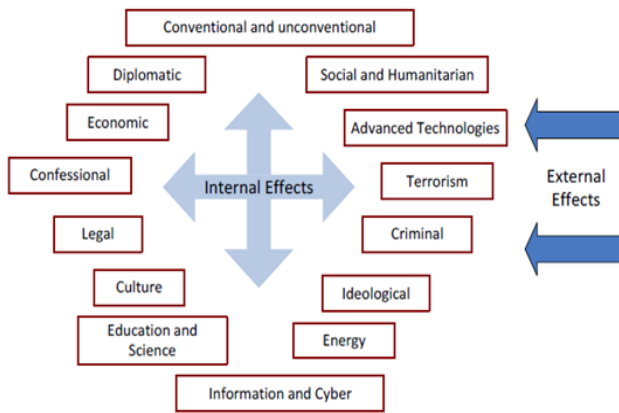


Fig 1. Hybrid warfare spheres [4]

III. THE IMPACT OF NEW TECHNOLOGIES ON HYBRID WARFARE

At the strategic level, the hybrid theory of warfare can be seen as the employment of information operations and diplomacy in conjunction with cyber and electronic operations to weaken an opponent or to sow the seeds of chaos in relation to an adversary [27]. In addition to traditional wars, hybrid wars are not declared and, therefore, cannot be completed in the classical sense of military conflicts. This is a permanent war of variable intensity across multiple sectors, with cascading impacts and synergistic destructive manifestations, in which the entire population of the country is involved. An essential feature of this concept is the diminished role of military content, more precise usage of armed struggle. Unlike the classic war conflicts, in which concepts based on the mass use of armed force were dominated, minimized often disguised military hard power is the most significant novelty in the history of warfare introduced by hybrid warfare [28].

Through the use of innovative technologies, it became possible to shift conflict from predominantly overt and forceful (kinetic) means to less obvious strategies focused on the structural vulnerabilities of adversaries, including achieving cognitive advantage over them [4]. Widespread usage of new technologies should provide reduction of hard military power to minimum creating a distorted image of the real attacker. In that way, modern technologies were the main factor that influenced and transformed warfare.

Hybrid war in Ukraine shows that the main battlefield is human mind so the most important elements of modern war become information and psychological means. Wide-ranging, multidimensional and by employing multifactorial information, hybrid warfare in Ukraine included applying of highly technological samples of weapons and military

hardware. Y. Danyik et al in the paper [4] identifies some of the most important areas of information technology involved in hybrid warfare:

1. electronic warfare systems and complexes;
2. modern information and communication systems;
3. innovative weapon control systems;
4. integrated reconnaissance-strike complexes;
5. innovative software;
6. complexes for conducting information-psychological activities and actions in cyber space
7. environmental control and space systems;
8. robotic systems (especially unmanned aircraft complexes).

All modern country are highly depended on various information infrastructure and information-based resources including complex management systems and infrastructures involving the control of electric power, money flow, air traffic, oil and gas, and other information-dependent item [29]. The development and use of new, and especially information technologies is a determinant of the state development, but also the most important means in the application of measures and countermeasures in hybrid warfare.

Ukrainian hybrid war demonstrates the complexity of strategy that includes military and nonmilitary means relying on new technologies at every stage of operation. Moscow employed methods that blended conventional and irregular combat, economic coercion, sponsorship of political protests, and the now notorious disinformation campaign [30]. Also, different technologies were use simultaneously as a part of strategically design campaign with main goal of undermining public confidence in the government. Bērziņš, identified eight phases of Russian hybrid strategy:

1. non-military means (encompassing information, moral, psychological, ideological, diplomatic and economic measures);
2. special operations carried out by media, diplomatic channels, top government and military agencies to mislead political and military leaders (can include leaking false data, orders, directives, and instructions);
3. intimidating, deceiving and bribing government and military officers with the objective of making them abandon their service duties;
4. use of destabilizing propaganda to increase discontent among the population (can be further enhanced by the arrival of 'volunteers', escalating subversion);
5. establishment of no-fly zones over the targeted country, imposition of blockades, extensive use of private military contractors and armed opposition;
6. commencement of military action, immediately preceded by large-scale reconnaissance and subversive missions of all types (including special operations forces; space, radio, radio engineering, electronic, diplomatic and secret service intelligence; and industrial espionage);
7. targeted information, electronic warfare and aerospace operations along with continuous air-force harassment, combined with the use of high-precision weapons launched

from various platforms (long-range artillery and weapons based on new physical principles, including microwaves, radiation, radiological and ecological disasters and non-lethal biological weapons);

8. crushing the remaining points of resistance and destroying surviving enemy units by using special operation units. [25]

Those are phases of war that Russians refer as “new generation of warfare” directed against Western influence in the world. While the Chinese concept of ‘unrestricted warfare’ was aimed at identifying ways to counter the West’s overwhelming hard and soft power through asymmetric means, the Russians concept of warfare is the answer on tolls that Western use: liberalism, international institutions, non-governmental organizations, and strategic communication [30]. Hybrid warfare, or new generation of war demonstrated tremendous success by usage of a sophisticated blend of psychological warfare, cyber - attacks, strategic communication, disinformation campaign and covert troops. The further risks also arise from the circumstances that nuclear states do not directly confront each other by traditional means. The doctrinal turnover that includes strategic means of hybrid warfare, as well as military modernization of states, creates a new kind of security dilemma. In that sense, nuclear security based on the concept of nuclear deterrence should be reconsidered in the context of hybrid warfare. Hybrid warfare ignores a key concept that builds nuclear deterrence as a viable strategy including concepts of stability, preparedness, clarity and rationality.

IV. CONCLUSION

Warfare is sui generis a socio-historical phenomenon with a pronounced technological component. Definition of war modified with the change of social circumstances and due to technological progress. In the last two decades, this definition expanded to incorporate non-state actors, cyber warfare and usage of non-military means. The blending of all used means of waging the war is what distinguishes hybrid war from other historical forms. The mind becomes the main battlefield of the 21st century which puts focus on information and psychological means of warfare. In the further transformation of hybrid war, the tendency will be on in developing strategies and means how to first defeat adversary mentally by the usage of non-military means. The main goal of modern warfare is the reduction of hard military power and defeating the enemy in the short term without human losses, which hybrid warfare perfectly demonstrates.

ACKNOWLEDGMENT

The research was funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia, as the part of theme "Fundamental and applied aspects of electrocatalysis in energy systems and green technologies", within the program Energy and energy efficiency, which are realized in the “Vinča” Institute of Nuclear Sciences - National Institute of Republic of Serbia, University of

Belgrade, Belgrade, Serbia.

REFERENCES

- [1] C. V. Clausewitz, “On War”, Oxford University Press, Oxford, 2007.
- [2] P. D. Williams, “On War”, *In Security Studies – An Introduction*. Routledge, London and New York, pp. 151-170. 2008.
- [3] G. Razma, “Modern Warfare Paradigm: Reconsideration of Combat Power Concept. Journal of Security and Sustainability Issues. Vol. 8, No.3, pp. 435-452. 2019.
- [4] Y. Danyik, T. Maliarchuk, C. Briggs. “Hybrid War: High-tech, Information and Cyber Conflict”. *The Quarterly Journal*, Vol. 10, No. 2, pp.5-24. 2017.
- [5] F. G. Hoffman. “Complex Irregular Warfare: The Next Revolution in Military Affairs”. *Orbis*, Vol. 50, No. 3, pp. 395-411, 2006.
- [6] YA. C. Janos, “Unconventional Warfare: Framework and Analysis”, *World Politics*, Vol. 15, No. 4, pp. 636-646, 1963.
- [7] K. Knorr, “Unconventional Warfare : Strategy and Tactics in Internal Political Strife”, *The Annals of the American Academy of Political and Social Science*, Vol 341, Issue 1, pp. 53-64, 1962.
- [8] D. Kilcullen, “The Evolution of Unconventional Warfare”. *Scandinavian Journal of Military Studies*, Vol. 2, No. 1, pp. 61–71. 2019.
- [9] C. S. Gray, “Irregular Warfare: One Nature, Many Characters”, *Strategic Studies Quarterly*, Vol. 1, No. 2, pp. 35-57, 2007.
- [10] W. S. Lind, K. Nightengale, J. F Schmitt, J. W. Sutton, Gary I. Wilso, “The Changing Face of War, Into the Four Generation“, *Marine Corps Gazette*, 1989.
- [11] W. S. Lind, “Understanding Fourth Generation of War“, *Military Review*, 2004.
- [12] Q. Liang, W. Xiangsui, *Unrestricted Warfare*. Beijing, PLA Literature and Arts 1999.
- [13] T. Huber, “Compound Warfare: A Conceptual Framework”, *Compound Warfare: That Fatal Knot*, U.S. Army Command and General Staff College Press, Kansas, 2002, 1-11.
- [14] D. Buffaloe, *Defining Asymmetric Warfare*, The Institute of Land Warfare, Virginia, 2006.
- [15] A. Lele, “Asymmetric Warfare: A State vs Non-State Conflict”, *OASIS*, No. 20, 2014, 97-111.
- [16] M. Čurčić, Asymmetric Threats in Security Studies in *Asymmetry and Strategy - Thematic Collection of Articles*. Strategic Research Institute and National Defence School, Belgrade, pp. 17-31, 2018.
- [17] E. Newman, “The ‘New Wars’ Debate: A Historical Perspective Is Needed. *Security Dialogue*. Vol. 35, No. 2, pp. 173–189. 2004.
- [18] F. G. Hoffman, Conflict in the 21st Century – The Rise of Hybrid Wars, Potomac Institute for Policy Studies, Arlington, Virginia, 2007
- [19] F. G. Hoffman, “Lessons from Lebanon: Hezbollah and Hybrid Wars”, Foreign Policy Research Institute, E-notes, 2006. Internet: <https://www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/> Access: 29.05.2021
- [20] G. Ben-Ari, “*Technological Surprise and Technological Failure in the Current Lebanon Crisis*”. Center for Strategic and International Studies. Washington D.C. 2006.
- [21] M. Vračar, M. Čurčić, “The Evolution of European Perception of the term „Hybrid Warfare“, *Vojno delo*, Vol. 1, pp. 5-21. 2018.
- [22] M. Čurčić, “Hibridni ratovi u savremenom bezbednosnom okruženju“ *U Hibridno ratovanje - dilema koncepta savremenih sukoba*, Beograd, Srbija, 2018, 47-62.
- [23] B. Renz, “Russia and ‘hybrid warfare’”. *Contemporary Politics*. pp. 1-18. 2016.
- [24] E. Reichborn-Kjennerud, P. Cullen, *What is Hybrid Warfare*, Policy Brief No.1. Norwegian Institute of International Affairs, 2016.
- [25] J. Berzins, J. *Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Policy Paper No. 2, Riga, National Defense Academy of Latvia, 2014.
- [26] M. M. Neag, “A New Typology of War – The Hybrid War”, *Revista Academiei Fortelor Terestre*, No. 1, pp. 15-20, 2016.
- [27] A. C. Fox. *Hybrid Warfare: The 21st Century Russian Way of Warfare*. School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth. Kansas. 2017.

- [28] M. Vračar, "Razmatranje adekvatnog teorijsko-epistemološkog pristupa u istraživanju fenomena hibridnog ratovanja". *Vojno delo*, No. 7, str. 292-307. 2017.
- [29] R. C. Molander, A. S. Riddile, P. A. Wilson, *Strategic Information Warfare – A New Face of War*. National Defense Research Institute. 1996.
- [30] S. Hadjitorov, M. Sokolov, "Blending New-generation Warfare and Soft Power: Hybrid Dimensions of Russia-Bulgaria Relations". *Connections: The Quarterly Journal*. No. 1, pp. 5-20, 2018.