INFORMATIVE COMBAT OF THE RUSSIAN HYBRID WAR

Marian – Valentin BÎNĂ, Cristian DRAGOMIR
"CAROL I" National Defense University, Bucharest, Romania

The objective of this paper is to analyze the control system that the media offered to Russian disinformation campaigns in a supposed context of hybrid warfare. The exposure of the news offered by the main media channels allows the analysis of the concept of hybrid warfare to be concentrated and its comparison with the traditional strategic conception, in order to determine if the activities in question can be classified in this type of conflict. Information warfare and related components such as cyber warfare, electronic warfare and more, are becoming increasingly complex and can be used both defensively and offensively in the current security context offered by the national media.

Key words: *hybrid war, media, propaganda, strategic ability, Russian Federation, security environment, independent system*.

1. INTRODUCTION

The incorporation of information and communication technologies (ICT) has brought a total change in the way we interact and communicate, but also in the way we inform ourselves. The expansion of what we know today as the Internet has allowed millions of people around the world to have access to the largest source of information in human history, primarily through smartphones, personal computers and state-of-the-art tablets.

One of the areas where the spread of the Internet had the greatest impact was communication, both in the structure of the media, in the field of its audience and in the content itself. Traditional media has been forced to adapt its organization to new formats and to a continuous demand for information from readers, in addition to the emergence of new media, exclusively digital. But this request for information has also raised some doubts about the credibility and quality of information, which is really worrying if we consider the importance of the media in democratic societies. The speed with which news is currently being propagated - either through websites, media or social networks - has an almost immediate impact on public opinion and, in many cases, ephemeral. The need to continuously generate news meant that they have a huge volatility, while conditioning the quality of the information.

In this context, public complaints addressed to Western governments regarding alleged misinformation campaigns led by the government of the Russian Federation have concentrated much of the attention of the international media. Concepts such as cyber-attacks, fake news, and hybrid threats have become widespread to denounce the spread of fake news in order to destabilize internal processes such as the June '20 Brexit, US presidential elections, and the Political Crisis and Catalan social network from Spain, which reached its peak in October 2017. According to the statements, attempts to intervene would be based on the use of information understood as a military element, of an asymmetrical nature, in a supposed context of hybrid war, directed by the Russian Federation against Western democracies, through the so-called "Gerasimov Doctrine".

2. METHODOLOGY

The purpose of this analysis is to compare the journalistic treatment that the media has offered to disinformation campaigns and to Russian hybrid problems. The concept of hybrid developed traditionally from a strategic-military field, influenced the events mentioned above in the current context of the hybrid war, as emphasized by most media and analysts in the field.

The article starts from the presentation of a series of news related to the disinformation campaigns of Russian origin and the influence that the concept of hybrid war had. Due to the large amount of news published on these issues, from the synthetic procedure, a general selection of news from various prestigious national and international media have provided a variety of perspectives such as The Guardian, The Washington Post, BBC and the Later Country, and following descriptive method, the term hybrid warfare is introduced from its traditional conception, starting from the origin of the concept, exposing some general definitions and characteristics and contextualizing it in what became popular as Gerasimov doctrine. Finally, by comparative method, the journalistic treatment of this type of conflict is compared with the traditional strategic conception.

3. CONTEXTUALIZATION OF THE HYBRID WAR

In recent years, taking as a temporary reference the referendum that took place in the UK to leave the European Union and especially after the US presidential elections held in November 2016, the media has concentrated much of its international information, warning of the danger posed by fake news - popularized as fake news - for Western democracies.

In its information objective, the media has used all kinds of concepts, new to a large part of the public, such as cyberspace, cyber-attack, cyber warfare or hybrid warfare, to explain the events that occur through what we commonly call the Internet, in which a state, in this case the Russian Federation, would use the digital sphere to interfere with another's state internal processes, in order to destabilize its democratic systems. In this unique and complex context, here's how the media reported on events.

Although Brexit is now considered an example of Russian interference in the election campaign, we found few references in the media that, both during the campaign and in the post-referendum period, accused the government of Vladimir Putin of wanting to influence the vote. The referendum defined these activities as a hybrid war. For the most part, the post-election analyzes focused on the uncertainty generated by the United Kingdom's exit from the European Union, the economic, political and social consequences that could follow, as well as the new role of the European Union at that time.

To a large extent, it was only in the US presidential elections, held in November 2016 that the media directly indicated to Moscow that they had carried out computer attacks against the Democratic Party and orchestrated misinformation campaigns to influence voting through public opinion. At this point, the emphasis was placed on cyberspace and the vulnerabilities it represents for Western democracies. Despite this fact, only after a few months began to appear continuously information about the possible Kremlin interference in the British referendum, through the spread of fake news, as well as through the use of social media.

The events marked before and after the role that a foreign power would have played in trying to influence an internal electoral process. These were a warning signal for the European countries that later months they were going to organize different electoral processes. In this context, the Guardian newspaper stated in a headline that *"the EU is intensifying its campaign against Russian propaganda*" [1] because of the fear that would have generated

the possible Russian influence in the US elections, as this could extend to Europe. It is emphasized that the Union will "*step up efforts to counter Russia's hybrid war campaign after Donald Trump's election.*" [2] The news refers to the East STRATCOM working group, an organization created in 2015 by the EU External Action Service - and therefore before the processes presented here - to counter Russian misinformation campaigns during the crisis in Ukraine.

In this international context of misinformation, fake news, Russian influences in electoral processes, cyber-attacks and alleged hybrid war, Spain has been plunged into a major political and social crisis because of a referendum by the regional government of Catalonia, at the beginning of October 2017, which was intended to decide by consultation on the possibility of independence from the Spanish state, without the consent of the Spanish government. These activities were quickly incorporated into the information language. Titles such as *"Cyber war between the Catalan and Spanish governments to close the referendum site*" [3], published in the El País newspaper a few days before the referendum or "*The great Catalan cyber war of 2017*" [4], published by The Washington Post, just two weeks after held the referendum, they used the concept of cyber war in a generic way, regardless of its significance and possible implications, for the simple fact that certain activities were carried out through the network.

The concept of cyber war was one of the most used in the journalistic field to refer to the activities that take place on the Internet, but in return, it created confusion. Richard A. Clarke, former US National Security, Infrastructure Protection and Counter-Terrorism Coordinator and President's Special Adviser on Cyber Security, defines cyber war as *"actions taken by a nation-state to break into computers or other state networks for the purpose of causing damage or alteration."* [5] Except for cyber-attacks against the Democratic Party, for which he had access to the campaign data and information of the Party members, the propaganda activities that took place in Brexit and in the Catalan conflict cannot be described as cyber war, according to Clarke's Definition, as they would not would have led to the illegitimate access to the systems or networks of other states, in order to cause damages or changes, but rather they would be influential and manipulative activities through the network.

This new doctrine, elaborated in Russia, seeks to weaken democracies, mixing in their electoral processes and fueling their internal conflicts, whether ideological or territorial, using tools such as fake news or manipulation of social networks.

Instead, they just say that we are in a conflict (hybrid war) promoted by a state actor (Russia), by spreading fake news over the internet and social networks, with the ultimate goal of weakening Western democratic governments. On the other hand, the news of these activities presents the hybrid war as something new, which is part of a military doctrine of Russian origin known as the Gerasimov doctrine.

4. THE ORIGIN AND CHARACTERISTICS OF THE HYBRID WARS

There are authors who attribute the origin of the term hybrid warfare to the retired US Marine General Robert Walker, who in 1998 analyzed in his paper the hybrid model of wars. On the other hand, there are those who point out that the origin should be placed a few years later, in 2002, when the term was used to explain the tactical actions of the First Chechen War, which took place between 1994 and 1996. However these were not officially used until the 2005 US National Defense Strategy [6]. Only in 2005 was the publication of Future Warfare: The Rise of Hybrid Warfare published by General James N. Mattis and Colonel Frank G. Hoffman and the

work Conflict in the Century. Rise of Hybrid Wars published by Frank G. Hoffman, when the concept gained theoretical content and became popular.

The concept has been largely extended to try to understand contemporary wars between state and non-state actors, in which a top theoretical actor in the field of technology, military or doctrinal capacity has been surprised by a non-state actor.

4.1. Definitions of hybrid warfare

One of the first approaches defines hybrid warfare as "*the one at the intersections between special war and conventional war.*" [7] For his part, Hoffman broadens and specifies his nature and considers that *"it mixes the lethality of the state conflict with the fanatical and widespread fervor of the irregular war"* [8]. It can be promoted by both state and non-state actors. These conflicts "*incorporate a variety of different ways of conducting war, including conventional capabilities, irregular tactics and formations, terrorist activities, including violence and coercion without discrimination and criminal disturbance.*" [8] In practice, this involves the combination of conventional and irregular activities. In a similar vein, the infantry colonel of the Spanish army, José Luis Calvo Albero, defines the hybrid war as the "*one in which at least one of the opponents uses a combination of conventional operations and irregular war, mixed with the latter, with actions. terrorists and connections to organized crime.*" [9]

Despite these approaches, there is currently no precise definition of the concept, which is widely accepted, beyond the smallest common denominator of the combination of conventional, asymmetrical means, procedures and tactics. In post-Cold War conflicts, those who faced western states would, at times, have used conventional forces, irregular troops, terrorist acts and organized crime.

4.2. The characteristics of hybrid wars

The news presented the hybrid war as a unique conflict, focusing mainly on the information element, misinformation and fake news, and its dissemination on the Internet. But such conflicts would also involve combining other elements to consider, such as the actors involved, the type of weapons they have and the scenarios that are constantly developing. Some features of hybrid wars are:

- *The physiognomy of the actors involved*: these include states, guerrilla groups and terrorists, as well as organized crime groups or private military contractors. These types of conflicts can be assumed by state actors or non-state actors. As noted above, analyzes of hybrid warfare have focused mainly on confrontations between non-state actors, regularly attacked by a failed state, and western states, such as in the wars in Afghanistan, Iraq, and confrontation between Hezbollah and Israel. Insurgent groups would develop hybrid warfare because they would have lower capabilities for state actors, personnel deficiencies, doctrine, weapons and technology. Comprised mainly of volunteers, the objective would be to counteract the superiority of the state actor and exploit its vulnerabilities. On the other hand, this type of conflict can also arise from the state actors, in a possible conventional confrontation with other state actors, superior from a military point of view. An unusual case would be the conflict between Ukraine and Russia in 2014, in which the most theoretically powerful state, Russia was the one who used the hybrid war against the least developed ones. This decision would be based on avoiding a conventional confrontation and, in turn, on a possible confrontation with the

United States and NATO, in which Russia would be the affected party.

- *Type of weapon used*: Irregular forces have more armament than ordinary armies, such as the latest technologies and heavy weapons, which makes it more difficult to distinguish between conventional and irregular forms of war.
- *The tactic used*: from the use of conventional actions to terrorist acts, the use of insurgent actions, informative operations or computer operations.
- *Use of information and communication technologies*: this feature of hybrid warfare includes the control of traditional media up to the internet and social networks. This would make it possible to strengthen one's own image or to counteract that of the adversary, in order to reach the "*hearts and minds of people*" [10], which would be largely psychological warfare. In this way, there is an increasing importance of the so-called information war and the use of cyberspace.
- *Scenarios for the battle space*: these types of conflicts are considered essentially urban, as opposed to guerrilla wars, which would take place in the jungle or mountains. This creates greater difficulties in achieving the military objectives, due to the presence of the civilian population and the possible consequences on the critical infrastructure, such as transport and energy.
- *Liaison with terrorist groups and organized crime*: It is common for groups involved in hybrid wars to have links with terrorist groups or organized crime. This does not necessarily imply that they have common goals.
- *The increasing importance of the psychological element*: there is an intentional disregard for the legality and international humanitarian law by the promoters of hybrid wars and the related criminal and terrorist groups. On the contrary, the Western Armed Forces are subject to rules, military traditions or confrontation rules. Therefore, hybrid wars can be considered formally different from traditional conflicts, in that they "*have been fought conventionally and symmetrically on clearly defined fronts, with time-advanced technological means and subject to the commonly accepted uses and customs of war for competitors.*" [11]
- *Planning*: the promoters of this type of conflict would have previously detected the weaknesses of the adversary, in the political, ideological, economic or demographic field, in order to prolong the conflict, to increase the costs or to influence the perception of the societies and of the western states.

It should be noted that hybrid wars involve the combination of regular and irregular elements. Therefore, the use of one of these elements does not imply that a conflict can necessarily be considered a "hybrid". Russian activities in the cases: Brexit, the US elections and the Catalan conflict, have received the hybrid qualification largely due to the use of cyberspace and the combination of computer attacks, propaganda and misinformation, the use of information and communication technologies, as well as information operations. However, it was by no means an armed confrontation involving state or non-state actors.

5. THE HYBRID WAR AND THE RELATIONSHIP WITH MASS-MEDIA

According to the press, Russia is waging a hybrid war against Western states. However, the above classification presents a different scenario from those described. The news, according to

the news, is that only one state, Russia would wage such wars simultaneously against several states, including the main military powers such as the United States and Britain. This, through a continuous process that extends over time, but in which we can identify high pressure moments, for example, shortly before the electoral processes in the UK. Despite the development that Russia has made in the digital sphere, along with misinformation campaigns, it has no monopoly on these activities. However, the media reported that it is an almost exclusive activity of Russia. It should be borne in mind that one of the fundamental characteristics of the hybrid war would be not only the use of information and communication technologies, but also the simultaneous use of other components mentioned above. That is, the combination of the usual and irregular elements referred to by Hoffman. In the supposed hybrid war between Russia and the western states, there is no armed conflict in which regular and irregular forces participate, advanced weapons are used or terrorist acts are carried out.

One of the features emphasized by the media was the novelty of this type of conflict and the exclusivity that Russia had in approaching hybrid wars. Some experts believe that "*these forms of action can hardly be described as new or considered as a specific response to the westernized fighting style.*" [12]

On the other hand, one of the characteristic elements of hybrid wars is the space in which they develop, mainly urban centers. If we look at the conflict in Eastern Europe, Russia would have used cyberspace as the main stage of its activities. For all these reasons, although computer operations were carried out via the Internet, not only the dissemination of news, but also computer attacks such as those against the United States Democratic Party, which allowed access to email accounts, these activities were defined as hybrid war, within the events exposed to the news.

6. GERASIMOV DOCTRINE AND THE HYBRID WAR

If the concept of hybrid warfare was concentrated in one part of the analysis, other concepts were used to contextualize these conflicts. The media emphasized that the hybrid war was part of a Russian military doctrine that became popular as the Gerasimov doctrine, which would expose the line separating the war from peace is now widespread, so they must develop tactics to allow it working in the shadows, conditioning the electoral processes, agitating the civilian population or hacking targets in other countries.

The origin of the concept dates from February 2013, with the publication of the article "The value of science in anticipation" of the Chief of Defense Staff of the Russian Army, General Valeri Gerasimov in the journal Voyenno-Promyshlennyy Kuryer. For most Western media and analysts, the article is the cornerstone of what is known in the West as the Gerasimov doctrine. "*It is interpreted as a proposal for a new Russian mode of war that combines conventional and unconventional warfare with aspects of national power*" [13], which refers to indirect and asymmetrical methods. With the events in Crimea and Ukraine, some of the elements set out in Gerasimov's 2013 document have been identified and the idea that it exposes a new way of acting has been propagated.

The hybrid then crossed the border of strategic debate to become a word of common use and was used to define the full range of informational, destabilizing and subversive activities that the Kremlin could conduct in a hidden, semi-covert or clandestine manner, below the threshold of conflict.

Despite widespread acceptance of the concept and the fact that it represents a new doctrine, some analysts have questioned whether it is military doctrine or propose a new Russian way of waging war. It is noteworthy that he

stated in his article "*his perspective on the recent past, present and future of the war*" [14], based largely on what happened in the "*Arab Spring"* [15] *and the "color revolutions*" [16]. Gerasimov emphasizes non-military means, such as political, economic, humanitarian, undercover operations, as well as the importance of information. Russia, for its part, considers hybrid warfare to be a Western term and therefore different from its doctrinal system. In fact, the Russian Federation refers to different terms related to hybrid warfare, such as "non-linear warfare", "*ambiguous warfare*" and "*network warfare*" [17].

Three years later, Gerasimov published a new article in which he presented some ideas about contemporary wars, apparently similar to the previous document, but in which he added the experiences of conflicts in Ukraine and Syria. Gerasimov identifies hybrid methods in color revolutions and states that these movements are, in fact, matters promoted by the West. Unlike the 2013 article, this document refers openly to wars and hybrid methods, but in a different way as the ones from the West.

As mentioned above, hybrid warfare would combine conventional and irregular methods, in which we found links with organized crime or terrorist groups, while, in Gerasimov's view, in contemporary conflicts, it is increasingly common to give priority to common uses of non-military, political, economic, informational and other measures that are implemented with the support of military force [18]. All of these elements integrated under the same umbrella are called hybrid methods.

In practice, this would imply a more limited perception of hybrid actions than the West has. Despite this difference, the author argues that the integration of traditional and hybrid activities is a feature of contemporary armed conflicts, in which he indicates the informative element as the main of the hybrid methods. This is because the falsification of events, the limitation of the media activity, become one of the most efficient asymmetrical methods for carrying out wars. Its effect can be comparable to the results of massive troop use.

In short, Gerasimov refers to hybrid warfare methods, as he believes that Russia should cope with these types of wars and, therefore, must know and adapt to them. In addition, it must be taken into account that Gerasimov presents it in a scenario of armed warfare, while misinformation campaigns and fake news in the West would take place in a context of political and social tension and confrontation, but in the absence of an armed conflict. Last but not least, Mark Galeotti, the analyst who coined the term *Gerasimov's doctrine* [19], not only denied the existence of that alleged doctrine, but also noted that Gerasimov's article was intended to resolve how to combat unconventional actions.

7. CONCLUSIONS

It is common to find news related to misinformation campaigns of Russian origin claiming to be registered in a context of hybrid warfare against the West. The main problem with the journalistic information presented here is that, for most part, the authors do not expose even a brief approximation to the concepts used, their meaning and implications, such as misinformation, fake news, cyber war or hybrid warfare.

Sometimes this leads to the use of some of these concepts as synonyms. Possibly, one of the reasons for the confusion is the mix between the use of recent concepts, in this case, those related to the cyber space, with others that are traditionally located in a military and academic field, in an attempt to wish to be informed about changes that appear on the international stage. This is also due to the spiral in which the media has entered, driven by a constant demand for information from citizens, wanting to be informed almost minute by minute about the latest news, which means the information

quantity rather than the quality of the messages is transmitted.

Undoubtedly, the use of cyber and information by Russia has been the focus of the news regarding the hybrid war. But while it is true that this country has encouraged the use of information operations and has taken advantage of the potential of the digital environment in its interests, it is true that the development of misinformation campaigns and the use of information and communication technologies cannot be identified solely with the hybrid war.

One of the characteristics of hybrid conflicts is the combination of different conventional and asymmetrical elements, but the news focused almost exclusively on the digital element, through which the campaigns of misinformation, fake news and the massive use of social networks were developed. Although they can be part of hybrid conflicts, and the fact that in recent years the cyber element has gained enormous importance in conflicts, we cannot stress that these activities are movements of the hybrid war.

Therefore, if we conclude that the events that took place on the occasion of Brexit referendum, in the US elections and in the Catalan conflict cannot be described as a hybrid war, a significant analysis framework to understand the news of cyberspace and its impact on international relations in these scenarios could be developed from the grey area concept. The concept defines those activities that are below the conflict threshold, which are conducted in peacetime, as opposed to hybrid warfare, and which include computer attacks or misinformation and propaganda campaigns that would have as a common feature the difficulty of determining their attribution. Therefore, this concept would allow an analysis of activities that are not specifically described as war actions, but could become just as decisive as a military conflict.

The analysis presented in the article focuses on the importance of conceptualizing and contextualizing the reported facts. It is clear that the practice of journalism differs from the academic field, but it is true that the news should transmit as rigorously as possible and expose to the reader what is happening in their specific context, trying to use appropriate concepts in each case. We are still in an early stage in the analysis of cyberspace capabilities, and its reduction only to the use that a single state can make for the dissemination of propaganda campaigns, which means we do not understand its potential in international relations.

ENDNOTES AND REFERENCES

[1]. Boffey, Daniel, Jennifer Rankin, "*EU escalates its campaign against Russian propaganda*." The Guardian, 23 November 2017;

[2]. Boffey, Daniel, *„UE strânge fonduri pentru combaterea războiului de dezinformare cu Rusia"*. The Guardian, 5 decembrie 2018;

[3]. Pueyo, Jordi. 2017. "Ciberguerra entre los gobiernos catalán y español por el cierre de la web del referéndum". El País, 14 de Septiembre. https://elpais.com/ccaa/2017/09/14/catalunya/1505390726_024743.html, accessed at 14.06.2019;

[4]. Caryl, Christian. 2017. *"The great Catalonian cyberwar of 2017"*. The Washington Post, 18 de Octubre. https://www.washingtonpost.com/news/democracy-post/wp/2017/10/18/the-great-catalonian-cyberwar-of-2017/, accessed at 04.08.2019;

[5]. Clarke, Richard A., Robert K. Knake. 2010. *Cyber War: the next threat to national security and what to do about it*. EEUU: Harper Collins Publishers;

[6]. Colom, Guillem. 2019. *"La amenaza híbrida: mitos, leyendas y realidades"*. Instituto Español de Estudios Estratégicos, Do-cumento de Trabajo. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICOL-hibrida.pdf, accessed at 19.01.2020;

[7]. Walker, Robert G. 1998. *"Spec Fi: The United States Marine Corps and Special Operations"*. Tesis de maestría, Naval Postgraduate School. https://apps.dtic.mil/dtic/tr/full-text/u2/a359694.pdf, accessed la 09.02.2020;
[8]. Hoffman, Frank G. 2007. *Conflict in the 21stCentury. The Rise of Hybrid Wars*. Virginia: Potomac Institute for Policy Studies. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, accessed at 09.02.2020;
[9]. Palacios, José Miguel. 2016. "Rusia: guerra híbrida y conflictos asimétricos". Revista Ejército 904, julio-agosto: 22-27;
[10]. Wither, James K. *"Making Sens of Hybrid Warfare"*. Connections: The Quarterly Journal 2, 2016;
[11]. Colom, Guillem. 2018. "La Doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo". Revista Ejército 933, diciembre. https://www.ugr.es/~gesi/Doctrina-Gerasimov.pdf, accessed at 12.02.2020;
[12]. Colom, Guillem "*Vigencia y limitacio-nes de la guerra híbrida*". Revista Científica General José María Córdova 1, 2012;
[13]. Bartles, Charles K., *"Cómo comprender el artículo de Gerasimov*". Military Review, 2016;
[14]. Gerasimov, Valeri. 2013. *"Ценностьнаукивпредвидении*". VPK 476 8, marzo. https://vpk-news.ru/articles/14632, accessed at 02.02.2020;
[15]. *"The Arab Spring has been a series of protest movements that have taken place in several countries in the Middle East and North Africa since the end of 2010. Mainly, these have taken place in Arab countries where an authoritarian or totalitarian regime has ruled*", https://en.wikipedia.org/wiki/Prim%C4%83vara_arab%C4%83, accessed 24.02.2020
[16]. *"The color revolution is the non-violent overthrow of power through street protests"*, https://ro.odkurzacze.info/2746-the-most-famous-color-revolutions.html, accessed on 23.02.2020;
[17]. Milosevich, Mira "*El poder de la influencia rusa: la desinformación*". Real Instituto Elcano, ARI 7/2017, 2017;
[18]. Gerasimov, Valeri. . *"По опыту Сирии". VPK 624 9*, 2016 marzo. https://www.vpk-news.ru/articles/48913 accessed at 09.02.2020;
[19]. Galeotti, Mark. 2018. *"I'm sorry for creating the Gerasimov Doctrine"*. Foreign Policy,https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/, accessed at 23.02.2020.