Cilt | Volume 25 • Sayı | Issue 54 • Haziran | June 2024

e-ISSN: 2667-7296

SOSYAL VE BEŞERİ BİLİMLER ARAŞTIRMALARI DERGİSİ

Journal of Social Sciences and Humanities Researches

SOBBİAD, 25/54 (Haziran/June 2024), 74-92.

A New Hybrid War Arena: Russia's Interventions in Ukraine in 2014 and 2022

Yeni Bir Hibrit Savaş Arenası: Rusya'nın 2014 ve 2022 Ukrayna Müdahaleleri

Özlem DEMİRKIRAN
Sorumlu Yazar | Corresponding Author
Dr. Öğr. Üyesi | Assist Prof. Dr.
Süleyman Demirel Üniversitesi, İİBF,
Uluslararası İlişkiler Bölümü
Isparta, Türkiye
ozlemdemirkiran@sdu.edu.tr | 0000-0002-6558-3206

Berkay Göktuğ ÖNER
Doktora| PhD
Süleyman Demirel Üniversitesi, İİBF,
Uluslararası İlişkiler Bölümü
Isparta, Türkiye
bgoktugoner@icloud.com| 0000-0003-2801-8600

Makale Bilgileri | Article Information

Makale Türü: Araştırma Makalesi

Geliş Tarihi | Received: 30.05.2024

Yayım Tarihi | Published: 30.06.2024

İntihal: Bu makale, en az iki hakem tarafından incelenmiş ve intihal içermediği teyit edilmiştir.

Hakem Değerlendirmesi: Dış bağımsız.

Katkı Oranı | Contribution Rate: Ö.D. % 50; B.G.Ö. %50

Etik Beyanı: Bu çalışmanın hazırlanma sürecinde etik ilkelere uyulmuştur.

Çıkar Çatışması: Yazar(lar) çıkar çatışması bildirmemiştir.

Finansman: Herhangi bir fon, hibe veya başka bir destek alınmamıştır.

Article Type: Research Article

Kabul Tarihi | Accepted: 26.06.2024

Yayın Sezonu | Pub Season: Haziran / June

Plagiarism: The paper has been reviewed by at least two referees and scanned via software.

Peer-review: Externally peer-reviewed.

Lisans | Copyright: CC BY-NC 4.0

Ethical Statement: Ethical principles were followed during the preparation of this study.

Declaration of Interests: The author(s) have no conflicts of interest to declare.

Funding: No funds, grants, or other support was received.

Atıf | Citation: Demirkıran, Ö., Öner, B. G. (2024). A new hybrid war arena: Russia's interventions in Ukraine in 2014 and 2022. *Sosyal ve Beşeri Bilimler Araştırmaları Dergisi*, *25*(54), 74-92.

Öz

Hibrit savaş kavramı, günümüzün karmaşık güvenlik ortamında giderek önem kazanan bir konudur. Bu makale, öncelikle literatürde hibrit savaş kavramının nasıl tanımlandığını ortaya koymayı, sonrasında ise hibrit savaş perspektifinden Rusya'nın 2014 ve 2022 Ukrayna müdahalelerini incelemeyi amaçlamaktadır. Hibrit savaş, üzerinde anlaşılan bir tanımı olmasa da geleneksel askeri yöntemlerin yanı sıra enformasyon savaşı, siber saldırılar, vekâlet savaşları gibi farklı araçların kullanıldığı karmaşık bir çatışma taktiği olarak karşımıza çıkmaktadır. Rusya'nın 2014 müdahalesinde bu farklı araçları yoğun olarak kullandığı kabul görmektedir. Makalede, Rusya'nın 2014 Kırım ve Donbas odaklı müdahalesinde olduğu gibi 24 Şubat 2022'de askerlerin Ukrayna topraklarına girmesiyle başlayan Rusya'nın 'özel askeri operasyonu'nda da daha geniş bir alanda hibrit savaş unsurlarının kullanıldığı değerlendirilmektedir.

Anahtar kelimeler: Hibrit savaş, Rusya, Ukrayna

Abstract

The concept of hybrid warfare is an increasingly important issue in today's complex security environment. This article first aims to reveal how the concept of hybrid warfare is defined in the literature and then to analyze Russia's 2014 and 2022 interventions in Ukraine from the perspective of hybrid warfare. Although there is no agreed definition of hybrid warfare, it appears as a complex conflict tactic that uses different tools such as information warfare, cyber attacks, proxy wars in addition to traditional military methods. It is widely accepted that Russia used these different tools extensively in its 2014 intervention. In this article, it is evaluated that, as it was the case in Russia's 2014 intervention that focused on Crimea and Donbas, hybrid warfare elements are being used in a wider area in Russia's 'special military operation', which started on February 24, 2022 with the entry of troops into Ukrainian territory, as in Russia's 2014 intervention focused on Crimea and Donbas.

Keywords: Hybrid Warfare, Russia, Ukraine

Introduction

When the discipline of international relations is examined, it is seen that war is usually explained by focusing on states as the level of analysis. However, while until the 19th century, war was seen as a subject that only soldiers were interested in, after the Napoleonic Wars, with the "militarization" of the entire nation, it turned into a situation that affected every segment of society. In this period, the effects of war were no longer limited to military institutions but became a phenomenon that deeply affected all segments of society (Yalçınkaya & Türkeş, 2008: 58-60).

From a realist perspective, the influences stemming from human instincts are reflected in the character of the states that people build and, most importantly, in the "anarchy" that characterizes the international political system. Kenneth Waltz, in his treatise "Man, The State and War", discusses the causes of war from three levels of analysis. At the first level, the nature of human beings and, at the second level, the internal political structures of states may not be sufficient to explain the exact causes of war. According to Waltz, only the third and final level of analysis, namely the ever-present "anarchy" in the international system, has the potential to explain the causes of war (Waltz, 2001: 72-80). However, if "war" is to be explained in an even better way, we will come across many areas and dimensions that have been subjected to significant changes until today. This transformation is primarily driven by significant technological advancements and strategic developments. The nature and form of warfare continues to evolve with the discovery and use of new technologies. For example, the defense industry in general, and cyber weapons and developments in particular, as well as systems such as satellites and positioning systems, are evolving at a dizzying pace with the help of artificial intelligence. Strategic thinking and war tactics are also adapting to these changes. As a result, developments in technology and strategy have greatly affected the way war is waged and its outcomes (Gürcan, 2012: 87).

War turns into a set of continuous actions on a piece of land in order to call it a homeland. These actions, on the other hand, aim not only to dominate that piece of land, but also to be effective in every dimension and sense, politically, economically and socially. Hard power elements are the first tools that come to mind at this point. As a matter of fact, when we look at the military expenditures of the countries in 2023, it was the 9th consecutive increase worldwide and reached 2,4 trillion in total. For the first time since 2009, military expenditures have increased in all five geographical regions. The US, China, and Russia allocate the largest budgets (SIPRI, 2024). However, military power is no longer the most effective factor for achieving the desired goals. In today's world new concepts are emerging in the literature for the elements used together with military power in war. One such concept is "hybrid warfare".

Hybrid warfare refers to an approach that utilizes the advances offered by contemporary technology and communication innovations to collectively employ various asymmetric tactics such as civilian and military forces, irregular and regular forces, conventional and cyber attacks, information warfare and proxy wars. There are still efforts to understand and evaluate the conceptual aspects of defining today's crises.

Russia's 2014 intervention is one of the first examples that the concept of hybrid warfare brings to mind. However, Russia's 2022 'special military operation' gives the appearance of a conventional war. This study firstly tries to reveal how the concept of hybrid warfare is defined in the literature and what types of actions are named this way. In this regard, it aims to examine Russia's actions on the field during Russia's 2014 and 2022 interventions and analyze these interventions in the context of hybrid warfare.

1. Conceptual and Definitional Research on Hybrid Warfare

The Turkish dictionary defines the word "hybrid" as "a mixture" or "a combination of two different elements". The word "hybrid", which has its origin in Latin, is defined in the English language as a substance formed by the combination of two different elements. The concept of hybrid warfare does not yet have a common definition. For this reason, there are different definitions in the literature. The main reason for this situation is that authors create definitions based on different case studies and it is difficult to categorise activities due to the hidden and complex nature of hybrid warfare (Erol and Oğuz, 2015: 262).

As mentioned above, the term 'hybrid' is defined as an item formed by the combination of two different elements; in fact, it draws attention to more than one element rather than a single one. When it is used as a kind or type of warfare, it is understood as the use of irregular or regular army, armed force, military force, as well as public and civilian elements (political, social, economic, etc.) and methods that do not require the use of force (economic, social, political, etc.). Talking about the threats that cause hybrid warfare, Hoffman emphasises the following point: The enemy simultaneously uses classical weapons, different tactics, political violence, terrorism and all forms of intertwined extralegal activities across the entire theatre of operations to achieve its political objectives (Hoffman, 2014). Mansoor defines hybrid warfare as 'the joint use of conventional military forces and irregular forces (guerrillas, insurgents and terrorists) to achieve a common political objective'. This definition points to the multidimensionality of hybrid warfare, where different parties come together to act with a common strategy and use conventional military forces as well as irregular forces (Mansoor, 2012: 2). However, these definitions seem to limit hybrid warfare to only violent activities. Such a definition ignores many elements that are used or could potentially be used for similar purposes. In particular, non-violent public events, economic and financial activities, overt or covert use of non-governmental organizations, the mobilization of different political elements, the use of fake websites or fabricated newspaper articles in disinformation warfare should also be taken into account. Serious disinformation can even be carried out through fake social media accounts. For example, the disinformation that began on October 20, 2022, when a user of RT Afrique claimed on Twitter that France's ambassador to Ukraine, Etienne de Poncins, had resigned after criticizing Zelensky and reacting that "we don't know what we are defending here anymore; even Vladimir Zelenski is no longer in Kiev." The outgoing Ambassador responded to a social media user who raised the allegation by saying, "This is fake news, please remove it immediately" (Kahyalar, 2022). When all explanations that attempt to articulate and refine hybrid warfare exclude all or some of the aforementioned "non-force" activities, the definition falls short of capturing the nature of contemporary conflicts. This shortcoming becomes particularly glaring if one analyzes some recent conflicts. The crisis in Ukraine, first in 2014 and then in 2022, is a notable example in this regard (Karabulut, 2016: 26).

Sun Tzu made important contributions to the history of warfare. One of these achievements, in relation to the subject we are studying, is that rather than defeating enemy elements directly, he reflected different methods onto the battlefield in such a way that they could be combined and used together. These methods are aimed at defeating the enemy strategically. With this tactic of attacking the enemy's weak sides, Sun Tzu emphasizes the indirect approach. He established the tactical and strategic value of guerrilla warfare 4,000 years ago. The approaches to warfare he developed in this very early period of history led Sun Tzu to argue that war can be fought between parties with different and unbalanced fighting capabilities. This approach claims that the imbalance of power in terms of strength is no longer a problem, i.e. it is not based on the assumption that the military stronger side always wins. Therefore, the foundation of the type of warfare that is now referred to as "asymmetric" or "hybrid warfare" was laid in those years (Segal, 2018: 48). While talking about the characteristics of war in the conventional sense, it should be noted that the concepts mentioned by Clausewitz, such as the declaration of war, the separation of innocent civilians from soldiers, and the front, are no longer seen today (Clausewitz, 2003: 45). While the state, which is the subject of war as an actor, continues to exist on the ground, at the same time, some elements outside the state have started to stand out. These other elements, i.e. those outside the state, include separatism, revolutionary movements and many other elements that rebel against the authority. These actors emerged entirely due to the weakening of the state structure. For example, new wars such as the Bosnian War have witnessed the presence of many non-state actors such as criminal organizations, paramilitary groups, foreign mercenaries and militias. Mello notes that some authors argue that contemporary wars and conflicts are increasingly characterized by barbaric war crimes and mass killings of civilians. Bosnia, the Republic of Congo and Sierra Leone are painful examples of this situation (Mello, 2010: 3).

Carl Von Clausewitz, a Prussian commander who claimed that every age creates its own war, draws attention with this prediction that is valid even today. In particular, the events that followed the terrorist attacks of September 11, 2001 have revealed that wars will no longer be the same as they were before. Conflicts with unknown parties and uncertain technology have created new concepts of war (Özer, 2018: 51).

The concept of hybrid warfare was first used in 1998 by Robert G. Walker in his master's thesis, in which he defined it as the combined operations of special forces and conventional forces (Walker, 1998: 4). Frank Hoffman drew the theoretical framework of the concept in 2007. According to Hoffman, hybrid warfare, which can be practiced by both state and non-state actors, is a combination of several types of warfare, including conventional capabilities, asymmetric tactics and formations, terrorist acts of indiscriminate violence and coercion, and criminal disturbances. It is the capacity of conventional and asymmetric elements to operate simultaneously, including military and non-military means (Hoffman, 2009: 36; Arslan, 2023: 335). In other words, Hoffman predicts that in the future, rather than conventional forces, the elements that will create asymmetric warfare will exist simultaneously, from terrorist groups to criminal organizations and mercenaries. Thus, the most striking feature of hybrid warfare is the combination of guerrilla tactics and advanced technological systems. From this point of view, it can be predicted that hybrid warfare will not be limited to actors outside the state, and that states may use it against more powerful states in the future (Hoffman, 2009: 37).

Hybrid warfare refers to a situation in which coordination and cooperation between separatist/destructive groups, conventional forces, non-state armed elements, criminal organizations and public political actors are uniquely considered at all levels of military decision-making (tactical, operational and strategic). It is also based on the observation that civilian infrastructures such as fiber optic cables, satellites, internet providers etc. are increasingly being used for military purposes (Hoffman, 2009: 37).

New technologies provide actors in conflict with the opportunity to react flexibly and adaptively to external events in an environment that allows them to operate directly. Based on the aforementioned qualities, beyond the physical environment such as land, sea and air, comprehensive assessments should be made regarding space platforms and especially the cyber environment, which is the most used area in hybrid warfare operations today. Thus, the ability to use data and information as weapons is increasingly becoming part of the process. These qualities of hybrid warfare form the main points that distinguish it from its predecessors. According to Frank Hoffman, the distinctive characteristics of this new type of warfare are the blurring of borders and the intertwining of dimensions such as time and space in the conflict environment (Hoffman, 2009: 37). The blurring of boundaries between actors in the implementation of hybrid warfare should be addressed first. Regular and irregular forces, terrorists, criminals and other social groups are involved in this type of warfare because they perceive it as an opportunity to realize their own objectives. Secondly, we talk about situations where active and passive effects of conventional and unconventional capabilities coexist on the same battlefield, blurring the boundaries between the means of warfare. Ultimately, there is a serious technologically induced uncertainty within physical, virtual and psychological environments. The nature and extent of the uncertainty between these three environments or platforms distinguishes hybrid warfare from similarly conceptualized forms of warfare such as fourth generation warfare and joint or combined warfare. Examples of such wars have been witnessed recently (Fairclough, 2018: 12).

In the aftermath of the Cold War, which Hoffman described using the concept of hybrid warfare and claimed that a new type of conflict had emerged, many studies have emerged on the subject. Considering that the concept of hybrid warfare has been used in recent events such as Ukraine and Syria, the interest has not diminished but even increased. These events show that the concept of hybrid warfare remains important in defining current situations (Fairclough, 2018: 7–21).

In his study "Historical Evolution of Hybrid Threat" Johnson argued that hybrid threats involve methods of conflict that are combined or blended using specially designed "methods" to achieve easily identifiable "political objectives". The aim of these methods is to persuade the adversary to agree to the desired outcomes. These methods manifest themselves in five different ways. First, there is a political element. For example, disrupting economic policies through misinformation, cybersabotage, or espionage. Second, diplomacy plays an important role. This is an attempt to separate or divide allies. Third, there is a military dimension. This includes local irregular forces, armies being used for different purposes, assassination and sabotage, proxy elements, psychological challenges such as fear and coercion, and terrorism. Fourth, there is the social dimension. In particular, media campaigns are used to demoralize the population. Fifth, economic aggression and sanctions. The tools and methods used in this dimension include the acquisition of assets, especially strategic resources, as well as interference in price policies and the purchasing power of consumers. These issues, which are mainly of interest to economics, manifest themselves in the form of implicit or direct sanctions through bilateral trade relations, international organizations, the trading status of the reserve currency, and technology companies. All of these problems emerge as unsolvable or seemingly threatening situations. This is because military forces do not have the capacity to deal with them. In fact, measures using military force are considered much less important than diplomacy, economic, or political measures (Johnson, 2018: 3).

Definitions of hybrid warfare primarily emphasize a complex, rapidly changing space with a disproportionate and imbalance of forces. This space is an environment in which there are many actors focused on their interests and objectives. These actors can be states or proxy states, as well as all the irregular, illegal entities within society, such as criminal organizations that consider themselves outside of society or seek to gain advantages and better conditions for themselves (Fairclough, 2018: 8).

Hybrid warfare has effectively entered the literature and influenced the concepts and strategic documents of national armies as well as organizations emerging from regional and international alliances. This concept is still being discussed in a multifaceted manner with its political, legal, social, cultural, and finally technological dimensions (Özel and İnaltekin, 2018: 3). According to the first examples of the definition of "hybrid" warfare, beyond the definition of "armed conflict in which technological innovations are combined with covert tactics", the practices used by new actors are a combination of insurgency and conventional warfare (Hoffman, 2009: 37). Notably, the concept, as articulated by Johnson, is not new. Johnson cites examples such as the "Hashemite Revolts" in the Ottoman Empire during World War I and the American Civil War to defend the thesis that hybrid warfare is not a new concept but that it has changed its shape (Johnson, 2018: 3).

The most important philosophical approach that can be shown as the main basis for hybrid warfare is to gain advantage with unexpected moves by avoiding predictability and some predictable behavior patterns. This approach involves using all kinds of attack methods. However, considering these characteristics and approach, it is difficult to say that hybrid warfare is a new type of warfare. Among the salient features of hybrid warfare are the inclusion of innovative tools and methods in the decision-making process and their spatial use in the entire theater of operations. The blurring of the military-civilian distinction and the involvement of many different actors besides the state actor can also be included among these qualities (Özel and İnaltekin, 2018: 5).

There are also different views that hybrid warfare is a completely new form of warfare, and therefore traditional theories of warfare have become invalid. However, Karaosmanoğlu, who investigated the differences and opposing views in the comparison of traditional and modern warfare in detail, stated that the traditional conceptualization attributed to Karl von Clausewitz is largely accepted (Karaosmanoğlu, 2011: 18). According to Karaosmanoğlu, changes in modern warfare do not affect its fundamentals. Similarly, Mansoor states that it is not the nature of war that has changed, but "the way of waging war". Karabulut states that some events in history, such as the activities of the British in the Ottoman territories during World War I and the clashes between the British, French, and Spanish during the Napoleonic Wars, involved similar tactics. Therefore, he argues that these events confirm the claims of Karaosmanoğlu and Mansoor (Karabulut, 2016: 28).

As a result, hybrid warfare, instead of being called a completely new type of warfare, has strongly started to find its place in the literature as a different type of warfare. Thanks to the opportunities brought by technology and temporal progress, the diversity and effectiveness of the methods applied have increased. This situation shows that hybrid wars have evolved and emerged in a different way from the traditional understanding of warfare. While hybrid wars represent a complex mix, they stand out with their unpredictability and the combination of various elements (Karabulut, 2016: 26).

Hybrid warfare is a concept that can be associated with or considered as an advanced version of the concept of "limited warfare" that has been used frequently in the literature. However, the main difference of hybrid warfare can be stated as the instrumental use of hard power elements, especially military power, instead of soft power types in limited war. The "hybrid" characterization of warfare makes it a concept with many more elements than limited warfare. It is important to include soft power elements in the equation along with hard power elements. This involves a broader perspective (Karabulut, 2016: 26).

Adjectives such as guerrilla geopolitics, unconventional, non-linear, proxy or political can be used interchangeably to refer to similar or identical issues. Among these different terms, hybrid warfare seems to be more common, especially in light of Russia's practices during the 2014 Ukraine crisis. This term is more accepted than other terms (Karabulut, 2016: 26).

2. Russia's "Hybrid War" and the Example of Ukraine

Russia sees hybrid warfare as the West's strategy to limit Russia's influence, which includes conflicts against Russia both in countries such as Syria and Ukraine and in areas such as the Covid-19 vaccine and the Eurovision Song Contest (Suchkov, 2021). Russia calls the changing strategic environment as new generation warfare, non-linear warfare, and modern warfare. However, despite the different nomenclatures, Western countries and Russia point to similar situations in the international environment (Arslan, 2023: 339).

In 2010, Russia's Military Doctrine was adopted and this official text included the characteristics of modern wars. It mentioned the use of non-military resources such as information warfare in combination with military power (Sadıkoğlu, 2022: 37).

With the outbreak of armed conflicts in Ukraine in 2014, the article written by Valery Gerasimov, Russia's Chief of General Staff, in 2013 came to the fore. Gerasimov's article was essentially based on a speech he had previously delivered at the Academy of Military Sciences. In this speech, Gerasimov mentioned that, especially in the conflicts in the Middle East, the distinction between war and peace has become blurred and the gap between the army and special forces has narrowed, and he gave examples of successes achieved by using military and non-military methods together. He also cited political, economic, communicative or informational, humanitarian and other fields as non-military methods. He noted that these activities can be supplemented by covert operational activities, especially under the name of "peace support". He particularly emphasized the use and care of today's modern communication and technology tools, and stated that in addition to all efforts, these can be even more effective through the use of some armed elements placed within the settled population (Karabulut, 2016: 28).

In his article published on February 27, 2013, Gerasimov argues that the rules of warfare have changed in the current political environment, and that non-military means have become effective in achieving political and strategic goals, in some cases even surpassing the power of weapons. According to Gerasimov, modern military strategy focuses on the massive use of political, economic, informational, humanitarian and all non-military means in coordination with the protest potential of the population. These are supported by covert military means. With asymmetric actions, the enemy's superiority in armed conflict is eliminated. For example, groups opposed to the country's leadership and operational special units are used in conjunction with Information Technology (IT) activities and tools to establish a permanent active front on the territory of the enemy state (Gerasimov, 2013).

The 2014 Russian Military Doctrine of the Russian Federation also defines the nature and characteristics of modern warfare, which includes the integrated use of military force, political, economic, information and other non-military measures, implemented primarily through the comprehensive use of the protest potential of the population and special operations forces (Russia's Military Doctrine, 2014). Russia's military doctrine is based on two fundamental principles. These are: War is everywhere (spatial) and it is not only about occupying a place but also about creating the desired effect at all times and in all dimensions (temporal) (Karabulut, 2016: 33). In 2014, Russia started to use the mentioned tools in Ukraine together in the changing environment.

In fact, protests started in November 2013 when Ukraine's President Yanukovich announced that he would not take part in the ongoing association talks with the EU (European Union). With the increase in popular protests, a crisis emerged in Ukraine, which then spread to Crimea. Russia intervened in the crisis, annexed Crimea and supported separatist actions in the Donbas region of eastern Ukraine, where the majority of the inhabitants are ethnic Russians. Thus, a 'total' hybrid war has emerged in Ukraine. Countries, international organisations and armed forces, directly or subsequently involved in the conflict, have chosen to use various forces and asymmetric methods instead of conventional approaches. The current tension has evolved in various directions between NATO-Ukraine-Russia (Karabulut, 2016: 34).

In addition to weakening and overthrowing the pro-Western administration in Ukraine, Russia aimed to bring a pro-Russian administration to power in the future, to limit or prevent Ukraine's relations with the West, to gain public support from Russian citizens and other Russian-speaking countries, and to create some suspicion in Western public opinion. In order to achieve these goals, Putin's Russia used a harmonious combination of hard and soft power factors (Karabulut, 2016: 34).

The events of 2014 between Ukraine and the Russian Federation are considered as a concrete expression of the example of 'hybrid warfare'. This operation carried out by the Russian Federation has shown that states can easily apply hybrid warfare tools with all their elements in asymmetric operations. According to Josan and Voicu, it has also revealed some defining characteristics of the hybrid war:

1. The state of war as defined in international law (jus ad bellum) is no longer declared,

2. The use of armed civilians and armed groups formed by them during operations and conflicts,

3. Obstruction of military units by so-called civilian protesters,

4. Use of asymmetric and indirect methods,

5. Organisation of operations in all spatial dimensions (land, sea, air and cyberspace) simultaneously,

6. Utilising media and information technology (Josan and Voicu, 2015: 51)

If we look at it in more detail, of course, Russia did not declare war, and even denied that the actions carried out there were related to it. In this context, proxy war is a step in Russia's hybrid war in Ukraine. In order to make it difficult to attribute their actions to Russia, "little green men" wearing uniforms without any insignia, with their faces covered, speaking Russian, and using Russian weapons played important roles in Crimea and Donbas. They were alleged to be elements of the Spetsnaz regiment of the GRU (Glavnoje Razvedyvatel'noje), the military intelligence agency of the Russian Federation (Reeves and Wallace, 2015: 393; Kurtdarcan, 2014: 122). These little green men neutralized Ukrainian law enforcement and military forces in Crimea by confining them to their own facilities and bases (Kurtdarcan, 2014: 119), and took part in the seizure of important buildings and facilities, but disappeared when militias and local troops arrived. In addition, Moscow's contracted mercenaries from Serbia, Moldova, Russia and Ukraine were found to have taken part in the protests, and Wagner was also found to have taken part in clashes in Donbas (Costea, 2020: 18-19).

Information warfare constituted another step of hybrid war waged by Russia in Ukraine. In this way, Moscow legitimised the annexation of Crimea by persuading the Russian-speaking minority and sympathisers in Crimea without resistance and the use of force. In this framework, propaganda broadcasts were made by both state radio and television channels and digital channels disguised as free press. In Crimea, Ukrainian channels were blocked and Russian channels started to be watched instead, Russia controlled telecommunications, including the internet, and the public perception was created that the events were prevented by Russia and that the Ukrainian government was incapacitated. As mentioned before, Russia's information warfare was not limited to the people of the region but also targeted the international public opinion. In this framework, political organisations, some non-governmental organisations, politicians, businessmen, journalists, writers, trolls, commentators and even paid internet commentators supported by the Kremlin were used (Karabulut, 2016: 35; Aras and Yıldırım, 2022: 505). According to Spiegel, Russia spent 100 million Euros annually on Russian media abroad to influence public opinion in the West (Spiegel, 2014). In 2016, it was claimed that RT alone had a budget of close to 250 million dollars (JBANC, 2017).

Russian propaganda described the Ukrainian government as a 'fascist junta' (Kofman et.al., 2017: 13), claimed that the revolution in Ukraine was a CIA-funded coup d'état (RT, 2015a), and frequently conveyed the message that the leaders in Kiev were acting in the interests of the US and other Western states (Kofman et.al., 2017: 80). It has also portrayed Ukraine as a failed, corrupt, divided state (RT, 2017a) and the poorest country in Europe (RT, 2017b). Reports have been heavily circulated that separatist demands are increasing in southeastern Ukraine (RT, 2015b) and that the Ukrainian army was no longer able to fight, with many soldiers leaving the army (Sputnik, 2015), aiming to influence both the public and the soldiers in the Ukrainian army (Aras and Yıldırım, 2022: 507). The EUvsDisinfo database, created by a team of experts in communication, journalism, social sciences, and Russian studies brought together by the EU, contains over 15,000 examples of disinformation allegedly linked to the Kremlin from 2015 (EUvsDisinfo).

At this point, the intelligence war should also be mentioned. It was claimed that the Kremlin used the Foreign Intelligence Service (SVR), -the military intelligence service- the Main Intelligence Directorate (GRU) and -the successor of the KGB- the Federal Security Service (FSB), to spread despair and disinformation, encourage secession and disrupt command and communication lines (Galeotti, 2015: 2). Furthermore, it was also revealed that Russia's Federal Security Service (FSB) has significant influence within Ukrainian National Security Service (SBU). In March 2015, Ukrainian President Petro Poroshenko announced that 80% of SBU officers were FSB agents. After the revolution in February 2014, the SBU Director fled to Russia, 90% of SBU officers in Crimea defected to the Russian side, and many SBU officers in Donetsk and Luhansk joined the separatists (Costea, 2020: 22). There are also allegations that the GRU and the FSB carried out numerous sabotage attacks against transportation and strategic infrastructure on Ukrainian territory, assassinations of dissidents and intelligence officers, bomb attacks to create chaos, and false bomb threats (Costea, 2020: 27-31).

While there is no conclusive evidence of Russia's involvement in cyberattacks against Ukraine, there are strong indications that such attacks were financed by Moscow. Through these cyber attacks, Russia undermined Ukraine's legitimacy and authority while disrupting the communication between Ukraine's political and military units and its ability to operate. After 2015, these cyber attacks were expanded. During key events such as the Maidan protests and the Russian forces' operation in Crimea, intensive cyber attacks were carried out for purposes such as disrupting communication and intercepting secret plans of the Ukrainian administration. Messages were sent to Ukrainian military personnel encouraging them to defect from the army. Another cyber attack attributed to Russia was carried out in December 2015 on Ukraine's power grid. More than 220,000 Ukrainians were left without electricity for 1 to 6 hours, but distribution centers could not be restored for a long time (Connel and Vogler, 2016: 19). However, it should be noted that Ukraine has also started to take important steps in cybersecurity and cyber warfare after the annexation of Crimea and the start of the conflict in Eastern Ukraine. In 2019, a Ministry of Digital Transformation was established. Before the Russian occupation began, the Ministry created its own Red Team, which continuously crash-tested state information systems to find vulnerabilities (Fedorov, 2023). And when the invasion began, Minister Mykhailo Fedorov announced the creation of the Ukrainian IT army as an international volunteer force. He called on volunteers to join the Telegram channel of the IT army, which was created to neutralize Russian information propaganda (Soesanto, 2023). It was announced that this army hacked the websites of the Moscow Stock Exchange, Sberbank, FSB, The President of the Russian Federation, the Government of the Russian Federation, the State Duma (Government Portal, 2022). Today Ukraine is also running a hybrid war in cyberspace.

Humanitarian support and assistance can be employed as an another non-violent strategy as part of hybrid warfare Russia used in Ukraine. This tactic exploits the humanitarian situation created by conflict and instability, and can provoke counter-reactions if criticized or blocked. With the spread of popular unrest in the Donbas region to other parts of the country, the Russian Federation engaged in such humanitarian support by sending convoys of aid to areas where the rebels were active. Such activities are effective strategies aimed at embarrassing the adversary side of the operation in front of domestic and foreign public opinion. For this reason, a number of researchers and authors describe the activities of non-violent public protests and humanitarian aid movements with terms such as jamming maneuver or indicative action (Sorensen and Martin, 2014: 80).

After the invasion began, pro-Russian communication channels frequently conveyed the message that the Ukrainian army was bombing its own people, and anti-Ukrainian propaganda and information originating from Russia was broadcast, especially from television and radio towers captured in eastern Ukraine (Gibbons-Neff and Yermak, 2022). For example, on February 25, 2022 when a hospital was attacked in Mariupol, Russia claimed that it was a provocation by Ukraine. Again, on April 8, 2022, the Kramatorsk Train Station attack, which killed fifty civilians and injured around 100, was carried out by Ukraine. Russia claimed that the Tochka missile used in both attacks was used by Ukraine. However, social media evidence shows that the Tochkas, which Russia has decommissioned, are still used in Ukraine. Russia also launched an intense disinformation process in Bucha, denying the attacks and claiming that civilian casualties were the results of operations carried out by Western states to sabotage peace talks and pave the way for additional sanctions (Arslan, 2023: 347).

Another example of information warfare, it has been reported that since 2014, messages containing threats against Ukrainian military personnel, including private information such as their names, families and residences, have been transmitted through channels such as Whatsapp and Telegram. But by 2022, most of this information was outdated (Giles, 2023).

As mentioned earlier, Russia had announced the launch of this special operation to protect Ukrainians and Russian citizens from the persecution of the Nazi-ideologized leadership (TASS, 2023). It used this argument to maintain public support for the intervention. In the third year of the war, the message continues to be that Russia will do everything to suppress and eradicate Nazism (The Moscow Times, 2024).

In 2014, Spetsnaz units played crucial roles. In the period after 2022, Spestnaz forces were used more in a conventional context as the precursor units of conventional forces. As part of the Russian military's modernization process, the number of conscripts in conventional units has been reduced, while the number of professional soldiers, particularly in Spetsnaz units, has been increased. Given the realization that the invasion, which began in February 2022, could not be accomplished quickly and was being conducted over a larger geographical area compared to the 2014 phase, the Russian military began to meet a significant portion of the emerging conventional force needs on the ground with Spetsnaz units (Arslan, 2023: 345). Although unconfirmed, there have been reports and statements from both sides of the war that Russia is using foreign fighters in Ukraine. In March 2022, Russia announced that it would allow the deployment of 16,000 foreign fighters from the Middle East to fight in Ukraine (Chehayeb, 2022). In February 2024, the Ukrainian military intelligence service (GUR) revealed that Russia had trained a group of 1,000 Syrian mercenaries near Aleppo and published a list of more than 100 Syrian mercenaries hired by Russia to fight in Ukraine (Court, 2024). According to CNN, Russia has also recruited up to 15,000 Nepalese to fight in the war in Ukraine (Pokharel, et.al., 2024).

Although the activities of private military security companies are prohibited under the laws of the Russian Federation, Wagner Group took part in frontline combat for the first time during the war that began in February 2022 (Öztopal, 2023: 63-69). It played a direct role in significant developments until the uprising in June 2023 (BBC, 2023). Apart from these, far-right groups such as the Russian Imperial Movement and Rusich have also actively been involved in the war. In addition, the federated states of the Russian Federation are also involved in the war with their own volunteer battalions/regiments (Arslan, 2023: 346)

Conclusion

The increase in the military expenditures of states demonstrates that states continue to attach importance to hard power elements. However, recent developments indicate that states are increasingly beginning to use various other elements alongside military power. A review of the literature reveals that this is not a new situation. However, especially technological developments transforming contemporary warfare. The most widely used concept to describe this transformation is 'hybrid warfare'.

While there is no universally agreed-upon definition of the concept, hybrid warfare can be described as the conduct of conflicts by states and other actors through complex strategies that incorporate non-military elements. Based on observed examples, certain elements of hybrid warfare can be identified. In this type of warfare, civilians, mercenaries, private armed forces or armed civilians are used together with military force to achieve the objectives. Various tools such as disinformation, espionage, cyber-attacks, media campaigns, humanitarian aid, etc. are used for various purposes such as intimidating the enemy, demoralizing the public, and fracturing allies.

These tools, especially those enabled by technological advances, make it possible to inflict serious damage on the other side even without any loss of life or costly military operations. At the same time, it also allows those who are weaker in conventional terms to achieve success against those who are stronger. It can be argued that Russia has tried to take advantage of these advantages of hybrid warfare in its operations against Ukraine since 2014. Russia's 2014 intervention is analyzed as a concrete example of hybrid warfare. In this intervention, Russia effectively used hybrid elements such as information warfare, proxy wars and cyber attacks. At the time, it can be said that Russia achieved its objectives such as annexing Crimea and preventing Ukraine's EU and NATO membership.

Its intervention in 2022, despite the widespread use of military force, also includes elements of hybrid warfare. In Ukraine, Russia is at war not only with Ukraine but also with Western states. It cannot be said that it has the possibility to emerge victorious from this war with its conventional power. As a matter of fact, cyber attacks and information warfare started even before the invasion began. Russia has also used mercenaries and special forces in conflicts with the tools brought by the digital age. The war is still ongoing and Russia has not achieved the objectives it had set at the beginning of the operation. However, it has led to the emergence of a lot of examples and literature on hybrid warfare.

In conclusion, hybrid warfare is an important concept to evaluate contemporary conflicts. As time progresses, the scope of hybrid warfare will expand as technology advances and states and other actors rely more on these tools to defeat their opponents. For example, artificial intelligence (AI) and machine learning are likely to make cyberattacks and disinformation campaigns more sophisticated. Advances in communication technologies could also increase the impact of such campaigns. Social media will continue to play an important role in spreading fake news or manipulative content in the future. Therefore, it will not be surprising that in the coming years, hybrid warfare tactics will cause inter-state crises and even conflicts, increase mistrust between states, complicate international cooperation and, of course, negatively affect global security.

References

Aras, Harun, Yusuf Yıldırım. (2022). "Rusya'nın 2014 Ukrayna Krizi'ndeki Hibrit Savaş Stratejisi". *Yönetim ve Ekonomi*. 29 (3): 499-516.

Arslan, Hasan. (2023). "Hibrit Savaş Perspektifi'nden Rusya'nın 2022 Yılı Ukrayna Müdahalesi". *Savunma Bilimleri Dergisi*. 43(2): 331-356.

Bachmann, Sacha, Hakan Gunneriusson. (2015). "Hybrid Wars: The 21st Century's New Threats to Global Peace and Security". *Scientia Militaria - South African Journal of Military Studies*. 43 (1): 77-98.

Bateman, Jon. (16 December 2022). "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications". Paper, Carnegie Endowment for International Peace, Washington, DC, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impactsinfluences-and-implications-pub-88657/ 11.05.2024.

BBC. (14 Temmuz 2023). "ABD'ye Göre Wagner Artık Ukrayna Savaşında Önemli Rol Oynamıyor". https://www.bbc.com/turkce/articles/cv217889we1o#:~:text=ABD'ye%20g%C3%B6re%20Wagner%20art%C4%B1k%20Ukrayna%20sava%C5%9F%C4%B1nda%20%C3%B6nemli%20rol%20oynam%C4%B1yor&text=ABD%20Savunma%20Bakanl%C4%B1%C4%9F%C4%B1%20(Pentagon)%20S%C3%B6zc%C3%BCs%C3%BC,%C3%B6nemli%20bir%20rol%20oynamad%C4%B1%C4%9F%C4%B1n%C4%B1%20s%C3%B6yledi/ 11.05.2024.

Chehayeb, Kareem. (1 April 2022). "In Syria, Russia Leads Effort to Recruit Fighters for Ukraine". *Al Jazeera*, https://www.aljazeera.com/news/2022/4/1/in-syria-moscow-leads-effort-to-recruit-fightersfor-ukraine/ 11.05.2024.

Connel, M. ve Vogler, S. (2016). "Russia's Approach to Cyber Warfare". *Center for Naval Analyses (CNA) Occasional Paper series*.

Costea, Catalin Alin. (2020). *Rusya'nın Ukrayna'daki Hibrid Savaşı (2014-2018)*. Seta Yayınları.

Erol, Mehmet Seyfettin, Şafak Oğuz. (2015) "Hibrit Savaş Çalışmaları ve Kırım'daki Rusya Örneği". *Gazi Akademik Bakış*. 9 (17): 261-277.

EUvsDisinfo. Database. https://euvsdisinfo.eu/disinformation-cases/?view=grid/ 15.05.2024.

Fedorov, Mykhailo. (2023). "Lessons from Ukraine in the Heat of an Ongoing Hybrid War". https://digitalfrontlines.io/2023/05/31/lessons-from-ukraine-in-the-heat-of-an-ongoing-hybrid-war/ 26.06.2024.

Fairclough, Graham. (2018). "Tank, Fare ve Rekabetçi Pazar: Hibrit Savaşa Yeni Bir Bakış". Ed. Yücel Özel ve Ertan İnaltekin. *Savaşın Değişen Modeli: Hibrit Savaş*. İstanbul: Milli Savunma Üniversitesi Basımevi: 7-21.

Furgacz, Przemysław. (2015). "The Russian-Ukranian Economic War". *Ante Portas – Studia nad Bezpieczeństwem*. 2(5): 115-130.

Galeotti, Mark. (16 April 2015). "'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't". *E-International Relations*. https://www.e-ir.info/pdf/55375/ 10.05.2024.

Gerasimov, Valery. (27 February 2013). "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations". *Military-Industrial Kurier*. çev. Robert Coalson: 23-29.

Gibbons-Neff, Thomas, Natalia Yermak. (17 June 2022). "Russians Breached This City, Not With Troops, but Propaganda". *New York Times*.

https://www.nytimes.com/2022/06/17/world/europe/ukraine-russia-propaganda.html/ 11.05.2024.

Giles, Keir. (14 December 2023). "Russian Cyber and Information Warfare in Practice". https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/04-information-confrontation-human-effects/ 11.05.2024.

Government Portal. (28 February 2022). "Ministry of Digiral Transformation: IT Army Blocks Russian Sites in a Few Minutes - the Main Victories of Ukraine on the Cyber Front". https://www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti/ 26.06.2024.

Gürcan, Metin. (2012). "Savaşın Evrimi ve Teorik Yaklaşımlar". Ed. Atilla Sandıklı. *Teoriler Işığında Savaş, Barış ve Çatışma Çözümleri*. İstanbul: Bilgesam Yayınları: 70-129.

Hoffman, Frank. (2009). "Hybrid Warfare and Challenges". *Joint Forces Quarterly*. 52: 34-39.

Hoffman, Frank. (28 Temmuz 2014). "On Not-So-New Warfare: Political Warfare vs Hybrid Threats", *War on the Rocks*, http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ 03.05.2023.

JBANC (The Joint Baltic American National Committee, Inc.) (30 June 2017). "The Undeniable Deniable Threats of Russian Subversion". https://jbanc.org/2017/06/30/the-undeniable-deniable-threats-of-russian-subversion/ 2.04.2024.

Johnson, Robert. (2018). "Hibrit Tehdidin Tarihsel Evrimi", Ed. Yücel Özel ve Ertan İnaltekin. *Savaşın Değişen Modeli: Hibrit Savaş*. İstanbul: Milli Savunma Üniversitesi Basımevi: 1-7.

Josan, Andrei, Cristian Voicu. (2015). "Hybrid Wars in the Age of Asymmetric Conflicts". *Review of the Air Force Academy*. 28 (1): 49-52.

Karabulut, Ali Nedim. (2016). "Eski Savaş, Yeni Strateji: Rusya'nın Yirmibirinci Yüzyıldaki Hibrit Savaş Doktrini ve Ukrayna Krizi'ndeki Uygulaması". *Uluslararası İlişkiler*. 13 (49): 25-42.

Karaosmanoğlu, Ali. (2011). "Yirmibirinci Yüzyılda Savaşı Tartışmak: Clausewitz Yeniden". *Uluslararası İlişkiler*. 8 (29): 5-25.

Kayalar, Volkan (28 Ekim 2022). "Fransa'nın Ukrayna Büyükelçisi Etienne de Poncins'in Zelenski'yi Eleştirerek İstifa Ettiği iddiası". https://teyit.org/analiz/fransanin-ukrayna-buyukelcisi-etienne-de-poncinsin-zelenskiyi-elestirerek-istifa-ettigi-iddiasi/ 25.06.2024.

Kofman, Michael, Katya Migacheva and Brian Nichiporuk et.al. (2017). *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. RAND Corporation. Santa Monica.

Korhonen, Outi. (2015). "Deconstructing the Conflict in Ukraine: The Relevance of International Law to Hybrid States and Wars". *German Law Journal*. 16 (3): 452-478.

Kurtdarcan, Bleda R. (2014). "Maskirovka: Rusya'nın Ukrayna'ya Müdahalesinin Yöntem ve Hukuki Gerekçelendirmelerinin İncelenmesi". *Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi*. 9 (121): 117-149.

Lewis, James Andrew. (16 June 2022) 'Cyber war and Ukraine', CSIS, https://www.csis.org/analysis/cyberwar-and-ukraine/11.05.2024.

Mansoor, Peter. (2012). "Introduction: Hybrid Warfare in History". Ed. Williamson Murray ve Peter Mansoor. *Hybrid Warfare:Fighting Complex Opponents from the Ancient World to the Present*. New York: Cambridge University Press. 1-10.

Mello, Patrick. (2010) "In Search of New Wars: The Debate about a Transformation of War". *European Journal of International Relations*. 20 (10): 1-13.

Microsoft Special Report. (2022). *An Overview of Russia's Cyberattack Activity in Ukraine*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd/ 11.05.2024.

O'Carroll, Lisa. (3 May 2023). "Germany Summons Russian Envoy over 2023 Cyber-attacks". *The Guardian*. https://www.theguardian.com/world/article/2024/may/03/germany-says-russians-behind-intolerable-cyber-attack-last-year/ 12.05.2024.

Oxford Synonym Dictionary. (2006). New York.

Özel, Yücel, Ertan İnaltekin. (2018). "Giriş", Ed. Yücel Özel ve Ertan İnaltekin. *Savaşın Değişen Modeli: Hibrit Savaş*, İstanbul: Milli Savunma Üniversitesi Basımevi: V-VI.

Özer, Yusuf. (2018). "Savaşın Değişen Karakteri: Teori ve Uygulamada Hibrit Savaş". *Güvenlik Bilimleri Dergisi*. 1 (7): 29-56.

Öztopal, Mustafa Kemal. (2023). "Özel Güvenliğin Uluslararasi Sorunlar Üzerindeki Etkisi: Rusya-Ukrayna Savaşinda Wagner Grubu Örneği". *Düşünce Dünyasında Türkiz*. 14 (66): 53-74.

Pokharel, Sugam, Matthew Chance and Mihir Melwani. (11 February 2024). "Russia has recruited as many as 15,000 Nepalis to fight its war. Many returned traumatized. Some never came back". *CNN*. https://edition.cnn.com/2024/02/10/asia/nepal-fighters-russia-ukraine-families-intl-cmd/ 11.05.2024.

Reeves, S. R. ve Wallace, D. (2015). "The Combatant Status of the "Little Green Men" and Other Participants in the Ukraine Conflict". *International Law Studies,* (91): 362-401.

RT. (19 February 2015a). "Brokering Power: US Role in Ukraine Coup Hard to Overlook". https://www.rt.com/news/233439-us-meddling-ukraine-crisis/ 10.05.2024.

RT. (28 August 2015b). "Balkanization? Southeast Ukrainian Region Demands Greater Autonomy". https://www.rt.com/news/313709-ukraine-zaporozhye-autonomy-draft/ 10.05.2024.

RT. (30 February 2017a). "Three Strikes and You're Out: Ukraine is a Divided, Failed, Rogue State". https://www.rt.com/op-ed/377978-ukraine-rogue-failed-state/ 10.05.2024.

RT. (11 December 2017b). "Ukraine is Europe's Poorest Nation with $220 Average Monthly Wage", https://www.rt.com/business/412692-ukraine-poorest-country-europe/ 10.05.2024.

Russia's Military Doctrine. (2014). https://thailand.mid.ru/en/o_rossii/vneshnyaya_politika/voennaya_doktrina_rf/ 24.06.2024.

Sadıkoğlu, Kübra. (2022). *Russian Military Doctrines Since 2000: An Analysis From Military Security Perspective*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul Sabahattin Zaim Üniversitesi Lisansüstü Eğitim Enstitüsü. İstanbul.

Segal, David. (2018) "Hibrit Savaşın Sosyolojik Boyutu". Ed. Yücel Özel ve Ertan İnaltekin. *Savaşın Değişen Modeli: Hibrit Savaş*. İstanbul: Milli Savunma Üniversitesi Basımevi: 47-56.

Soesanto, Stefan. (2023). *Ukraine's Counter-Hybrid Campaigns in Cyberspace*. The Hague Centre for Strategic Studies.

Sorensen, Majken ve Brian Martin. (2014) "The Dilemma Action: Analysis of an Activist Technique". *Peace & Change*. 39 (1): 73-100.

Spiegel (30 May 2014). "How Russia Is Winning the Propaganda War". https://www.spiegel.de/international/world/russia-uses-state-television-to-sway-opinion-at-home-and-abroad-a-971971.html/ 01.04.2024.

Sputnik. (21 June 2015). "Farewell to Arms: Over 10,000 Soldiers Desert Ukrainian Army". https://sputnikglobe.com/20150621/1023647747.html/ 10.05.2024.

TASS, (12 March 2023). Decision Taken on Denazification, Demilitarization of Ukraine - Putin, https://tass.com/politics/1409189/11.05.2024.

The Moscow Times. (27 January 2024). "Putin Repeats Ukraine Nazi Claims at Leningrad Siege Memorial". https://www.themoscowtimes.com/2024/01/27/putin-repeats-ukraine-nazi-claims-at-leningrad-siege-memorial-a83877/ 11.05.2024.

The United States Army Special Operations Command, (2016). *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine: 2013–2014*. North Carolina: USASOC.

Tian, Nan, Diego Lopes Da Silva, Xiao Liang, Lorenzo Scarazzato. (2024). *Trends in World Military Expenditure, 2023*. SIPRI Fact Sheet. https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf/ 15.05.2024.

Türk Dil Kurumu (TDK). (2018). Türkçe Sözlük. Ankara: Türk Tarih Kurumu Basım Evi.

Yalçınkaya, Haldun, Tamer Türkeş. (2008). "Yirmi Birinci Yüzyılda Çatışma Alanlarında Görülen Yeni Unsurlar". *Güvenlik Stratejileri Dergisi*. 7 (7): 55-89.

Yıldız, Gültekin. (2018). "Hibrit Savaş Ne Kadar Post-moderndir? Avrasya Askeri Tarihine Yeniden bir Bakış". Ed. Yücel Özel ve Ertan İnaltekin. *Savaşın*

Değişen Modeli: Hibrit Savaş. İstanbul: Milli Savunma Üniversitesi Basımevi: 21-29.

Uzun, Mehmet Cengiz. (2018). "Hibrit Savaşın Hukuki Boyutları", Ed. Yücel Özel ve Ertan İnaltekin. *Savaşın Değişen Modeli: Hibrit Savaş*. İstanbul: Milli Savunma Üniversitesi Basımevi: 29-47.

Walker, Robert G. (1998). *Spec fi: The United States Marine Corps and Special Operations*. Yayımlanmamış Yüksek Lisans Tezi. ABD Deniz Kuvvetleri İhtisas Okulu.

Waltz, Kenneth, (2001). *Man, the State and War: A Theoretical Analysis*, (3. baskı), New York: Columbia University Press.

Watling, Jack, Nick Reynolds. (2022). *The Plot to Destroy Ukraine*. The Royal United Services Institute, https://static.rusi.org/special-report-202202-ukraine-web.pdf /11.05.2024.

Watling, Jack, Oleksandr V. Danylyuk, Nick Reynolds. (2023). *Preliminary Lessons from Russia's Unconventional Operations during the Russo-Ukrainian war, February 2022–February 2023*, The Royal United Services Institute, https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.pdf/ 11.05.2024.