

DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF INTERNATIONAL RELATIONS
INTERNATIONAL RELATIONS PROGRAM
MASTER'S THESIS

**HYBRID WARFARE: A COMPARATIVE ANALYSIS OF
ISIS AND RUSSIAN CASES**

Emre TANIK

Supervisor
Prof. Dr. ALİ ŞEVKET OVALI

2024

DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF INTERNATIONAL RELATIONS
INTERNATIONAL RELATIONS PROGRAM
MASTER’S THESIS

**HYBRID WARFARE: A COMPARATIVE ANALYSIS OF
ISIS AND RUSSIAN CASES**

Emre TANIK

Supervisor
Prof. Dr. ALİ ŞEVKET OVALI

İZMİR – 2024

APPROVAL PAGE



DECLARATION

I hereby declare that this master thesis titled as “Hybrid Warfare: A Comparative Analysis of ISIS And Russian Cases” has been written by myself in accordance with the academic rules and ethical conduct. I also declare that all materials benefited in this thesis consist of the mentioned resources in the reference list. I verify all these with my honour.

Date

04/01/2024

Name SURNAME

Signature

XXXXXXXXXX

ABSTRACT

Master's Thesis

Hybrid Warfare: A Comparative Analysis of ISIS and Russian Cases

Emre TANIK

Dokuz Eylül University

Graduate School of Social Sciences

Department Of International Relations

International Relations Program

This study investigates the notion of hybrid warfare and its importance in comprehending contemporary conflicts. Furthermore, it offers a comprehensive examination of the components of hybrid warfare and the distinct ways different actors employ and interpret these elements to further their political objectives.

The study provides a comprehensive examination of the hybrid warfare strategies employed by Russia, a nation-state, and ISIS, a non-state actor, through a comparative analysis. It examines similarities and differences between the two actors, focusing on the fact that state and non-state actors can utilize hybrid warfare.

This study emphasizes the crucial significance of hybrid warfare within contemporary conflict conditions. It also examines the efficacy of hybrid warfare strategies employed by Russia and ISIS and the potential risks these strategies present to international security. Furthermore, the study identifies these potential dangers and investigates how they might be identified and reduced.

Keywords: Hybrid Warfare, War Theories, Contemporary Conflicts, Russia, ISIS, Ukraine.

ÖZET

Yüksek Lisans Tezi

Hibrit Savaş: IŞİD ve Rusya Vakalarının Karşılaştırmalı Analizi

Emre TANIK

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Uluslararası İlişkiler Anabilim Dalı

İngilizce Uluslararası İlişkiler Programı

Bu çalışma hibrit savaş kavramının ne olduğunu ve modern çatışmaların anlaşılmasında nasıl bir öneme sahip olduğunu incelemektedir. Ayrıca tez hibrit savaşın bileşenlerinin neler olduğu ve bu bileşenlerin farklı aktörler tarafından farklı şekillerde yorumlanarak kendi politik ajandaları kapsamındaki kullanım şekillerine dair detaylı bir analiz sunar.

Bu çalışma bir devlet aktörü olan Rusya ile devlet dışı aktör olan IŞİD'in hibrit savaş kampanyaları üzerine durarak karşılaştırmalı bir analiz sunar. Bu analizler kapsamında her iki aktörün benzerlikler ve farklılıklarına değinir. Bu benzerlik ve farklılıklar incelenirken devlet ve devlet dışı aktörlerin hibrit savaşı kullanabileceğinin altı çizilir.

Bu çalışma, hibrit savaşın modern çatışma ortamındaki kritik rolünü ortaya koymaktadır. Rusya ve IŞİD örnekleri hibrit savaş taktiklerini etkinliğini ve kullanılan taktiklerin uluslararası güvenliğe nasıl tehditler oluşturabileceği incelenir. Ayrıca çalışmada sadece tehditlerin neler olduğu değil, bunların nasıl fark edileceği ve önlem alınabileceğinin incelenmesi yapılır.

Anahtar Kelimeler: Hibrit Savaş, Savaş Teorileri, Güncel Çatışmalar, Rusya, IŞİD, Ukrayna.

HYBRID WARFARE: A COMPARATIVE ANALYSIS OF ISIS AND RUSSIAN CASES

CONTENTS

APPROVAL PAGE	ii
DECLARATION	iii
ABSTRACT	iv
ÖZET	v
CONTENTS	vi

INTRODUCTION	1
--------------	---

CHAPTER ONE

THE CONCEPTUAL FRAMEWORK OF HYBRID WARFARE

1.1. THE EMERGENCE AND GROWTH OF HYBRID WARFARE CONCEPT	8
1.1.1. The Origins of Hybrid Warfare Concept: Chechen Wars and Hezbollah Case	8
1.1.2. Evolution of the Hybrid Warfare Concept	10
1.1.3. Hybrid Warfare Through Time: An Exploration of Historical Examples	13
1.2. COMPONENTS OF HYBRID WARFARE	17
1.2.1. Military Components of Hybrid Warfare	17
1.2.2. Non-military Components of Hybrid Warfare	20
1.3. HYBRID WARFARE and ITS DISTINCTIVENESS AMIDST OTHER WARFARE CONCEPTS	22
1.3.1. Comparing Non-linear and Hybrid Warfare: Key Distinctions	22
1.3.2. Comparing Limited and Hybrid Warfare: Key Distinctions	23
1.3.3. Comparing Asymmetric and Hybrid Warfare: Key Distinctions	24
1.3.4. Comparing Compound and Hybrid Warfare: Key Distinctions	25
1.3.5. Comparing Fourth-Generation and Hybrid Warfare: Key Distinctions	26
1.4. THE REASONS FOR RESORTING TO HYBRID WARFARE	28

1.4.1. Military and Technological Dominance of Western Countries	29
1.4.2. Low-cost Approach of Hybrid Warfare	30
1.4.3. Reduced Need for Traditional Large Armies	31
1.4.4. Anonymity Advantage of Hybrid Warfare	31
1.5. DEBATES ON HYBRID WARFARE	33

CHAPTER TWO

RUSSIAN HYBRID WARFARE: CRIMEA AND EAST UKRAINE CASES

2.1. RUSSO-UKRAINIAN TENSIONS: UNRAVELING THE GEOPOLITICAL STRIFE	37
2.2. COMPARISON OF WESTERN AND RUSSIAN PERSPECTIVES ON THE UKRAINIAN WAR: AN ANALYSIS OF THE GERASIMOV DOCTRINE: WHY DOES RUSSIA WAGE A HYBRID WARFARE?	38
2.3. EXPLORING HYBRID WARFARE METHODS EMPLOYED BY THE RUSSIAN FEDERATION IN THE UKRAINE CRISIS	42
2.3.1. The Role of Russia's Cyberspace Activities in Conducting Hybrid Warfare: An Analysis of Tactics, Techniques, and Strategies	42
2.3.1.1. Information Warfare and Disinformation Campaigns	42
2.3.1.2. Propaganda	44
2.3.1.3. Intelligence Activities	45
2.3.1.4. Hacker Attacks	47
2.3.2. Economic Pressure and Ukraine's Dependence on Energy	49
2.3.3. Deployment of Conventional Forces	52
2.3.3.1. Russian Military Drills and Construction of Military Buildups on Ukrainian Borders	53
2.3.3.2. Direct Intervention of Russia's Conventional Forces in Ukraine	55
2.3.4. Deployment of Irregular Forces	57

CHAPTER THREE
THE HYBRID WARFARE OF THE ISLAMIC STATE OF IRAQ AND
SYRIA (ISIS)

3.1. THE STRUCTURE OF ISIS	62
3.2. ORIGINS OF ISIS	64
3.3. HYBRID METHODS OF ISIS	68
3.3.1. Activities in Cyberspace	68
3.3.2. Disinformation Campaign and The Manipulation of Information Flow	69
3.3.3. Propaganda	70
3.3.4. Hacker Attacks	72
3.4. CONVENTIONAL FORCES	74
3.5. NON-CONVENTIONAL METHODS: TERRORISM AND INSURGENCY	77

CHAPTER FOUR
A COMPARATIVE ANALYSIS OF HYBRID THREATS: RUSSIAN AND
ISIS CASES

4.1. PSYCHOLOGICAL WARFARE AND PROPAGANDA TOOLS	82
4.2. CYBER ATTACKS	84
4.3. REGULAR FORCES AND TACTICS	86
4.4. ASYMMETRIC TACTICS	88
4.5. NATURAL RESOURCES AS HYBRID MEANS	92
4.6. TERRITORIAL ACQUISITION AND GEOPOLITICAL INFLUENCE	
ASPIRATION	94
CONCLUSION	96
REFERENCES	102

INTRODUCTION

In the middle of the 2000s, hybrid warfare was developed to clarify and better comprehend the intricate nature of contemporary battles. During this time, unconventional warfare tactics and conventional military operations became common. These strategies included economic sanctions, cyberattacks, asymmetric attack plans, social media campaigns, propaganda techniques, information warfare, and psychological warfare. This diverse approach to fighting highlighted the need for a theory that could sufficiently characterize these new kinds of combat (Hoffman, 2007).

“Synchronization” is a crucial idea that needs to be emphasized in this context. These approaches were not used initially on the front lines in the 2000s. Conversely, several of these ideas—like psychological warfare, propaganda, and terrorism—have been applied to conflict for thousands of years. On the other hand, hybrid warfare refers to wars in which these elements are simultaneously deployed at various strategic and tactical levels, working in concert as complementary and mutually reinforcing elements rather than in isolation (Caliskan & Cramers, 2018: 3).

Consideration should also be given to complementary and supporting elements. The hybrid components seen concurrently in conflicts are more than secondary and supportive elements of conventional wars. Hybrid warfare does not replace conventional disputes, nor should the persistence of conventional warfare give the impression that other factors are less significant. A fight that employs both conventional and unconventional elements simultaneously, to differing degrees of importance depending on the stage of the war, is referred to as hybrid warfare (Johnson, 2018: 157-158). In this case, conventional components might be given precedence at some point and then demoted to a supporting role or not employed at all at other times. This is a product of hybrid warfare's adaptability and flexibility.

As a result, the definition of hybrid warfare highlights two essential ideas: adaptation and flexibility. Hybrid warfare's adaptability and flexibility enable the application of novel and unexpected tactics in combat situations. This strategy combines conventional and unconventional aspects of warfare to create complex strategies that defeat the opponent's defenses and yield strategic benefits (NATO,

2016). This adaptability demonstrates how dynamic hybrid warfare is; the strategy can quickly shift and adjust to meet the demands of the battle. For example, one scenario would prioritize cybersecurity measures, while another might focus more on covert intelligence operations or psychological strategies to sway public opinion. The dynamics of the fighting environment are constantly changing due to hybrid warfare's capacity to quickly integrate and modify different military techniques in addition to combining them (Bachmann & Gunneriusson, 2015: 79–91). This versatile and flexible strategy demonstrates why hybrid warfare is so essential in today's theories and practices of conflict.

In this context, Frank Hoffman made some particularly significant contributions to creating the notion of hybrid warfare. By presenting this idea, Hoffman sought to clarify the complexity of conflicts in the early 21st century. His research showed how conventional and unconventional combat tactics can be combined effectively, particularly in the 2006 Israel-Hezbollah War. Hoffman's study addressed the actual applications of hybrid warfare and provided the theoretical underpinnings.

Hoffman underlined that hybrid warfare helps states and non-state actors to create more adaptable and flexible strategies by combining different military and non-military tactics. So, hybrid warfare incorporates unconventional components such as cyber warfare, terrorism, propaganda, and psychological warfare in addition to conventional warfare (Renz & Smith, 2016: 2-4). Hoffman's conceptual framework has opened up new ways for studying and analyzing contemporary warfare and is an invaluable resource for military strategists and decision-makers.

Hoffman's research on hybrid warfare has been essential to comprehending the complexity and diversity of conflicts, particularly those that arise in the early 21st century. His research is crucial for understanding how warfare changes and the difficulties that arise in contemporary conflicts. Due to Hoffman's contributions, hybrid warfare has gained prominence in studying war and conflict.

Even if Hoffman and some scholars' work has brought the concept of hybrid warfare to the forefront, there is still debate on it. The notion has been around for less than 20 years, making it difficult to have a consensus. As a result, the literature has a wide range of diverse viewpoints and assessments on hybrid warfare. Thus, this

study aims to perform a comprehensive literature analysis on hybrid warfare by systematically analyzing different approaches to the hybrid warfare concept and adding to the knowledge on the subject. Therefore, there are four significant chapters to this study.

A detailed overview of the literature is included in the first chapter, which creates the conceptual framework. This chapter clarifies the concept's origins, evolution, history, and emergence. The historical examples offered by certain scholars and researchers who assert that hybrid warfare has been employed at various historical points are then listed.

The chapter details both the military and non-military aspects of hybrid warfare and provides historical and theoretical material. The differences between the hybrid warfare idea and other warfare concepts start to show as the components of hybrid warfare are explained. The distinctions and overlaps between hybrid warfare and other warfare concepts are discussed in this context. Furthermore, the rationales behind players' decisions to employ hybrid warfare instead of conventional warfare and their reasons for doing so are examined. The ongoing discussions in the literature about hybrid warfare are made clear by the end of the first part.

The second chapter of this study thoroughly explores the hybrid warfare methods used by Russia, a state actor, during its annexation of Crimea in 2014 and the conflicts in Eastern Ukraine. This is made possible by the use of the comparison case analysis method. The chapter discusses the underlying strategic considerations and incentives that drive Russia's transition to hybrid warfare. The present discourse delves into the historical and political background of the growing tensions between Russia and Ukraine and the particulars of Russia's doctrine surrounding the notion of hybrid warfare.

This chapter also examines Russia's hybrid warfare tactics against Western nations and Ukraine, including how these methods were put into practice and how they affected regional security. The study shows how Russia employs various hybrid warfare strategies, including economic pressure, cyber operations, propaganda campaigns, and deploying conventional and unconventional armed troops. It also illustrates how these methods have wide-ranging effects on security and international

affairs. Understanding the complexity of Russia's hybrid warfare tactics and their place in the international arena requires this in-depth analysis.

The study's third chapter thoroughly analyzes the hybrid warfare tactics of non-state actor ISIS in Syria and Iraq. An extensive analysis of the structure and origins of ISIS starts this chapter. A more profound comprehension of ISIS's motivations for using hybrid warfare has been made possible by the thorough examination of the group's formation and origins. After that, an in-depth investigation of the factors that led to ISIS's adoption of the idea of hybrid warfare and a detailed examination of the power asymmetry it generated against its enemies follow.

The analysis of ISIS's hybrid warfare tactics follows next in this chapter. This study highlights ISIS's cyberspace activities, the way conventional and unconventional strategies blended, and the impact that factors like terrorism had on the group's ambitions. The various aspects of ISIS's hybrid warfare tactics and their effects on international operations, political stability, and regional security have all been extensively studied. The study clarifies the intricate structure of ISIS's hybrid warfare tactics and shows how these tactics endanger international security in addition to that of the Middle East.

The comparison chapter of the study is discussed in chapter four. Here, an in-depth analysis of the hybrid warfare tactics used by ISIS, a non-state actor, and Russia, a state actor, is provided. This analysis aims to illustrate the adaptability of hybrid warfare to various combat situations. This chapter looks at how ISIS and Russia employ similar tactics but also emphasizes how they might differ on tactical and strategic levels. In addition to facilitating a deeper comprehension of the nature of hybrid warfare, this comparison of the methods used by different sides in different regions seeks to illuminate possible future conflicts through various case studies.

The study's conclusions and implications are presented in the last chapter. The findings of the in-depth analysis of the hybrid warfare methods used by ISIS and Russia are thoroughly discussed. Considering both sides' methods, this chapter discusses hybrid warfare's fundamental characteristics and effects. Several aspects of hybrid warfare have been clarified by analyzing ISIS's non-state actor strategies and Russia's state-level hybrid warfare operations. The main discussion topics in the

conclusion are the significance of hybrid warfare in contemporary conflict contexts and how these tactics affect regional security. The study strongly emphasizes how complicated hybrid warfare is and how it affects international security and relations.



CHAPTER ONE

THE CONCEPTUAL FRAMEWORK OF HYBRID WARFARE

In recent years, hybrid warfare has led to the transformation and development of existing approaches by simultaneously employing conventional and unconventional tactics in conflicts. Hybrid warfare utilizes tactics involving military, economic, informational, and cyber operations by both state and non-state actors to achieve strategic and political objectives. The novelty and uncertainty of hybrid warfare, as well as its components not being fully defined, hinder the development of effective countermeasures (Hoffman, 2007; Prins, 2002: 1-95).

To outline the theoretical and conceptual framework of hybrid warfare and better understand it, this thesis seeks answers to the following questions: (1) How has the concept of hybrid warfare evolved historically? (2) What are the main definitions, characteristics, and components of hybrid warfare? (3) How does hybrid warfare differ from other war concepts? and (4) What are the main criticisms of the hybrid warfare concept? Answers to these questions will be sought under the following headings.

First, the origins of the hybrid warfare concept, how it emerged, and the factors that influenced hybrid warfare during this historical period will be analyzed. Thus, a more comprehensive explanation will be provided by examining the evolutionary process of hybrid warfare, the factors influencing this process, and the historical and technological developments.

Secondly, the components of hybrid warfare will be examined. In this thesis, the components of hybrid warfare are categorized into two main headings: military and non-military components.

Subsequently, to fully comprehend hybrid warfare, the similarities and differences with other war concepts have been analyzed in detail. During this analysis, hybrid warfare has been compared with other war concepts such as asymmetric warfare, limited warfare, nonlinear warfare, compound warfare, and fourth-generation warfare.

Following that, the motivations behind state and non-state actors resorting to hybrid warfare have been examined. By considering actors' motivations, the reasons for resorting to hybrid warfare have been attempted to be explained.

Finally, we will focus on the key objections to and discussions on hybrid warfare brought up by academics, historians, military strategists, and diplomats.

The International Institute for Strategic Studies (IISS) defined hybrid warfare as a campaign that combines military and non-military means to gain psychological and physical advantage, seize the initiative, and achieve surprise advantage in its annual assessment, *Military Balance*, published in 2015. This definition states that hybrid warfare comprises covert and overt military and intelligence operations, sophisticated information, electronic and cyber operations, as well as economic pressure (*Military Balance*, 2015: 18-20). This term is significant because it emphasizes both the psychological and physical aspects of hybrid warfare.

Similarly, in the same year, the European External Action Service (EEAS) published *Food for Thought: Countering Hybrid Threats*, which provided a comprehensive definition of hybrid warfare. This definition describes hybrid warfare as the coordinated use of economic pressure, military and non-military methods, intelligence and cyber operations, and political and strategic goals by a central authority. In order to attain their political objectives, hybrid players combine coercive and subversive tactics to weaken and destabilize an opponent (EEAS, 2015: 2).

Others have provided more straightforward definitions, while some scholars and strategists have regarded hybrid warfare as a complicated and multifaceted notion. For instance, hybrid warfare is defined by Peter Mansoor (2012) as the combined use of conventional and irregular forces by actors from both the state and non-state sectors. This description, however, falls short in explaining modern instances of hybrid warfare, such as the circumstance in the Crimea. Despite the fact that Mansoor highlights the significance of terrorist and guerrilla actions, his concept of hybrid warfare excludes the elements present in Crimea, such as sabotage, disinformation, communication disruption, and proxy fighters (Mansoor, 2012: 3-4).

In this thesis, NATO's definition of hybrid warfare has been chosen, and the subsequent analysis of Russian and ISIS cases will be conducted based on this

definition. According to NATO, hybrid warfare is defined as “a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, employed in a highly integrated design by state and non-state actors to achieve their objectives.” (Warsaw Summit Communiqué , 2016). There are several reasons for selecting NATO's definition of hybrid warfare. The first reason is that NATO is an international military alliance with experience in dealing with various forms of warfare and security threats. As a result, its definition carries significant weight and credibility in the field. Secondly, NATO's definition is comprehensive and flexible, capturing the complex and adaptive nature of hybrid warfare while encompassing both state and non-state actors. This allows for a more nuanced analysis of the concept, accounting for the diverse strategies and tactics employed in hybrid conflicts. Lastly, using NATO's definition enables a consistent and coherent framework for understanding hybrid warfare, facilitating comparisons with other warfare concepts, and providing a solid foundation for the analysis and discussion throughout the thesis.

1.1. THE EMERGENCE AND GROWTH OF HYBRID WARFARE CONCEPT

1.1.1. The Origins of Hybrid Warfare Concept: Chechen Wars and Hezbollah Case

The Chechen Wars are often considered among the first examples of hybrid warfare for several reasons, as they showcased the complex blend of conventional and unconventional tactics employed by non-state actor in a post-Cold War context.

The Chechens' hybrid warfare approach in the Chechen Wars was a blend of conventional and unconventional tactics that significantly complicated the Russian military's response. Guerrilla warfare, which is characterized by small, mobile groups employing hit-and-run tactics, played a crucial role in the Chechen resistance, as did the use of improvised explosive devices (IEDs) to disrupt Russian forces (Galeotti, 2014: 26). Furthermore, the Chechen forces deftly employed information warfare to undermine the morale of the Russian soldiers and garner support from the

global community. This included the strategic use of media outlets to disseminate their narrative and conduct psychological operations. As evidence of their remarkable capacity for adaptation, the Chechens also switched from conventional warfare in the First Chechen War (1994–1996) to a more decentralized, cell-based structure in the Second Chechen War (1999–2009), which allowed them to better take advantage of the flaws in the Russian military (Souleimanov, 2013: 1601-162). These methods and ideas have been quite successful since they have both made it difficult for Russia to put down the revolt and caused the fight to become a protracted insurgency.

In the literature on hybrid warfare, the Chechen Wars take center stage. These conflicts offer insightful information on the practical application of hybrid warfare's complexity.

In his 2002 thesis, “Future War and Chechnya: A Case for Hybrid Warfare,” William Nemeth—one of the pioneers in the field of hybrid warfare—explained how conventional and unconventional techniques were combined and applied by state and non-state actors.” He wrote, “It must be remembered that hybrid warfare, the contemporary form of guerrilla warfare, is a continuation of pre-state warfare that has become more effective because it employs both modern technology and modern mobilization methods” (Nemeth, 2002: 29). In contrast to the contemporary understanding of hybrid warfare, Nemeth's definition seems insufficient and antiquated. This is due to its narrow focus on the Chechen wars, which fails to account for the evolving nature of modern warfare. Hybrid warfare extends beyond conventional asymmetric tactics and encompasses a diverse array of strategies. Despite these shortcomings, it is worth acknowledging the significance of Nemeth's work as one of the earliest and most influential studies in the field of hybrid warfare, which has substantially contributed to the academic discourse on the subject and the understanding of modern warfare dynamics.

Besides, Frank G. Hoffman is a prominent name in hybrid warfare, although other researchers have also studied and written about the concept before him. The primary reason for his recognition is Hoffman's holistic perspective on hybrid warfare (Johnson 2018: 150). In 2007, Hoffman first used the idea of hybrid warfare to explain Hezbollah's military victory over Israel in the Second Lebanon War of

2006, aided by the Iranian government (Bachmann & Gunneriusson, 2015: 78). Hoffman claims that the form of conflict that led to Hezbollah's triumph was hybrid warfare, which he defines as “incorporating a range of different modes of warfare including conventional capabilities, irregular tactics, and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder” (Hoffman, 2007: 29).

While defining hybrid warfare, Hoffman has referred to two significant sources: the Quadrennial Defense Review of 2006 and the National Defense Strategy of 2005. However, since he believed that neither of these sources was sufficient to fully define and understand hybrid warfare, he came up with a new definition. (Hoffman, 2010: 443). The National Defense Strategy of 2005 makes it abundantly clear that the United States has an advantage in conventional warfare practices around the globe; consequently, future adversaries will avoid direct conventional warfare and employ irregular methods and capabilities combined with conventional aspects of warfare. This document classifies the threats to U.S. interests into four categories: traditional, irregular, catastrophic, and disruptive challenges (Rumsfeld, 2005: 2).

On the other hand, Hoffman claims that there is no evidence to suggest that future threats will strike separately. According to him, they will be a mix of several forms of warfare. Future conflicts will blur the lines between conventional, irregular, terrorist, and violent actions. Therefore, Western nations must comprehend that potential adversaries will not strike separately but in concert. This circumstance will not only make future conflicts multimodal and multivariable but will also exacerbate their complexity. This new style of warfare, which incorporates numerous advances and may be waged by both state and non-state actors, is referred to as “hybrid warfare” (Hoffman, 2007: 7-14).

1.1.2. Evolution of the Hybrid Warfare Concept

During the Cold War, the international system was divided into two power blocs, consisting of the United States and the Soviet Union and their respective supporters. This situation facilitated academics and military strategists in analysing

potential conflicts and security issues. Although the international system was threatened by the possibility of a nuclear war and high tensions between the poles, a stable and predictable environment was provided for military and strategic studies. Moreover, the overt nature of conflicts during the Cold War and the clear objectives of the parties involved made analysis easier. In contrast, in the post-Cold War period, security studies became more challenging due to the difficulty in determining the causes of conflicts and the intentions of the actors involved. This has made it more difficult for scholars to analyse security issues and predict potential conflicts, as the lines between state and non-state actors and between different types of conflict have become increasingly blurred. As a result, it is now more challenging to identify and manage security threats in the modern era (Waltz, 2000: Yalçinkaya, 2019: 1-10).

Throughout ongoing conflicts, various terms have been utilized by analysts, scholars, defence communities, and military strategists to conceptualize and reinterpret new wars. These terms include “Fourth Generation Warfare,” “Asymmetric Warfare,” “Compound Warfare,” “Unrestricted Wars,” “Ambiguous Warfare,” “Full-spectrum Conflict,” “Non-linear Warfare,” “Irregular Warfare,” “Revolution in Military Affairs (RMA),” and “New Wars” (Caliskan, 2019: 40-58; Weisman, 2019: 17-26; Kaldor, 2012: 3; Liang and Xiangsui, 1999: 12). Hybrid warfare began to gain prominence among these concepts as a buzzword after the mid-2000s (Weissmann, 2019: 18).

When examining the origins of the concept, hybrid warfare initially emerged as a term used to analyse the strategies and methods employed by Chechen fighters and the radical terrorist organization Hezbollah in order to balance their military and economic disadvantages. Consequently, hybrid warfare initially appeared as a war concept employed by non-state actors. However, these definitions and analyses proved insufficient in explaining the hybrid warfare conducted by Russia in Crimea and Ukraine's Donbas regions (Renz, 2016: 285). Russia utilized a highly effective version of hybrid warfare in Crimea and Donbas, demonstrating that the concept had evolved into a far more dangerous form than initially anticipated. This led to the realization that a more comprehensive explanation of modern hybrid warfare was necessary (Rühle, 2019: 1). With the adoption of hybrid warfare by Russia, the Western perspective on the concept of hybrid warfare has also shifted. This

transformation in viewpoint has necessitated a reconsideration of strategies and approaches to address the evolving threats posed by this form of warfare (Wither, 2016: 73-74).

Following Crimea's annexation, the West has realized the urgency of hybrid threats. In addition, the conflict between Russia and Ukraine has motivated member states to expand NATO's capacity to respond to hybrid threats (Giegerich, 2016: 66). Consequently, the EU and NATO have developed several bodies to counteract hybrid threats. Significant examples of these organizations include the NATO Transnet Network on Countering Hybrid Threats (CHT), Rapid Alert System-Disinformation (RAS-DIS), Hybrid Fusion Cell (HFC), EU Intelligence and Situation Centre (INTCEN), Strategic Communication Task Forces (STRATCOM), and European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). (Parkes, 2019: 10; Smith, 2019: 17; Bachmann and Gunneriusson, 2015: 82-83). Hybrid CoE, in particular, is of great significance to these organizations. This organization, established on 1 July 2017 by NATO and the EU, provides one of the most comprehensive and detailed descriptions of hybrid threats. According to this definition, the concept of "hybrid threat" pertains to activities undertaken by state or non-state entities with the intent to weaken or damage a target by influencing its decision-making processes at various levels, such as local, regional, state, or institutional. These actions are meticulously coordinated and synchronized, specifically targeting the vulnerabilities of democratic states and institutions. Hybrid threats can manifest in diverse domains, including political, economic, military, civil, or informational spheres. They employ a broad array of methods while maintaining a level of subtlety to avoid detection and attribution. (Hybrid threats as a concept, n.d.).

Initially associated solely with non-state actors and limited to a mixture of conventional and unconventional warfare strategies, hybrid warfare has gained a new dimension and increased popularity within military and academic circles following Russia's execution of hybrid warfare against Ukraine and the West (Michael, et al., 2017). This evolution has prompted further examination and discussion regarding the implications of this form of warfare on global security and geopolitics.

1.1.3. Hybrid Warfare Through Time: An Exploration of Historical Examples

Despite numerous sources examining the concept of hybrid warfare, a clear definition on which academics and military strategists can agree has not been created. This ambiguity makes it challenging to determine which conflicts should be considered within the scope of hybrid warfare. Consequently, some historical wars and conflicts have been analysed under the concept of hybrid warfare by various authors. In this section, we will examine various wars that have been classified and evaluated as hybrid warfare by different authors, exploring the diverse perspectives on this evolving concept.

Hybrid warfare, a term popular among Pentagon leaders, has been a topic of debate among military historians for years. Mansoor (2012) contends that hybrid warfare, while not altering the character of conflict, does change its conduct. Despite its value as a framework for analysing symmetric and asymmetric warfare as well as its regular and irregular (guerrillas, insurgents, and terrorists) components, hybrid warfare is not a novel concept. Mansoor traces its origins back to the Peloponnesian War between 431 and 404 B.C., where despite their military superiority, the Spartans were forced to accept certain terms due to Athens backing Spartan uprisings (Mansoor, 2012: 1-4). This is seen as an example of hybrid warfare.

Also, prominent military historian Max Boot (2015) agrees that the history of hybrid warfare dates back to ancient times, but he argues that its inception can be traced even further back to 5000 B.C. According to Boot, conventional conflicts during this time were impossible, as all hostilities were irregular and there were no conventional forces with bureaucratic organizations to conduct conventional wars. The rise of hybrid warfare, he suggests, is a result of the existence of city-states. Both Boot and Mansoor concur that the Peloponnesian War was a mixed conflict. However, Boot posits that both the Athenians and Spartans employed hybrid strategies during this conflict, as both city-states encouraged revolutions against each other's (Boot, Brahim, Kemp, Tobias, & Weiss, 2015: 11-12).

Furthermore, the American colonies' resistance against British soldiers during the American War of Independence serves as another instance of hybrid warfare. The

British, attempting to force the Americans to stay within their colonies and submit, were unaware of the impending conflict. Despite being ill-equipped and lacking the training of the British military, the Continental Army, the colonies' regular forces, managed to overcome the British by effectively combining regular and militia forces. This victory in the face of adversity exemplifies the concept of hybrid warfare (Murray, 2012: 73-86).

Writers such as Mansoor, Murray, and Boot may trace the historical examples of hybrid warfare further back in time, yet many scholars believe that the 20th century witnessed numerous instances of hybrid warfare. The wars claimed by these authors and other scholars as examples of hybrid warfare can be listed in chronological order below.

The Second Sino-Japanese War, that occurred from 1937 to 1945, serves as another example supporting this argument (Mansoor, 2012: 5). The Japanese government had not planned for this war, and it was never officially declared by Japan. The General Staff of the Imperial Army, fearing that the war would escalate into a full-scale revolutionary conflict, opted for a limited military expansion. Japanese leaders believed they could subdue the Chinese before the war intensified. However, events did not unfold as they had anticipated. The General Staff of the Imperial Army expected a brief and decisive conflict between the two nations, but the Chinese Nationalist regular forces strategically avoided a conventional war, opting instead for a limited and protracted engagement using both regular and irregular forces. The Second Sino-Japanese War stands as a notable example of hybrid warfare that took place neither in the West nor involving Western countries. It is important to note, though, that the hybrid warfare employed by the Chinese Nationalist regular and irregular forces during this conflict represents a more primitive form of today's hybrid warfare (Yamaguchi, 2012: 225-227).

McCulloh and Johnson (2013) assert that the Vietnam War represented hybrid warfare, even though some authors have labelled it a compound war. In a compound war, irregular forces support the efforts of regular forces as part of a secondary plan. However, in the case of the communist forces, the difference between regular and irregular soldiers was less clear, with both forces acting concurrently. Moreover, the North Vietnamese Army, the regular force, occasionally

took a backseat during the conflict, while the Viet Cong, the irregular force, played a crucial role.

Communist forces engaged in hit-and-run operations using guerrilla tactics, avoiding decisive battles. According to the Central Office for South Vietnam (COSVN) and the Viet Cong, political objectives could be achieved through gradual attrition rather than decisive engagements. Recognizing this, communist forces combined information and influence operations with armed propaganda and military power, presenting a novel and successful example of hybrid warfare to US soldiers. The Vietnam case also demonstrated the synergistic potential of employing regular and irregular forces, methods, and tactics (McCulloh & Johnson, 2013: 71-78).

In agreement with McCulloh and Johnson, Lowe (2012) argues that the Vietnam War was characterized by layered civil and regional conflicts. This complex nature made the war inherently hybrid, combining conventional weaponry and tactics with guerrilla and counterinsurgency warfare strategies. The efficacy of North Vietnamese hybrid approaches against American and South Vietnamese forces at the operational and tactical levels served as a powerful demonstration to the Western world of hybrid warfare's potential effectiveness (Lowe, 2012: 254).

Yıldız (2017) notes that instances of hybrid warfare can be found in the military history of Eurasia. One such example occurred during the First World War when Germany launched a strategic hybrid attempt in Eurasia. Max von Oppenheim, a German ambassador, attempted to mobilize the Muslim communities in Russian, British, and French Eurasian territories by invoking the Great Jihad of the Ottoman Caliphate against the Entente Powers. Yıldız also argues that the origins of the hybrid warfare utilized by the Russian Federation in Crimea can be traced back to Tsarist Russia's actions in the Balkans two centuries ago. In the Balkans, Tsarist Russia incited local Slavic populations against the Ottoman Empire to gain territory (Yıldız, 2017: 26-27).

In addition, Johnson (2017) contends that during the First World War, the Hashemite rebellion against the Ottoman Empire during serves as another example of hybrid warfare. Hashemite Sheriff Hussein, the Guardian of Mecca, rejected the Caliph's call in 1914 and declared independence from the Ottoman Empire in 1916, following covert negotiations with British officials. In the ensuing period, the

Hashemites sought to undermine the Ottoman Army's morale by capturing Mecca. They enlisted fighters from other Bedouin tribes, reframing their uprising against the Ottoman Empire as a broader Arab revolt. The Hashemites engaged in hybrid warfare by challenging the Sultan's call for jihad as illegitimate, leveraging British political, military, economic, and logistical support to achieve their goals. In 1918, they declared their political triumph in Damascus (Johnson, 2017).

It should be noted that the identification of historical examples of hybrid warfare is not without controversy. For example, authors such as Johnson and Mansoor disagree on the identity of the actor conducting hybrid warfare with regards to the Arab Revolt against the Ottoman Empire. While Johnson argues that Sharif Hussein bin Ali waged hybrid warfare, Mansoor claims it was conducted by Britain. According to Mansoor, the British government sought to defeat Turkish forces in Palestine, enlisting the help of Sharif Hussein with the efforts of Captain T.E. Lawrence. The British Army subsequently mobilized Arab irregular forces against the Ottoman soldiers and used their intelligence to achieve victory at Megiddo in 1918. Despite differing interpretations of who conducted hybrid warfare in this historical context, the case of the Arab Revolt remains a valuable example for analysing the complexities of hybrid warfare (Mansoor, 2012: 6-7).

Several authors have pointed out other examples of historical hybrid warfare in addition to those mentioned earlier. For instance, Pakistan's involvement in Afghanistan since the Soviet occupation in 1979 and its confrontations with India from the 1947-1948 Indo-Pak War are considered examples of hybrid warfare (Chadha, 2014: 37-61). Additionally, the irregular partisan operations of Soviet partisans against the German Army during World War II, coupled with the conventional war conducted by the Red Army, and the joint operations of the Spanish guerrillas alongside the British and Portuguese conventional armies against the French army in the Peninsular War, are also viewed as examples of hybrid warfare (McCulloh & Johnson, 2013: 27-33; Sinnreich, 2012: 104-151).

1.2.COMPONENTS OF HYBRID WARFARE

Since hybrid warfare has a multifaceted and complex structure, it encompasses numerous components. Therefore, it is possible to categorize these components in different ways. In this thesis, the components of hybrid warfare will be examined under two headings: military components and non-military components.

1.2.1. Military Components of Hybrid Warfare

Throughout history, various wars have witnessed the coexistence of regular and irregular military forces. Notable examples include the Peloponnesian War, the American War of Independence, the Spanish guerrilla war against the French Army, the Second Sino-Japanese War, and the Vietnam War, which will be further examined in subsequent sections. Nevertheless, it would be erroneous and reductive to assert that all wars featuring both regular and irregular components can be classified as hybrid (Schroefl & Kaufman, 2014: 867). In other words, it is imprecise to label coordination and coexistence of regular and irregular military forces as hybrid warfare (Parkes, 2019: 5).

There are numerous military components that hybrid actors may employ during their attacks. These components can be grouped under general categories such as ground forces, air forces, naval forces, insurgency, counterinsurgency, terrorism, paramilitary forces, and proxy warfare. In hybrid warfare, military components are used in conjunction with non-military components to create a destructive impact. The aforementioned military components may all be present simultaneously in a single hybrid conflict, or they may be employed separately at different times, depending on the situation and strategic objectives.

Conversely, the military aspect of technologically advanced and hybrid warfare exhibits distinct features that set it apart from conventional conflicts. These specific traits encompass a transition from strategic oversight to operational combat control, emphasizing real-time battlefield management and informational supremacy in domains such as intelligence collection, decision-making, and the execution of effects. Additionally, there is an increased focus on cyber and airspace environments,

including intelligence, surveillance, and reconnaissance (ISR) operations. Furthermore, advances in technology have led to a greater reliance on robotic systems, stealth concepts, and remote warfare capabilities. In such conflicts, the advancement and implementation of situational and automated surveillance and attack systems hold a critical significance. There is also a growing emphasis on the use of non-lethal weapons that can be highly effective in achieving strategic objectives. Hybrid wars often involve the integration of irregular militia groups, such as paramilitary forces, resulting in an increase in asymmetric combat actions. This trend is further complemented by the expanding role and involvement of Special Forces, highlighting the evolving nature of warfare in the context of highly technological and hybrid conflicts (Danyk, Maliarchuk, & Briggs, 2017: 22-23).

Hybrid warfare involves intensive blurring, integration, and mixing of distinct regular and irregular elements, as well as the ability to work synchronously and simultaneously (Treverton, Thvedt, Chen, Lee, & McCue, 2018: 45). In order to establish successful synchronization, hybrid operations may be conducted by centralized or decentralized cells (Aoi, Futamura, & Patalano, 2018: 700). Moreover, contemporary battles, i.e., hybrid warfare, are fundamentally distinct from historical wars that contained hybridization of regular and irregular forces. In numerous historical cases, irregular components were utilized to prolong the duration of battles, prevent a swift response, increase the cost of war for the adversary, and exhaust enemy forces. Now, like regular troops, these components have decisive hybrid warfare activities (Hoffman, 2007: 29). This indicates that irregular and non-military components supported regular forces in the past. In the twenty-first century, however, the regular armed forces no longer significantly participate in hostilities.

Unlike conventional wars, hybrid warfare is never proclaimed. Moreover, hybrid warfare is a low-intensity, continuous conflict (Bıçakçı, 2019: 1-2). This is a crucial issue for state actors to consider when implementing hybrid warfare. Because declaring war shows belligerent adversaries. Nevertheless, the hybrid actor can conceal itself to avoid identification and punishment by employing hybrid strategies and tactics (Kilcullen, 2013: 105). In this manner, the hybrid actor might avoid international community and international law sanctions.

Furthermore, because these wars have yet to be formally declared, they are easy to refute. For instance, Moscow has consistently denied involvement in the 2014 unrest in Ukraine, while the Russian government deployed the so-called “little green men” (*zelonyye lyudishki*)¹ (Wither, 2016: 81). Similarly, when it became apparent that Moscow employed the little green men in Crimea, the international community did not respond strongly against Russia (Schnauffer, 2017: 22).

The hybrid actor gains an advantage since hybrid warfare is undertaken in grey zones. Some scholars suggest that hybrid warfare can remain below the threshold of conflict, thereby protecting actors who employ hybrid strategies from military or political responses (Reichborn-Kjennerud & Cullen, 2016: 2). This highlights the danger posed by hybrid warfare. It may be too late when actors confronting hybrid warfare understand they are at war. They may even lose the war substantially (Abdyraeva, 2020: 14). Detection and consolidation of vulnerabilities are, therefore, crucial for target states. The following sections will examine how target countries should protect themselves from hybrid threats.

The emergence of hybrid warfare may be interpreted as signal the end of conventional combat. However, it creates more complex and unexpected issues for 21st-century defence agencies. (Hoffman, 2007: 43; 2009: 37). The hybrid nature of warfare has resulted in two significant changes to military practices. Firstly, hybrid warfare restricts the use of conventional strategies. For instance, Russia annexed Crimea and achieved its political and strategic objectives without firing a shot while providing information operations greater weight than military actions (Thornton, 2015: 42). Secondly, the expansion of blurring, integration, and the blending of regular and irregular components presents another change in the levels of wars. According to Hoffman (2007), conventional, unconventional, regular, and irregular wars were coordinated strategically in past wars. However, in hybrid warfare, diverse modes of combat converge even at the operational and tactical levels of war.

¹ The little green men are combat troops that first emerged during Crimea's annexation and later played an active role in internal conflicts in Ukraine. These forces were speaking Russian, uniforming like the Russian soldiers, and using Russian equipment. Although they pursued pro-Russian policies in both cases, Moscow claimed that these troops were not affiliated with Russia and described them as local resistance forces. For more details, see also (Reeves & Wallace, (2015). 361-401; Haines, John R. 2016.

1.2.2. Non-military Components of Hybrid Warfare

Incorporating diplomatic, economic, political, social, technological, and cyber components, hybrid warfare is a dynamic and complex approach to contemporary conflict. Understanding the challenges posed by hybrid warfare requires a thorough examination of each component and their interplay.

Diplomatic and political components are crucial to hybrid warfare strategies. Often, adversaries engage in political subversion and exploit existing societal and cultural divides to weaken the cohesion and governance of the targeted nation (Dayspring, 2015: 1). Diplomatic efforts may be employed to garner support from international actors, thereby increasing pressure on the target nation and making its response to hybrid threats more difficult (Military Balance).

In hybrid warfare tactics, economic factors are equally important, with adversaries utilising economic dependencies and vulnerabilities to exert control and influence over targeted nations. Utilizing advanced technological systems can increase the effectiveness of a state's existing military capability while potentially reducing costs by a third compared to traditional budgets (Danyk, Maliarchuk, & Briggs, 2017: 23).

Social factors are significant in determining the landscape of hybrid conflicts, as well. To gain local support and establish a foundation for their military and political objectives, adversaries may invest in constructing social infrastructure, providing humanitarian aid, education, and medical services (Glenn, 2009: 3).

Modern technology has enabled new methods of intelligence gathering, surveillance, and reconnaissance, which have fundamentally altered the conduct of hybrid warfare. The incorporation of advanced technologies into military strategies can provide a strategic advantage and facilitate a more efficient response to hybrid threats (Danyk, Maliarchuk, & Briggs, 2017: 17). Adopting emerging technologies is essential for maintaining a competitive advantage in the domain of hybrid warfare.

In recent years, the cyber component of hybrid warfare has gained increasing importance. Cyber warfare capabilities, such as network attacks, data breaches, and disinformation campaigns, are used to undermine the digital infrastructure of the target nation, disrupt vital services, and manipulate public opinion (Muradov, 2019:

306). As the cyber landscape continues to evolve, nations must establish robust cyber defences and decentralised organisations capable of swiftly responding to cyber threats (Wilkie, 2009).

It is essential to recognise that the specific fears exploited by a hybrid actor depend on their objectives and operating environment. To identify the specific fears being exploited and the objectives of the hybrid actor, a meticulous analysis of the situation is required. By utilising diplomatic, military, economic, and technological means and processes, the hybrid actor can more effectively coerce the target nation and its population to comply with its political goals. This creates a climate of discord across the nation, making it difficult to establish vital alliances in a chaotic setting. Thus, the target nation's political and economic ties are affected (Boyer & Lindley-French, 2012: 266).

As a complex and adaptable approach to modern conflict, hybrid warfare incorporates diplomatic, economic, political, social, technological, and cyber elements. For effectively countering and adapting to the challenges posed by hybrid warfare in the current geopolitical landscape, a comprehensive understanding of these elements, informed by the provided is crucial. To address the evolving nature of hybrid threats and to ensure a resilient and secure global order, it is necessary to develop multifaceted strategies and to foster international cooperation.

As can be observed, hybrid warfare damages a country's internal and external relationships over time. On the other hand, destabilizing the target state through military conflict is not a simple endeavour. Consequently, hybrid warfare transcends the battlefield. By adding additional battlegrounds to conventional war, hybrid warfare extends the battlefronts. Furthermore, the dimensions involved extend beyond physical realms such as land, sea, air, and space, encompassing political, economic, cultural, cyber, informational, structural, and social dimensions as well. (Reichborn-Kjennerud & Cullen, 2016: 3; Danyk, Maliarchuk, & Briggs, 2017: 5). With the addition of transnational terrorism, transnational crime, and diasporas, war becomes a global phenomenon that transcends nations and boundaries and affects not just the government and military of the target state but also the entire population (Schroefl, & Kaufman, 2014: 862).

1.3. HYBRID WARFARE and ITS DISTINCTIVENESS AMIDST OTHER WARFARE CONCEPTS

The hybrid warfare concept has become a widely debated topic among military strategists and scholars, following the examination of new strategies employed by Hezbollah during the Second Lebanon War in 2006. While authors like Frank G. Hoffman (2009) argue that hybrid warfare is an unprecedented warfare concept, others like Hanna Smith (2019) claim that it presents only minor differences. On the other hand, writers such as Mikael Weissman (2019) and Robert Johnson (2017) have contended that the components and threats of hybrid warfare are not unique. The lack of consensus on what hybrid warfare entails in academic and military circles has made it difficult to discern its differences from other warfare concepts. As a result, hybrid warfare has often been compared with other warfare concepts, such as “non-linear warfare,” “limited warfare,” “asymmetric warfare,” “compound warfare,” and “fourth-generation warfare.” To comprehend what hybrid warfare is, the innovations it brings to the battlefield, and the new threats it creates, it is necessary to analyse the distinctions between the hybrid warfare concept and other warfare concepts.

1.3.1. Comparing Non-linear and Hybrid Warfare: Key Distinctions

Hybrid warfare not only introduces complexities in the means and methods employed but also adds intricacy to the various phases of warfare (Weissmann, 2019: 22). In contrast to conventional warfare, hybrid warfare does not adhere to the progressive nature of conflict due to its non-linear progression. Owing to this non-linear development, the concept of hybrid warfare has been scrutinized by numerous defense communities. According to these critics, hybrid warfare merely represents a variant of non-linear warfare, as both concepts share several common features, such as cyberattacks, propaganda, smear campaigns, and political and social provocations.

However, equating hybrid warfare with non-linear warfare would be an oversimplification. A closer examination of non-linear warfare reveals that it encompasses a grand strategy, whereas the notion of a grand strategy is absent from

the concept of hybrid warfare (Schnauffer, 2017: 22). Furthermore, non-linear warfare assumes that tactical nuclear weapons would be frequently employed to create substantial gaps in defensive lines, which follow-on ground forces could then exploit (Dayspring, 2015: 54). In contrast, the use of nuclear weapons for tactical purposes or other objectives has not been emphasized under the umbrella of hybrid warfare.

In summary, while hybrid warfare complicates both the means and methods of warfare and the phases of conflict, it should not be considered synonymous with non-linear warfare. Despite sharing some common characteristics, distinctions in the presence of a grand strategy and the role of tactical nuclear weapons set these two concepts apart.

1.3.2. Comparing Limited and Hybrid Warfare: Key Distinctions

The distinction between limited war and hybrid warfare is both significant and conspicuous. The concept of limited war entails that both parties involved in the conflict voluntarily agree to confine the scope of the confrontation, regardless of whether a formal agreement is reached or not (Freedman, 2014: 8-11). This mutual understanding serves to restrain the intensity of the battle and maintain a certain level of control over its progression.

Conversely, hybrid warfare does not involve any mutual agreement to limit conflict. Moreover, the country targeted by hybrid attacks may not even be aware that it is engaged in a war (Cullen & Reichborn-Kjennerud, 2017: 10). Due to the inherently diverse range of attack methods utilized in hybrid warfare, it is challenging to fully detect and comprehend its nature.

Another significant distinction lies in the underlying reason for resorting to limited war. Limited war encompasses a one-dimensional military spectrum, involving the limited use of conventional military means to achieve political and strategic objectives. Limited war ensures that conflict remains contained at a restricted level rather than escalating. In contrast, hybrid warfare is a form of war that is not solely confined to the military spectrum and incorporates the military, informational, political, and social aspects of warfare, operating across these domains (Karabulut, 2016: 26). The ability of hybrid warfare to affect such diverse areas

allows the aggressor to exploit various vulnerabilities of the targeted country simultaneously or separately.

In summary, the key difference between limited war and hybrid warfare lies in the voluntary restriction of the conflict by both parties in the former, and the absence of any such agreement in the latter. Furthermore, limited war is characterized by its reliance on conventional military means, while hybrid warfare employs a wide range of tactics that span across various domains.

1.3.3. Comparing Asymmetric and Hybrid Warfare: Key Distinctions

Asymmetric warfare is another concept that is frequently juxtaposed with hybrid warfare in academic discourse. Numerous authors and researchers contend that hybrid warfare is not an entirely new concept, but rather a reimagined and updated form of asymmetric warfare. According to this perspective, hybrid warfare serves as an extension of pre-existing asymmetric warfare (Wither, 2016: 78; Johnson, 2018: 147). As such, the study of hybrid warfare initially unfolded within the broader context of asymmetric warfare.

Over time, however, the limitations of this narrow framework became evident, and hybrid warfare emerged as a distinct concept in its own right (Thornton, 2015: 41). The abstract nature of asymmetric warfare gave rise to the development of unique advantages for hybrid warfare. By virtue of being more tangible, comprehensive, and operationally focused than asymmetric warfare, hybrid warfare has garnered increased attention in defence circles (Weissman, 2019: 25).

It is essential to note that there is a significant difference between asymmetric warfare and hybrid warfare. Asymmetric warfare is characterized by a relatively weaker opponent engaging a more formidable adversary in terms of technology, equipment, and operational capabilities. The primary objective in this type of conflict is to mitigate weaknesses and neutralize the opponent's strengths by employing asymmetric methods (Bachmann & Gunneriusson, 2015: 86; Weissmann, 2019: 19).

Although hybrid warfare is frequently compared to asymmetric warfare and was initially studied within its context, it has since evolved into a distinct concept. Hybrid warfare's more tangible, comprehensive, and operational nature has

contributed to its increasing popularity in defence environments. Moreover, the key distinction between the two lies in the objective and approach of asymmetric warfare, which seeks to counter a stronger adversary through unconventional means. In addition, the primary distinction between the two lies in the objective and strategy of asymmetric warfare, which seeks to counter a stronger opponent through unconventional means.

1.3.4. Comparing Compound and Hybrid Warfare: Key Distinctions

Compound warfare bears notable similarities to hybrid warfare due to its inherent characteristics. Among the most salient commonalities is the presence of both regular and irregular elements within the conflict. As a result, compound warfare is often equated with hybrid warfare owing to this shared feature. As previously discussed, hybrid warfare, akin to compound warfare, encompasses both regular and irregular elements. Nevertheless, the deployment and significance of irregular components serve as key distinguishing factors between the two concepts.

Under the framework of compound warfare, irregular components constitute a secondary strategy. Their primary function is to prolong the conflict and inflict economic, physical, and psychological damage on the adversary, with no direct bearing on the ultimate outcome of the war. In the context of hybrid warfare, however, irregular components hold equal importance to their regular counterparts, potentially even serving as a supplementary force if required (Hoffman, 2007: 29).

Moreover, the amalgamation and integration of elements in compound warfare are less pronounced than in hybrid warfare. While a convergence of these elements may be present at the strategic level, their tactical and operational levels necessitate greater complexity in compound warfare (Hoffman, 2009a: 36). A key indicator of this lack of complexity is the separation of regular and irregular forces across different regions of the battlefield. The aggressor's ability to merge these forces on the same battlefield is limited. Conversely, this capacity is considered a fundamental characteristic of hybrid actors (Hoffman, 2009b).

In conclusion, compound warfare shares certain similarities with hybrid warfare, particularly in the presence of both regular and irregular elements. However,

differences in the deployment and significance of irregular components, as well as the degree of blending and fusion of elements across strategic, operational, and tactical levels, serve to distinguish the two concepts.

1.3.5. Comparing Fourth-Generation and Hybrid Warfare: Key Distinctions

The relationship between fourth-generation warfare (4GW) and hybrid warfare is distinct compared to other conceptual pairings. While formulating the concept of hybrid warfare, Hoffman drew inspiration from various academics and institutions. His conception may have been influenced by the theories of Chinese and Australian analysts, the notion of compound warfare, and the concept of the power of networks developed by John Arquilla and T.X. Hammes. Notably, the concept of 4GW played a significant role in shaping Hoffman's perspective, as it highlighted the increasingly blurred nature of conflict and the rising employment of violence by non-state actors (Hoffman, 2007: 30).

T.X. Hammes, the originator of the term, defines 4GW as a form of warfare that “uses all available networks—political, economic, social, and military—to convince the enemy's political decision-makers that their strategic goals are either unachievable or too costly for the perceived benefit. It is an evolved form of insurgency” (Hammes, 2007: 14). Given Hammes' description, the utilization of diverse means across multiple spectrums to attain strategic objectives can be recognized as a characteristic of hybrid warfare. However, a closer examination of the definitions reveals a critical distinction between the two concepts.

4GW has not been able to provide a comprehensive understanding of war in its entirety, focusing predominantly on insurgency and resistance. Rather than serving as a war-winning strategy, the 4GW concept aims to compel the political elites of the target to capitulate. Guerrilla operations and uprisings are designed to erode the political elites' resolve to continue the conflict (Özer, 2018: 38; Johnson, 2018: 149). Consequently, hybrid warfare can be perceived as a more holistic and comprehensive approach to understanding the nature of conflict and its various actors.

Although the differences between hybrid warfare and other war concepts have been separately examined above, it is necessary to further discuss a distinguishing feature that sets hybrid warfare apart from all these war concepts. The ability of the hybrid aggressor to escalate and de-escalate conflict across different spectrums in hybrid warfare provides the aggressor with distinct advantages over their adversaries.

Hybrid warfare does not adhere to the sequential phases of conventional war due to its capacity to escalate conflicts. An actor employing hybrid methods can escalate or de-escalate the conflict to achieve political and strategic objectives. A hybrid actor can escalate or de-escalate warfare in different domains throughout various stages of conflict. Furthermore, it is possible for hybrid actors to employ both escalation and de-escalation tactics simultaneously. For example, a hybrid actor may increase political tensions during a conflict while simultaneously decreasing military tensions. (Reichborn-Kjennerud & Cullen, 2016: 3).

Since at least the Napoleonic Wars, Western nations have sought to gain an advantage over their adversaries by strengthening their capacity to escalate conflicts (Angstrom, 2017: 842). In the logic of conventional warfare, Western states have thus far outperformed non-Western powers. Similarly, escalation potential is of utmost importance for hybrid actors. The ability to combine and synchronize escalation and de-escalation is considered one of the primary qualities of a hybrid actor (Cullen & Reichborn-Kjennerud, 2017: 12).

Synchronization and combination of tactics provide the hybrid actor with several advantages. Firstly, the hybrid actor has the option to adapt its means and exploit the enemy's weaknesses to achieve political objectives. A second significant advantage is that it is difficult to detect hybrid actors. As hybrid warfare is not publicly declared, it is challenging for the target nation to identify the enemy attacking its vulnerabilities. Thirdly, hybrid warfare is a difficult type of conflict to counter. Since there is no evidence that the hybrid actor is either waging war or has not declared war, determining how to respond becomes problematic. Ultimately, the hybrid actor may be able to escalate and de-escalate the conflict simultaneously (Cullen & Reichborn-Kjennerud, 2017: 13).

Although both state and non-state actors can engage in hybrid warfare, it should be noted that the ability of state actors to escalate the conflict horizontally and vertically is superior due to the sophistication and breadth of the state's toolbox (Reichborn-Kjennerud & Cullen, 2016: 4).

1.4. THE REASONS FOR RESORTING TO HYBRID WARFARE

Throughout history, particularly from the 20th century to the present, various military techniques and conceptions have been adopted as winning formulas. Significant examples include strategic bombardment, The Revolution in Military Affairs (RMA), Fourth-Generation Warfare, Sixth-Generation Warfare, Counterinsurgency warfare (COIN), and Asymmetric warfare. Unfortunately, the concept of hybrid warfare is the culminating illustration of this misconception (Renz & Smith, 2016: 1-5).

Some authors, for example, erroneously equate Russia's straightforward victory in Crimea with a misperception that hybrid warfare would enable easy victories for the actors using this strategy. Nonetheless, it must be recognized that hybrid warfare alone may not be sufficient to achieve the desired outcomes. Favourable conditions must exist in order to realize a particular objective. Hybrid warfare is overly glorified when it is suggested that a victory similar to that in Crimea could be achieved under identical circumstances in another instance. In conclusion, as previously mentioned, hybrid warfare is contextual. Each success or failure of the hybrid warfare must be examined holistically. As in the past, there will not be a universal formula for winning wars in the future, since triumph is always context-dependent (Renz, 2016: 284-287).

On the other hand, hybrid warfare may occasionally lead to unanticipated outcomes in certain situations. Even if it does not directly provoke a conflict, a minor skirmish can arise. The tension generated by China's hybrid operations in the South China Sea serves as a prime example of this (Aoi, Futamura, & Patalano, 2018: 705). It is crucial to acknowledge that hybrid operations may create more significant challenges for aggressors. In other words, an aggressor conducting hybrid operations must be prepared for the possibility of a conventional conflict or international

sanctions if detected.

State or non-state actors engaging in hybrid warfare are aware that it is not sufficient for victory. Consequently, it is necessary to determine why they opt for hybrid warfare even though they are conscious of this fact. In other words, it is essential to explore why state and non-state actors' resort to hybrid warfare. Factors such as the actor's military strength, political structure, and position in the international system may contribute to this choice, and external influences might also play a role. Four explanations for the utilization of hybrid warfare are categorized below.

1.4.1. Military and Technological Dominance of Western Countries

The primary factor predominantly influences the decisions of non-state actors; nevertheless, it has been observed that this factor also plays a role, albeit indirectly, in the decision-making processes of state actors. The foremost criterion is the military and technological dominance exhibited by Western countries (Kaldor, 2012: 152, 203; Gray, 2007: 30-47). One exemplary illustration of this dynamic is the Second Lebanon War, where Hezbollah engaged in combat against Israeli forces. This conflict represents the first instance of contemporary hybrid warfare, characterized by a confrontation between the innovative, yet underpowered, Hezbollah forces and their conventionally superior adversary (Johnson, 2018: 147).

Hybrid actors, such as Hezbollah, implement ingenious strategies that encompass the utilization of technology, resourcefulness, asymmetric tactics, and unconventional forces in conjunction with conventional forces. This fusion aims to dismantle the dominance of their opponents (Hoffman, 2007: 25). A notable example of employing hybrid warfare to challenge and ultimately neutralize the military and technological supremacy of adversaries can be seen in Russia's annexation of Crimea. Primarily through the deployment of hybrid tactics, Russia succeeded in annexing Crimea without resorting to armed conflict (Renz, 2016: 291).

By executing hybrid operations effectively and efficiently, Russia prevented both the United States and NATO from formulating an adequate response in time (Giles, 2016: 6-12). Consequently, Russia managed to counteract and ultimately

eliminate the military superiority and advanced technical advantages held by both the United States and NATO through the adoption of this innovative concept of warfare (Renz, 2016: 291).

1.4.2. Low-cost Approach of Hybrid Warfare

The second criterion is that hybrid warfare is significantly more cost-effective compared to conventional military approaches. To reduce expenses, it is essential for actors to stay current with emerging technologies and integrate them into hybrid operations. Competent actors who can achieve this integration incur lower costs. States that invest in technological advancement can enhance their capabilities by allocating approximately one-third of their traditional expenditures towards this endeavour (Danyk, Maliarchuk, & Briggs, 2017: 23).

Cyberspace warrants further examination to understand why hybrid warfare is cost-effective. When considering primitive examples of hybrid warfare, it becomes evident that methods similar to modern hybrid warfare have been utilized in the past. One of the distinctive features of contemporary hybrid warfare is the prominent role of cyberspace. The use of the internet in hybrid warfare provides the aggressor with numerous additional capabilities, including fake news, disinformation, perception-building campaigns, propaganda, and cyberattacks. Thus, reduced costs become a significant factor influencing an actor's decision to engage in hybrid warfare (Treverton, Thvedt, Chen, Lee, & McCue, 2018: 9, 73).

ISIS exemplifies the efficient conversion of information into a weapon. By employing information warfare and propaganda tactics, it has reached millions of people worldwide, thereby glorifying its terrorist acts and recruiting numerous foreign soldiers (Wither, 2016: 76). James C. Pearce contends that while hybrid warfare has minimal economic costs, it still aims to achieve political and strategic objectives. In both conventional and hybrid wars, the ultimate goal is to persuade the opponent to accept our will. The nature of warfare remains unchanged in this context; the objective is constant, but the cost of attaining it has decreased (Pearce, 2019: 250).

1.4.3. Reduced Need for Traditional Large Armies

Thirdly, the advent of hybrid warfare has significantly altered the traditional dependence on large conventional armies to exercise control over a country or region. Historically, states had to deploy troops physically to occupy a territory and engage in activities within that region. However, hybrid warfare has considerably diminished the reliance on constraining factors such as manpower, time, and distance. The objective has shifted from the physical domination of territory to a more nuanced focus on exploiting the adversary's weaknesses (Danyk, Maliarchuk, & Briggs, 2017: 11).

The hybrid warfare approach demonstrates that it is no longer necessary to employ military force to compel the adversary into compliance with one's will. This strategy is both cost-effective and challenging to detect, which makes it particularly appealing. It captures the attention of not only the international community but also that of the aggressor's population (Cilluffo & Clark, 2012: 53). By adopting hybrid warfare, decision-makers can shield themselves from potential questioning by their own populace, at least until their actions are eventually noticed, if ever. This aspect is particularly crucial in liberal democracies, where war expenditures and casualties may lead to increased political scrutiny and potential repercussions for those in power.

In summary, hybrid warfare has introduced a transformative approach to exerting control over a country or region, reducing reliance on traditional constraints and shifting the focus to exploit the weaknesses of adversaries. This innovative approach offers benefits to the hybrid actor in terms of cost-effectiveness and challenges in detection. Furthermore, the ruling elites who engage in hybrid warfare are less likely to be scrutinized by their own citizens due to the difficulty in discerning such activities.

1.4.4. Anonymity Advantage of Hybrid Warfare

Last but not least, the anonymity of hybrid warfare is a significant factor that makes it appealing to aggressors, particularly state hybrid actors. Unlike non-state

groups such as ISIS, Al-Qaeda, and the Taliban, which often do not conceal their identities and objectives, state hybrid actors can maintain anonymity unless they choose to reveal themselves. The detection of hybrid strikes may be delayed or even impossible, leaving the responsible parties unidentified (Cilluffo & Clark, 2012: 50). States that wish to avoid the loss of troops and resources in traditional armed conflicts and are concerned about the reactions of the international community and their citizens may prefer to engage in hybrid warfare against their adversaries.

The anonymity of cyberspace, combined with a lack of effective regulation, allows it to become a valuable asset for military strategy. States organize, coordinate, and execute computer network attacks aimed at gathering information, disrupting information systems, and damaging the cyber infrastructure of other countries. By employing private individuals, companies, or other non-state actors to carry out these attacks, states can maintain a significant level of impunity in their cyber activities. The 2003 Titan Rain attacks and the 2007 cyber attacks on Estonia demonstrate that the absence of strong evidence linking the origins of these attacks prevented attributing responsibility to a foreign state (Reed, 2008). Russia has consistently maintained in the international arena that it has no connection to the forces fighting against the Ukrainian government in Donbas and has rejected any attempts to associate itself with them. In this context, the United Nations and NATO have been unable to find definitive evidence that the attacks were carried out by Russia and, consequently, have not been able to intervene. This serves as a prime example of the advantages provided by the anonymity of hybrid warfare (Muradov, 2019: 295).

In hybrid warfare strategy, the employment of paramilitary groups and cyberspace serves as key elements in preserving a state's anonymity. Hybrid warfare is executed to obstruct the attribution of hostile actions and to impede the enforcement of legal frameworks. Legal responses to hybrid warfare ought to encompass a reassessment of the attribution rules concerning non-state actors and their relation to state actions. This reevaluation aims to challenge states' assertions regarding the inapplicability of international law and non-attribution of illicit activities. Such reevaluation is not a novel development in international law, as international mechanisms have previously addressed analogous situations and proposed varying criteria for attributing behaviors (Uzun, 2017: 41-46).

1.5. DEBATES ON HYBRID WARFARE

Hybrid warfare, a prevalent term in contemporary discourse, has faced significant scrutiny. Upon its initial introduction, military communities neither embraced nor recognized the concept. Nonetheless, it has since become a term frequently utilized by policymakers (Hoffman, 2010: 441-442). Various factors contribute to the recognition of hybrid warfare in different areas. Certain analysts and scholars assert that contemporary conflicts cannot be understood through traditional frameworks, necessitating a novel concept that can accommodate these changes. They advocate hybrid warfare as a beneficial and relevant approach to elucidating future combat scenarios (Hoffman, 2009c). Notably, major organizations such as NATO, the European Union, and the United States Department of Defense have recognized hybrid warfare in official publications (Caliskan, 2019: 40). Despite its widespread acceptance, the debate surrounding hybrid warfare persists. Some scholars maintain that it is an inconsequential concept for comprehending the modern battle landscape. As a result, hybrid warfare has emerged as the most debated war concept of the past decade.

Since the introduction of the concept of hybrid warfare, this topic has been the subject of endless debate. The first debate concerns the novelty of the hybrid warfare concept. Scholars that suggest that hybrid warfare is not a novel concept assert that it can be witnessed in several wars throughout history, and they provide various historical examples to support their argument. Discussions surrounding hybrid warfare can be examined across six major topics.

The first discussion revolves around whether hybrid warfare is a novel concept or not. Scholars assert that the concept of hybrid warfare, although not unique, is essential and valuable for comprehending contemporary conflicts in the post-Cold War era (Weissmann, 2019: 25). The notion is not entirely new, as numerous wars have inherently involved both regular and irregular components at the strategic level. However, it would be inaccurate to categorize every battle featuring both regular and irregular elements as hybrid warfare. In previous conflicts, regular and irregular forces were deployed separately at distinct stages of the conflict. In contrast, modern wars, often referred to as hybrid warfare, integrate

regular and irregular components operationally and tactically on the same battlefield to achieve a synergistic effect (Hoffman, 2007: 8). Addressing these debates, Hoffman (2009) contends that the Vietnam War, the American War of Independence, the Spanish guerrilla war against the French Army, and the Arab uprisings against the Ottoman Empire should not be considered examples of hybrid warfare; rather, they exemplify compound warfare (Hoffman, 2009a: 36).

The second major discussion centres on the lack of consensus concerning the conceptual clarity of hybrid warfare. Numerous studies assert that the concept requires further clarification. Within the literature on hybrid warfare, there is no agreement on its definition, what it signifies, or the methods and equipment it encompasses. This ambiguity allows for varied interpretations of the concept. Consequently, due to the differing perceptions and misuse of the term, it has evolved into a catch-all phrase. Therefore, some scholars criticize hybrid warfare as a buzzword devoid of analytical value (Weissmann, 2019: 18; Reichborn-Kjennerud & Cullen, 2016: 1).

Thirdly, the concept of hybrid warfare requires further development to adequately explain contemporary conflicts, particularly Russian actions in Crimea and Ukraine. Some scholars contend that Hoffman's conceptualization of hybrid warfare fails to encapsulate Russia's course of operations. Despite being a term introduced in the 21st century, it struggles to clarify conflicts within its own era. This shortcoming naturally raises questions about the viability of the hybrid warfare concept (Giles, 2019: 1). Following the 2014 Russian annexation of Crimea, Hoffman acknowledged that the notion of hybrid warfare could not account for non-violent activities, such as economic, financial, and informational measures. The annexation of Crimea highlighted this deficiency. Consequently, NATO and the EU have introduced new criteria that encompass non-kinetic operations, including diplomacy, economics, and information (Caliskan, 2019: 12). While these concerns may be valid, it is crucial to recognize that the efforts of international and regional organizations to conceptualize hybrid warfare, particularly those of NATO, have significantly advanced the understanding of Russia's activities.

The fourth issue central to the discussions concerns the long-term sustainability of the hybrid warfare concept. Unlike conventional war, hybrid warfare

lacks tools and techniques that yield immediate results. As hybrid actors do not overtly infiltrate target countries and populations, achieving the desired outcomes takes time. Consequently, the effects require time to spread and become evident within the community of interest. Therefore, hybrid actors necessitate patience and consistency (Cilluffo & Clark, 2012: 50; Ozer, 2018: 51). In other words, only powerful actors possessing the requisite resources and weaponry can initiate and sustain hybrid warfare.

Fifth, a prominent topic of discussions within the literature on hybrid warfare is whether it constitutes a form of conflict or a strategy. Scholars, analysts, and authors are divided into two factions when examining hybrid warfare. Frank Hoffman is the most renowned advocate of the perspective that hybrid warfare represents a new form of conflict. He argues that the most striking transformation in the nature of contemporary conflict, specifically hybrid warfare, stems from the fusion and unification of combat traits. Hybrid warfare merges the lethality of state-to-state clashes with the zealous and enduring intensity of irregular warfare, forging a sophisticated and interconnected landscape at both operational and tactical levels. As a result, the notion of hybrid warfare ought to be viewed as a distinct form of warfare within the realm of international relations literature (Hoffman, 2009a: 36-37). Rod Thornton, another eminent figure in hybrid warfare studies, characterizes it as “a form of warfare characterized by 'blurring'... A feature of hybrid warfare is that the modes of conflict overlap and meld” (Thornton, 2015: 41).

On the other hand, some scholars contend that hybrid warfare has not yet fully established itself. They argue that not only hybrid warfare, but also other novel concepts must be assessed. As such, embracing hybrid warfare as a strategic concept or method of conflict may be an overstatement (Renz, 2016: 287). The narrow approach of hybrid warfare focuses solely on operations and tactics. All war conceptions must be based on a holistic viewpoint to be regarded as a new form of warfare. Regrettably, Hoffman's concept of hybrid warfare has not successfully integrated non-kinetic aspects of conflict, such as cyberattacks, economics, and information warfare. In this context, hybrid warfare proves more effective in understanding the military aspects rather than the entirety of war (Caliskan, 2019: 47-51).

The final argument concerns whether or not the concept of hybrid warfare legitimizes terrorism and crime. In 2007, when he originally conceptualized hybrid warfare, Hoffman made it clear that terrorist activities, corruption, and violence are involved in hybrid warfare. Hoffman maintains that hybrid warfare blurs the borders between war, criminality, and terrorism. Thus, its destructive force derives from violent acts (Hoffman, 2007: 8, 11, 29). Naturally, it would not be incorrect to assert that hybrid warfare develops criminal networks for users. The critical aspect here is how globalization affects these criminal networks. Current criminal networks acquire transnational dimensions in light of the opportunities brought by globalization. Besides, as a consequence of globalization, criminal networks with religious and ethnic affiliations receive more resources and recruit more soldiers (Schroefl & Kaufman, 2014: 862, 876). In addition to warlords, these international criminal networks may encompass gangs, drug smugglers, and hackers (Johnson, 2018: 146).

In conclusion, it is apparent that the concept of hybrid warfare encompasses criminal and terrorist actions that Western nations denounce for their use in conflict. Even more concerning, hybrid aggressors view crime and terrorism as objectives of the war, rather than threats to be mitigated. They regard illicit activities as tools for undermining the targeted society. By incorporating crime and terrorism, hybrid warfare has also obscured the boundary between the military and civilians (Angstrom, 2017: 841). Consequently, hybrid warfare, which involves a significant proportion of terrorist and criminal actions and accepts them as a necessary evil, has become the subject of extensive debate.

As can be clearly seen, hybrid warfare is still subject to criticism from various perspectives. The fact that the notion of hybrid warfare has not yet been fully comprehended and that a commonly accepted definition has not been put forth by academics and military researchers has fuelled these criticisms.

CHAPTER TWO

RUSSIAN HYBRID WARFARE: CRIMEA AND EAST UKRAINE

CASES

2.1. RUSSO-UKRAINIAN TENSIONS: UNRAVELING THE GEOPOLITICAL STRIFE

Numerous factors contribute to Russia's inclination to control the Ukrainian government and its territory. The foremost reason stems from the historical relationship between Russia and Ukraine. Historically, Russia has regarded Ukrainian territory as an integral part of its homeland. While Ukraine experienced occasional invasions by various states, the Russian Empire controlled a significant portion of Ukrainian territory from the mid-ninth century until Ukraine gained independence in 1917. However, this independence proved short-lived, as Ukraine, having seceded from Tsarist Russia, rejoined the Soviet Union under the Ukrainian Soviet Socialist Republic in 1919 (Schmidt, 2020).

The widely acknowledged historical, economic, geographical, and strategic significance of Ukraine to Russia is a topic of discussion among numerous politicians and statesmen. For instance, Adolf Hitler identified Ukraine and Leningrad as the focal points of Nazi Germany's assault on the Soviet Union during World War II. Conversely, Joseph Stalin sacrificed 600,000 soldiers to prevent the loss of Kyiv (Parker, 2005: 369-371). These examples underscore the enduring importance of Ukraine.

In 1991, Ukraine (then known as the Ukrainian Soviet Socialist Republic) separated from the Soviet Union and gained independence under the leadership of Leonid Kravchuk. Although Russia (previously the Union of Soviet Socialist Republics) was reluctant to recognize Ukraine as a sovereign and equal state, the Ukrainian government pursued a firm policy to maintain bilateral relations on an equal footing. Issues previously non-problems under Soviet rule emerged as points of contention between the two nations. For example, in 1954, Nikita Khrushchev transferred Crimea from the Russian Soviet Republic to the Ukrainian Soviet Republic. While this was not an issue under Soviet governance, Crimea's ownership

became problematic. Additional challenges in their relationship included the status of the Russian Black Sea fleet, the ethnic Russians living in Ukraine (approximately 8 million people), and energy supply concerns. Due to these and similar issues, relations remained troubled until 1997. However, the Treaty of Friendship signed in 1997 improved their relationship (Kappeler, 2014: 107-110).

On the other hand, even during periods of relatively amicable relations, Russia harbored concerns about the possibility of a pro-Western government taking power in Ukraine. 2004 the Orange Revolution erupted due to Viktor Yanukovych's electoral fraud. The revolution concluded when pro-Western politician Viktor Yushchenko became Ukraine's third president, validating Russia's apprehensions and initiating a tense period in their relationship (Cin, 2019: 93). In 2010, Viktor Yanukovych was elected as Ukraine's president. However, when he failed to fulfill his campaign promises of improving relations with the West, pro-Western protests began in November 2013 (Afineevsky, 2015). On February 23, 2014, the Ukrainian Parliament enacted legislation that banned Russian as a second language. However, they rescinded this decision in response to a significant backlash from the Russian-speaking population. This decision angered the Russian-speaking population and gave the Russian Federation a pretext to conduct military operations in Crimea to protect the Russian-speaking minority. These factors contributed to the tense relations and subsequent conflicts between the Russian Federation and Ukraine in recent years.

2.2. COMPARISON OF WESTERN AND RUSSIAN PERSPECTIVES ON THE UKRAINIAN WAR: AN ANALYSIS OF THE GERASIMOV DOCTRINE: WHY DOES RUSSIA WAGE A HYBRID WARFARE?

Although Russian and Western governments and institutions recognize the conflict in Ukraine as hybrid warfare, their perspectives differ significantly. The Russian government, media, and scholars argue that Russia is battling not only Ukrainian forces but also the West, particularly NATO, the United States, and the European Union. They contend that these Western entities attack Russia's national

interests by installing a puppet government in Ukraine (Müür, Pruulmann-Vengerfeldt, & Sazonov, 2016).

General Valery Gerasimov asserts that the West initiated a hybrid war in Ukraine, accusing it of attempting to overthrow undesirable governments and causing unpredictable regional consequences through tools like Color Revolutions, the Arab Spring, and soft power (Clark, 2020). General Gerasimov maintains that Russia had to employ hybrid methods to counter these attacks (Ulu, 2019). This sentiment is shared by the Russian government, media, scholars, and some Western scholars who hold the West responsible for the conflict in Ukraine. In 2014, John J. Mearsheimer articulated an argument stating that the Ukraine crisis resulted from provocation by the West, pointing to NATO's and the EU's expansion eastward and Western support for the 2004 Orange Revolution. The Eastern Partnership Project, launched by the European Union in May 2008, aimed to detach Ukraine from Russia's sphere of influence and integrate it into the EU's economy and policies. The West's liberal policies were viewed unfavorably by Russian leader Vladimir Putin, making the crisis in Ukraine inevitable (Mearsheimer, 2014).

On the other hand, many Western scholars argue that Russia's hybrid campaign in Ukraine is not solely about the EU's policies or the Color Revolutions. Russia has a history of supporting separatist movements in Ukrainian territory, predating the Orange Revolution. Tsarist Russia and the Soviet Union considered the Crimean Peninsula to hold symbolic and geostrategic importance due to past wars and victories. Furthermore, the Black Sea Naval Base is in Crimea, making it crucial for Russia's access to the Black Sea and the Mediterranean Sea. Russia began supporting separatist movements in Crimea between 1991 and 1992, immediately following the fall of the Soviet Union (Kilinskas, 2016).

Over the years, Ukrainian governments have generally appeared sympathetic to Russia when making political and economic decisions. In 1997, former Ukrainian President Leonid Kuchma signed the Treaty of Friendship, which granted Russia a 20-year lease of the Sevastopol Port for its Black Sea Fleet. Nevertheless, Russia has consistently perceived the rise of a pro-Western government in Ukraine as threatening its national interests. As a result, supporting separatist movements in Ukraine has been a longstanding contingency plan. Russia has promoted these

movements through the intelligence agencies of the Main Intelligence Directorate (GRU). Indeed, GRU agents intensified their activities when a pro-Western government assumed power after the Orange Revolution 2004. Russia's swift annexation of Crimea on March 18, 2014, without deploying regular troops, may have been the culmination of long-term preparations (Cin, 2019). Thus, although the annexation of Crimea by “little green men” seemed sudden, Russia's success resulted from years of meticulous and systematic intelligence, propaganda, and disinformation efforts to undermine the Ukrainian government and incite the local population. In this context, Russia endeavored to create a Russian-speaking population loyal to its culture through GRU activities in Crimea and Federal Security Service (FSB) operations in the Donbas region (Gök, 2019: 193-196).

Furthermore, a consensus among numerous scholars suggests that Russian hybrid warfare's doctrinal foundation in Ukraine originates in a 2013 piece written² by General Valery Gerasimov, the Chief of the Russian General Staff. In this research, Gerasimov examines the transformations in warfare in the 21st century. He contends that modern wars often commence without a formal declaration, leading to an increasingly indistinct boundary between war and peace. Gerasimov underscores the diminishing reliance on conventional armed forces and the growing significance of information, political, economic, and other non-military tools. The destructive, political, economic, and social effects of local populations' protest demonstrations on governments were evident during the Arab Spring. Additionally, a key characteristic of 21st-century conflicts is their clandestine nature. States no longer conduct overt operations or overtly deploy their forces; instead, they conceal their objectives behind peacekeeping missions and crisis management activities (Gerasimov, 2013).

General Gerasimov's article has divided scholars into two camps. Some authors assert that Russia employed the methods described in this article during the Ukraine crisis. Conversely, Russian thinkers argue that scholars began studying the works of Russian military thinkers after the annexation of Crimea, seeking works that could be cited as sources for Russian military doctrine. However, General Gerasimov's article neither mentions hybrid warfare nor military actions in Ukraine. It also fails to establish a roadmap for Russia's future warfare strategies. In essence,

² The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations

the article is an evaluation and analysis of contemporary wars. Gerasimov's article has been mistakenly and selectively cited as a doctrinal source for Russian hybrid warfare (Renz, 2016: 286). Moreover, from the perspective of Russian scholars, General Gerasimov endeavored to shed light on the West's new war strategies, which were evident during the Arab Spring and Coloured Revolutions (Arslan, 2019: 88).

Determining whether Gerasimov's article highlighted Western warfare strategies or outlined potential military methods for Russia's use in Ukraine presents a challenge. However, it can be observed that there has been a transformation in the Russian perception of warfare. Additionally, the Military Doctrine of the Russian Federation stated the need for a doctrinal transformation on February 5, 2010, three years prior to Gerasimov's article. According to the doctrine, the Russian Federation would prioritize information warfare and bring its information technologies to international standards to achieve its political goals without using military force. The doctrine focuses on the importance of information warfare, but it also mentions using non-military means such as economics, politics, diplomacy, and law to serve national interests.

The 2010 Military Doctrine of the Russian Federation acknowledges the possible use of military force but advises limiting its use as much as possible. The transformation in Russian military doctrine highlights the evolution of Russia's perception of war into hybrid warfare. Russia's use of hybrid warfare tactics and methods in Ukraine has allowed it to achieve its political goals without drawing the international community's or NATO's attention. Russia's limited economic power is a significant factor in its choice of hybrid warfare over conventional war (Arslan, 2019). Despite its aspirations to become a hegemonic power like the Soviet Union, its economic and military resources are insufficient. The Russo-Georgian War of 2008 exposed these weaknesses, and the experiences in Afghanistan and Chechnya further influenced Russian political elites to increase their capacity to conduct hybrid warfare (Veljovski, Taneski, & Dojchinovski, 2017: 297). Both battles resulted in negative political, economic, and military consequences for Russia, leading officials to understand that integrating diplomatic initiatives into military strength could achieve their desired results. Based on Russia's past experiences, its necessity for a

doctrinal change, and its economic and military vulnerabilities, it is understandable why Russia conducts hybrid warfare.

2.3. EXPLORING HYBRID WARFARE METHODS EMPLOYED BY THE RUSSIAN FEDERATION IN THE UKRAINE CRISIS

2.3.1. The Role of Russia's Cyberspace Activities in Conducting Hybrid Warfare: An Analysis of Tactics, Techniques, and Strategies

Cyberspace campaigns are a significant aspect of hybrid warfare. They refer to attacks on a target state's information technology by a state or non-state actor (Bachmann & Gunneriusson, 2015: 82). The tools, attack methods, and targets may vary based on the aggressor's capability to conduct a cyber campaign. For instance, the Russian Federation's cyber warfare against Ukraine encompasses intelligence activities, disinformation campaigns, control of information flow, discouragement of the target state's public, governors, and armed forces, perception operations, attacks on internet and telecommunications infrastructure, hacker attacks on civilians and public organizations, propaganda activities, and the use of social media and traditional media (Giles, 2019: 3). Russian cyber warfare in Ukraine can be divided into five categories for analysis.

2.3.1.1. Information Warfare and Disinformation Campaigns

The importance of the role of knowledge in wars is not new. Throughout history, many military strategists, commanders, and statesmen have emphasized the importance of using knowledge in warfare. In 1832, Carl von Clausewitz defined knowledge as the basis of all our ideas and actions during the war, encompassing everything known about the enemy and their country (Clausewitz, 2010: 139). Thirteen centuries before Clausewitz, Sun Tzu wrote that the supreme form of war subjugated the enemy using information rather than physical force. Additionally, Tzu highlighted the importance of spies, stating that they were the only reliable source of necessary information (Tzu, 2009: 11-55).

The primary goal in information warfare is to influence the behavior and perception of the enemy through controlling information. By conducting offensive information campaigns, the aggressor aims to force the enemy to retreat, surrender, or react at the wrong time (Waltz, 1998: 4-10). Today, the use of information has become much more complex and sophisticated. Information warfare is waged to manipulate the enemy and its population and shape the international environment and even the aggressor's population. In 2014, General Phil Breedlove, Supreme Allied Commander Europe, claimed that Russian information operations were the most impressive display of information warfare ever (Vandiver, 2014).

The success of Russia's information warfare against both Europe and Ukraine is fundamentally rooted in its robust media power. Possessing television and news channels broadcasting in Western languages, Russia has been enabled to conduct disinformation campaigns effectively, thereby proliferating its narratives within Europe. In contrast, the impact of Russian information warfare has proven significantly more potent and destructive in Ukraine. Key factors contributing to this phenomenon include the substantial market share held by Russian companies within the Ukrainian media landscape and the tendency of the Russian-speaking population in Ukraine to consume content predominantly from Russian channels (Rácz, 2015: 51-53).

Russia's operations during the Ukraine Crisis demonstrated that information manipulation and disinformation are crucial components of Russian hybrid warfare (Veljovski, Taneski, & Dojchinovski, 2017). Russia complicates accessing accurate information by promoting false narratives, thereby buying time for its activities before facing reactions from the international community. For example, during the two-week referendum in Crimea, Russia disseminated false information, claiming that the Ukrainian government had massacred civilians. As the international community struggled to obtain accurate information, this two-week period passed smoothly in Russia's favor, culminating in the annexation of Crimea (Cin, 2019).

The Colour Revolutions and the Arab Spring significantly influenced Russia's understanding of the importance of information manipulation. By controlling information, Russia aimed to suppress the voices of both internal and external opposition. The denial of responsibility for the shooting down of Malaysia Airlines

Flight 17 (MH17) is a prime example of information manipulation and disinformation. MH17, en route from Amsterdam to Kuala Lumpur, was shot down in Eastern Ukraine on July 17, 2014, resulting in the deaths of 298 civilians. Russia accused the Ukrainian Defence Forces and NATO allies of being responsible for shooting down MH17 and obfuscated the truth (Mulford, 2016). Immediately after the incident, Russian media propagated numerous conspiracy theories implicating the Ukrainian government. Komsomolskaya Pravda even broadcasted fabricated photos and videos to show the Ukrainian Defence Forces shot down MH17 (Mölder & Sazonov, 2018). In 2019, although Dutch prosecutors charged Igor Girkin, a former Russian intelligence officer, as the prime suspect, the incident remains unresolved (BBC, 2019).

Vladimir Putin and other high-ranking Russian military officials consistently denied the presence of Russian special forces in Ukraine since the inception of the crisis. On February 27, 2014, a specialized unit called “little green men” seized strategic buildings in Simferopol, Crimea. Subsequently, the little green men assumed responsibility for occupying other strategic buildings in various cities, managing transportation and logistical operations, pacifying Ukrainian troops, and conducting patrol activities. Despite speaking Russian, possessing Russian weapons, and wearing Russian military uniforms, the Russian government adamantly denied that these were not Russian soldiers. Putin even claimed that ordinary people could purchase Russian uniforms in local stores. Eventually, on April 17, 2015, Putin conceded that Russian special forces had intervened in Ukraine. Nonetheless, the systematic denial of Russian forces' involvement in Crimea allowed Russia sufficient time to capture strategic locations and orchestrate the Crimean referendum. Russia annexed Crimea without facing a robust international response (Snegovaya, 2015: 35).

2.3.1.2. Propaganda

Propaganda campaigns play a significant role in Russian cyber activities during the Russo-Ukrainian War. By investing billions of dollars, Russia strives to disseminate its narratives globally and establish its legitimacy. It funds channels

broadcast in Russian and various foreign languages to achieve this. Russian channels such as Komsomolskaya Pravda, TV Zvezda, and Regnum support Russia's agenda. These channels cater to the Russian population and Russian speakers in the former Soviet Union territory. They aim to incite Russian-speaking individuals against Ukraine and the West and justify Russian arguments by portraying the war as a crime perpetrated by the West (Sazonov & Müür, 2016: 66-94). Furthermore, globally recognized channels like Russia Today, Channel One, and Sputnik News emphasize the legitimacy of the Russian government with their broadcasts in foreign languages (Mulford, 2016). Russia's efforts to assert its righteousness to its people and the world stem from its reluctance to face backlash from the international community.

In addition to investing heavily in traditional media propaganda, Russia effectively utilizes the internet as a powerful tool. It employs individuals called trolls for internet propaganda purposes. These trolls are tasked with spreading false news and stories on the internet. Their effective deployment has been observed during conflicts in Eastern Ukraine, where they conducted intense propaganda against Ukraine and the West, particularly on websites like VKontakte and Odnoklassniki (Arslan, 2019: 103-108). Moreover, world-renowned social media platforms such as Twitter, Facebook, and YouTube have also been exploited by Russian trolls for propaganda purposes.

Both conventional media outlet propaganda and social media propaganda frequently emphasize historical elements. They accuse Maidan insurgents and the provisional Ukrainian government of being pro-Nazi. In doing so, Russia keeps the memory of the Soviets' crucial victory against the Nazis alive. These accusations are not limited to the Ukrainian government and insurgents; they also label the Ukrainian Defense Forces as Nazi execution squads. Alongside these allegations, the Jewish community and Ukrainian government leaders are portrayed as fascists (Reisinger & Golts, 2014).

2.3.1.3. Intelligence Activities

Another component of Russian cyber warfare encompasses the activities of intelligence services. Following the dissolution of the Soviet Union, Ukraine

regained its independence in 1991. Until the early 2000s, Russia encountered no difficulties in obtaining intelligence about Ukraine, as Soviet intelligence units continued to operate within Ukraine even after the Soviet Union's collapse. Additionally, historical ties between Ukraine and Russia contributed to Ukrainian officials' willingness to share information with Russia. Despite this, Russia persisted in its covert intelligence activities, driven by concerns that Ukraine would abandon the Russian axis and adopt pro-Western policies. The 2004 Orange Revolution marked a turning point in the relations between the two countries and the activities of intelligence services. From that point onward, Russia decentralized its intelligence operations against Ukraine, primarily focusing on Crimea and Eastern Ukraine. Russian agents collaborated with locals who were anti-Ukrainian and sympathetic to Russia's policies. Some local community members provided intelligence to Russia, aiding in establishing a pro-Russian demographic. This group included orthodox individuals who embraced “the Russian World” concept, separatists, individuals nostalgic for the Soviet era, and criminal paramilitary forces (Horbulin, 2017: 45-52).

Russia possesses numerous institutions capable of conducting information operations. The Federal Agency of Government Communication and Information organization operated from 1993 to 2004 and had extensive authority and 54,000 employees. This organization was responsible for counterintelligence, information acquisition, cybersecurity, technical intelligence, information protection, and telecommunications. However, when it was revealed that the organization was involved in corruption, it was disbanded, and four new organizations were created: the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), the Federal Protection Service (FSO), and Military Intelligence (GRU). The resources and responsibilities of the defunct organization were distributed among these new institutions. These four organizations employ over 300,000 personnel (Fabian, 2019).

Among these four organizations, the FSB and GRU, in particular, played crucial roles in the Ukrainian Crisis. While the FSB was responsible for conducting intelligence activities in Eastern Ukraine, the GRU's area of operation was Crimea. Both intelligence services executed operations exploiting economic, political, ideological, ethnic, and religious issues to undermine the Ukrainian government

(Gök, 2019: 193-194). As a result of the extensive activities of Russian intelligence services in Crimea and Eastern Ukraine, the region's populace lost confidence in the Ukrainian government. Moreover, Russian special forces infiltrated protests against the Ukrainian government, provoking the demonstrators and escalating the protests into separatist riots (Cin, 2019: 93-95).

From the outset of the Ukraine Crisis, Russia has consistently denied the involvement of its special forces and intelligence services. However, Roman Filatov, a GRU official, and his three colleagues were arrested while gathering military intelligence in Northern Crimea. The Security Service of Ukraine (SBU) interrogated Roman Filatov, who confessed to being a GRU official. Sergei Shoigu, the Russian Minister of Defence, negotiated with the Head of the Ukrainian Presidential Administration, Sergei Pashinsky, to return Roman Filatov to Russia. As a result of the negotiations, eight Ukrainian prisoners held by Crimean separatists and Ukrainian Rear Admiral Serhii Haiduk were returned to Ukraine by Russian officials (Renz & Smith, 2016: 28-29). This incident not only confirmed the involvement of Russian agents in Ukraine but also exposed the Kremlin's cooperation with Crimean separatists.

2.3.1.4. Hacker Attacks

Lastly, hacker attacks also play a significant role in Russia's cyberspace activities for two main reasons. First, hacker attacks are exceedingly difficult to detect. The Russian government may deny responsibility even if the perpetrators of such attacks are identified. In other words, hacker attacks do not directly result in consequences that would hold Russia accountable under international law (Connell & Vogler, 2016). Since the international community primarily focuses on regulating physical space, international law has yet to determine the repercussions of cyberattacks (Bargiacchi, 2020). The second reason is that hacker attacks are both more accessible and more cost-effective than physical assaults. Furthermore, most hackers employed for such purposes are not on the Russian government's payroll. Instead, the Russian government enlists the services of patriotic and nationalist individual hackers when necessary.

Russian hacker attacks are sophisticated, with hackers stealing information and weaponizing it. On numerous occasions, they have published altered stolen documents from the Ukrainian government on websites such as VKontakte to serve their propaganda purposes (Horbulin, 2017: 19). Research indicates that Russian hackers targeted the Ukrainian government in at least five cyberattacks between 2013 and 2017 (Treverton, Thvedt, Chen, Lee, & McCue, 2018: 28). Moreover, the Russian government can coordinate hacker attacks with military offensives. Some cyberattacks have occurred during critical moments in the Ukraine conflict, such as parliamentary elections, the Maidan protests, and the entry of Russian forces into Crimea.

“Russian hackers have employed spear phishing, malware, DDoS attacks, telephone denial of service (TDoS) attacks, and other forms of cyber disruption and espionage to conduct a steady barrage of cyberattacks targeting Ukraine's government, military, telecommunications, and private-sector information technology infrastructure” (Connell & Vogler, 2016: 14).

Russian hackers have employed various methods to attack Ukraine. For instance, they interfered in Ukrainian elections and attempted to manipulate the results. On May 22, 2014, Russian hackers targeted the Election Commission just two days before the Ukrainian presidential election. Another hacking attack occurred on election night when they infiltrated the Central Election Commission's server and tried manipulating the commission's website to announce a right-wing extremist and pro-Russian candidate as the winner (Costea, 2020: 54).

Moreover, Russian hackers targeted the Ukrainian government and governmental agencies aimed at soldiers and their families. They sent messages to Ukrainian soldiers fighting in the ATO Region (Anti-Terrorist Operation Area), urging them to go home or die in vain. These messages were designed to discourage soldiers from fighting, convincing them that their commander had fled and no help would come. Similarly, the soldiers' families were targeted; Russian hackers sent messages informing them that their husbands and children had been killed or captured (Mölder & Sazonov, 2018).

Furthermore, Russian hackers carried out cyberattacks aimed at the Ukrainian population. For example, days before the Ukrainian parliamentary elections, pro-Russian and nationalist hacker groups like Cyber Berkut hacked several electronic billboards in Ukraine. Cyber Berkut posted a video on these billboards accusing the

Ukrainian government of being responsible for the war (Svetoka, 2016: 12). The group aimed to erode the Ukrainian people's confidence in their government. During the Ukraine Crisis, Russian hackers did not solely target the Ukrainian government's websites and soldiers; they occasionally attacked countries that provided political support to Ukraine. In early January 2015, Cyber Berkut hacked the German government's websites due to Berlin's political backing of the Ukrainian government. Additionally, this hacker group infiltrated three NATO websites and the websites of the Polish and Estonian governments (Pawlak & Petkova, 2015).

2.3.2. Economic Pressure and Ukraine's Dependence on Energy

Ukraine's foreign trade has historically depended on Russia due to its limited number of trade partners. Additionally, Russia has made Ukrainian producers and consumers reliant on itself by imposing low custom tariffs on Ukraine. In 2013, Ukrainian trade with Russia accounted for 30.19 percent of its imports and 23.81 percent of its exports (World Integrated Trade Solution, 2021). In this context, Russia has used its economic power as a means of pressure on Ukraine not only during wartime but also in peacetime. Although economic pressures are not a standard method of hybrid warfare, the dependence of the Ukrainian economy on the Russian economy has allowed Russia to use economic pressures against Ukraine as a tool of hybrid warfare. According to an agreement signed in 1997, the Sevastopol Port was leased to Russia's Black Sea Fleet under the Treaty of Friendship until 2017. In 2010, Yanukovich's government extended the right to use the port by signing the Kharkiv Pact until 2042 in exchange for a 30% discount on natural gas (Harding, 2010).

Moscow has employed its economic power and Ukraine's dependence on Russian energy as a foreign policy tool. In July 2013, the Russian government levied an extra tax on Ukrainian steel products, and later, the Ministry of Health of the Russian Federation banned the import of confectionery from Ukraine. In September, the Russian government suspended the licenses of Ukrainian transportation agencies. In November 2013, Yanukovich's administration was expected to sign an Association and Free-trade Agreement with the EU, increasing trade with European

countries and reducing Russia's share in foreign trade. After Yanukovych's government announced its intention to sign the free-trade agreement, Russia began imposing harsh economic sanctions against Ukraine (Horbulin, 2017: 59-60). Ultimately, the Ukrainian government did not sign the agreement due to fear of Russia's economic and political sanctions. Pro-European protesters gathered in Maidan of Independence to demonstrate against Yanukovych's pro-Russian policies (Schmidt, 2020).

After that, in December 2013, Russia offered to write off Ukraine's debt, valued at 15 billion American dollars, and reduce the price of natural gas by one-third in order to curb pro-European protests. However, these measures were insufficient to halt the Euromaidan protests, and the first Yatsenyuk Government—a pro-European provisional government—took office in February 2014. The pro-European nature of the new government prompted Russia to increase its economic pressure on Ukraine further. On March 31, 2014, and April 3, 2014, Moscow raised the price of natural gas twice, resulting in a total increase of 80 percent (Arslan, 2019: 130-131).

Between 2014 and 2015, Moscow significantly intensified its pressure on Ukrainian producers. It deliberately extended customs controls for perishable goods such as dairy products, maize, and potatoes for 15 days, resulting in losses for Ukrainian manufacturers as their products perished at customs. In 2016, Russia excluded Ukraine from the Most Favoured Nation (MFN)³ status and implemented the classic tariffs agreed upon by the Customs Tariff of the Eurasian Economic Union. Furthermore, the Russian government inflicted heavy losses on the Ukrainian economy by placing an embargo on several Ukrainian products and preventing the transit of these goods to Asian countries (Horbulin, 2017: 59-61).

The control and disruption of energy supply is another hybrid warfare method employed by Russia, targeting not only Ukraine but also Southeast European states and the Baltic States. Many European and Baltic states depend on Russian energy

³ The Most Favoured Nation (MFN) status refers to a state granting certain privileges, such as low tariffs, to any of its trade partners. However, the World Trade Organization (WTO) has regulated this principle to prevent discrimination. According to the WTO's regulation, if a state treats one trade partner as most favoured, it must extend the same treatment to all WTO members. For more details, please consult the following resources: https://www.wto.org/english/thewto_e/w-hatis_e/tif_e/fact2_e.htm#seebox and https://www.wto.org/english/res_e/webcas_e/ltt_e/ltt1_e.htm.

sources, particularly natural gas. The Russian government has exploited its energy resources to destabilize and pressure undesirable governments. For instance, Russia twice attempted to undermine Ukraine's pro-Western governments and politicians by cutting off the natural gas supply in 2006 and 2009 (Treverton et al., 2018: 66).

After the Ukraine Crisis began, Russia conducted several operations to break the resistance of the Ukrainian government. For example, “little green men” and paramilitary forces occupied energy distribution facilities and infrastructure during the annexation of Crimea. As a result, Russia both damaged the Ukrainian economy and profited from exploiting these resources. Moreover, Russian forces targeted Ukrainian energy infrastructure to disrupt the energy supply when military operations commenced in Eastern Ukraine (Ratsiborynska, 2016: 15).

The seizure of properties in the energy sector by “little green men” and local militias has resulted in the loss of billions of dollars for Ukrainian publicly owned corporations and private companies. During the annexation of Crimea, Ukraine's National Energy Ukrenerho Company alone lost assets worth \$1 billion (Horbulin, 2017: 69). According to a report published by the Ukrainian Energy Ministry, Ukraine lost 80 percent of its national oil and gas deposits because of Crimea's annexation (Cohen, 2019).

2014 Russia supplied five times less natural gas to Ukraine in 2013. Moreover, gas prices increased by 70 percent because Russia canceled discounts it had applied in previous years. Due to the cost of new prices and insufficient supply, Ukraine had to use its stored natural gas. Furthermore, Dmitry Medvedev, the former Prime Minister of the Russian Federation, claimed that the Kharkiv Pact was abolished because Crimea was separated from Ukraine through a legal referendum. As a result, the Ukrainian government was required to pay back past years' discounted natural gas prices, amounting to 11 billion American dollars (Wierzbowska-Miazga & Sarna, 2014).

In addition, almost 3% of Ukraine's GDP consists of transit fees for natural gas from Russia to European countries. However, Russia and Germany agreed to build the Nord Stream 2 Pipeline⁴, which bypasses transit countries, in September

⁴ In 2005, Russia's largest natural gas company GAZPROM and German companies BAFT and E.ON agreed in principle to construct North European Gas Pipeline (it is now named as Nord Stream 2). The pipeline will bypass transit countries such as Ukraine and Poland because it passes under of the

2005. With this pipeline, Russia can supply its natural gas directly to Germany (Schoen & Krijger, 2019). When the pipeline construction is completed, Ukraine's economy, which has suffered from Russian hybrid warfare for years, will face additional economic challenges.

It can be asserted that Russia employs its economic power and Ukraine's dependence on natural resources as an effective hybrid warfare tool. It appears that Russia utilizes economic sanctions as a hybrid weapon to diminish the Ukrainian people's support for their government and weaken the Ukrainian government's resistance.

2.3.3. Deployment of Conventional Forces

As previously mentioned, hybrid warfare does not signify the disappearance of conventional forces. Some scholars argue that the aggressor may deploy its conventional forces if hybrid methods fail to yield the desired results. This misperception persists, suggesting that conventional forces must provide an alternative to hybrid warfare. However, deploying conventional forces is not an alternative to hybrid warfare but rather an instrument of it. In his 2007 article, Hoffman also asserted that hybrid warfare encompasses conventional capabilities (Hoffman, 2007: 29).

Although conventional forces are part of hybrid warfare, they no longer play the primary role in conventional wars. General Valery Gerasimov anticipated this development, contending that conventional armies would be relegated to a secondary role in future conflicts (Gerasimov, 2013). The Ukraine Crisis confirmed General Gerasimov's predictions, as Russian conventional forces largely remained in the background to obscure direct Russian intervention. In the Ukraine Crisis, irregular forces took on the leading role. These irregular forces, comprised of Russian separatists and "little green men," captured nearly 190 Ukrainian military positions.

Baltic Sea and delivers Russian gas directly to Germany. Although, many Western governments, especially Washington, see the pipeline as a project that weaken European energy security, the project is scheduled to be finished in 2021. For more detail, see <https://www.nord-stream2.com/>, <https://www.gazprom.com/about/history/>, and <https://www.dw.com/en/nord-stream-2-us-warns-companies-to-immediately-abandon-work/a-56920315>.

In doing so, they received equipment assistance from Russia, but no conventional physical force was deployed (Arslan, 2019: 9-11).

Hybrid warfare is inherently flexible and does not adhere to a single, rigid operational plan. Concurrently, the instruments and methods of hybrid warfare can be employed in various ways to serve the same objectives. Russian conventional forces pursued two different courses of action during the hybrid war in Ukraine.

2.3.3.1. Russian Military Drills and Construction of Military Buildups on Ukrainian Borders

The first course aimed to discourage the Ukrainian army from fighting, slow military decision-making, engage in military deception, intimidate the Ukrainian government, and deter NATO members from military intervention. Military drills were the most effective means for Russian conventional forces to fulfill these duties. Russia conducted eight major military drills between February 2014 and October 2015, excluding nuclear force and joint exercises, in its territory and adjacent areas.

The military drill conducted on February 26, 2014, is significant due to its timing, scope, and the number of personnel and equipment involved. The Russian Army deployed 150,000 land, navy, and air force personnel, 90 aircraft, 120 helicopters, 880 tanks, 1,200 other pieces of equipment, and 80 warships, with the drill taking place in a 500 km² area near the border with Ukraine (European Leadership Network, 2016). Moreover, the timing of the military drills was crucial for the annexation of Crimea. Pro-Russian separatists in Crimea initiated military activities, such as blocking roads and seizing strategic buildings, on February 26, 2014. This synchronicity suggests a planned strategy rather than a coincidence. The Ukrainian Army dispatched its troops to the Russian border to protect its territory from potential Russian attacks. With most troops sent to the border, no robust military structure remained in Crimea capable of resisting the separatists. Separatist forces gained an advantage over Ukrainian forces in their military operations in Crimea. The military drill also showcased Russia's commitment to supporting Ukrainian separatists and signaled to the Ukrainian government and NATO allies that Russia would invade Ukrainian territory if necessary (Kilinskas, 2016: 152).

Furthermore, the timing of the military drill conducted in April-May 2014 is also noteworthy. On May 25, 2014, the Ukrainian people were set to go to the polls to achieve political stability and restore public confidence. During this critical period, Russia aimed to create insecurity and uneasiness among the Ukrainian people and army by conducting a military drill involving 40,000 troops and multiple battalion tactical groups on the Ukrainian border. Russian conventional forces attempted to intimidate the Ukrainian government and demonstrated their determination regarding Ukraine by conducting air harassment of NATO allies and neighbors (Veljovski, Taneski, & Dojchinovski, 2017: 297).

Additionally, the Russian government aimed to instill fear in the Ukrainian government and population, employing other methods. Russia's military drills were predominantly snap exercises, most lasting no longer than a week. Russia established military buildups along Ukraine's eastern borders to maintain constant military pressure on the Ukrainian government. In April 2014, satellite photos revealed that Russia had embarked on a massive military buildup, including fighter planes, helicopters, artillery, infantry, and special forces, in an empty field 50 km from the Ukrainian border. It became apparent that the Russian Army had not established military buildups in just a single region. Subsequently, new satellite images revealed that Russia had initiated buildups in different cities, such as Buturlinovka (roughly 150 km from the Ukrainian border) and Belgorod (40 km from the Ukrainian border). Approximately 35,000 to 40,000 Russian soldiers were estimated to serve in these buildups. Brigadier Gary Deakin, a NATO official, argued that these troops could be ready for battle within 12 hours (Cendrowicz, Harding, & Luhn, 2014). Therefore, their presence on the borders was not only to intimidate the Ukrainian government but also to demonstrate to the world that Russia could invade Ukraine if necessary.

On the other hand, Kyiv was not inclined to escalate military tensions with Russia and thus kept its massive military buildups away from Russia's borders. Initially, the Ukrainian government deployed small military troops and patrol bases on the border but later had to increase the number of buildups. The Ukrainian Army relocated most troops from the Crimean Peninsula to its eastern border. As

mentioned earlier, the movement of Ukrainian troops from west to east facilitated the separatists' annexation of Crimea (Kasapoglu, 2015: 6-12).

2.3.3.2. Direct Intervention of Russia's Conventional Forces in Ukraine

On May 25, 2014, Petro Poroshenko assumed the mantle of presidency in Ukraine. Before Poroshenko's term, Ukraine grappled with significant political instability, leading to many misguided military decisions. Nevertheless, with the advent of the 2014 election, Ukraine has since found political equilibrium, subsequently translating into several military victories against pro-Russian separatists (Ulu, 2019: 102). In the summer of 2014, pro-Russian paramilitary groups and Russian special forces seemed distant from their anticipated military triumphs. The Ukrainian Army, especially in Eastern Ukraine, achieved a series of accomplishments, reclaiming sites like Donetsk Airport, which was previously captured by paramilitary groups in the nascent stages of the war.

Russian authorities recognized their inability to attain their political objectives when the engagement of conventional forces was not part of their conflict strategy. Russia deployed its 18th Army Brigade, composed of an estimated 3,000 to 4,000 soldiers, to the Donetsk and Luhansk region. However, these soldiers operated as battalion tactical groups, refraining from launching full-scale attacks, as Russian officials persistently denied their army's involvement despite compelling evidence to the contrary. Even when Russian paratroopers were captured, or Russian soldiers were reported killed in the Ukrainian city of Mariupol, Russian officials maintained their denial, insisting that the soldiers involved were volunteer fighters who had independently crossed the border to combat the so-called fascist Ukrainian government and were not acting under Russian command. The narrative suggested that these soldiers were off duty, having inadvertently crossed the border while on vacation. Russian authorities have exerted substantial effort to negate any insinuations of Russia's engagement in the war. Hence, Russian conventional forces curtailed their offensive against the Ukrainian army in Mariupol in August 2014 despite their tactical superiority. Their objective was to persist in their denial of Russian involvement and to sway the international community's opinion in their favor (Reisinger & Golts, 2014: 1-7).

Despite Russia's staunch denial of its conventional forces' involvement in the conflict, there have been sightings of Russian military hardware in Ukraine. Moscow frequently employed ground forces, which are harder to detect than air forces. Artillery units assumed a more prominent role, predominantly utilizing tank battalions. Various series of Russian-manufactured tanks have been observed in Ukraine, including the T90, T80, and T72 series. Moreover, motorized rifle battalions played crucial roles in numerous operations. These battalions have employed the BTR-90 armored personnel carrier, the BMP-3M amphibious infantry fighting vehicle, and the 9P162 Kornet anti-tank missile carrier. Additionally, the Russian Armed Forces have deployed a range of rocket and artillery systems in Ukraine. Some of the more notable ones include SS-26 Stone (Iskander-M), 2S35 Koalitsiya-SV SP Artillery and BM-30 Smerch MLRS. In addition to employing offensive weaponry designed to inflict physical damage on the Ukrainian army, Russian conventional forces also used air defense systems such as SA-11 Gadfly (BuK-M1-2), along with anti-access systems like 55Zh6UE NEBO-UE and TOR-M1 (Asymmetric Warfare Group, 2016: 5-26).

In 2015, Dr. Phillip Karber, President of the Potomac Foundation, attended “The Russian Military Forum: Russia's Hybrid War Campaign: Implications for Ukraine and Beyond,” organized by the Center for Strategic & International Studies. As a discussant, he presented documented evidence of Russia's military and economic aid to the separatists. According to these documents, various weaponry from Russian conventional forces was provided as military aid to irregular forces in Ukraine. This aid included Russian APCs (specifically the BTR-80, an 8x8 wheeled amphibious armored personnel carrier), BM-21 Grad MRLS Field Rocket Systems, Russian man-portable air-defense systems (MANPADS), anti-tank missiles, mines, and sniper rifles. Additionally, irregular forces known as “little green men” were photographed with Russian military equipment, including Russian rifles, state-of-the-art Russian Kevlar helmets, level-four body armor, and flash suppressors. Russia's contribution to the conflict extended beyond merely deploying its conventional forces and equipment; it also provided financial assistance to the separatists. Ukrainian officials intercepted a \$2.8 million consignment intended for the separatists at the Goptoka checkpoint on July 10, 2014 (Karber, 2015).

Furthermore, Unmanned Aerial Vehicles (UAVs) such as the Orlan-10 drone, Forpost (the largest serial drone in the Russian armed forces), and the Dozor-100, all belonging to the Russian Army, have been deployed for reconnaissance and offensive missions. Russian conventional forces have primarily employed these drones to pinpoint the locations of Ukrainian troops, subsequently subjecting them to artillery bombardment. In addition, Russian forces have used UAVs to ignite the frontline positions of Ukrainian soldiers, and a second wave of UAVs has been unleashed on the soldiers who expose themselves while attempting to escape the fire (Asymmetric Warfare Group, 2016: 26-28).

It is essential to underscore that Russia did not resort to employing its conventional forces merely when hybrid warfare tactics proved ineffective. Instead, conventional forces were used concurrently with irregular forces, in alignment with the principles of hybrid warfare. Moscow has strategically leveraged the timely deployment of conventional forces while denying Russian involvement.

2.3.4. Deployment of Irregular Forces

While the involvement of Russia's conventional forces in the Ukrainian Crisis was significant, it is arguable that they served in a supporting role. The role of irregular forces, which achieved notable successes such as the annexation of Crimea, should not be underestimated. These forces, markedly active in Eastern Ukraine in support of Russia, have been integral from the inception of separatist protests until the summer of 2014 when the Ukrainian Army started to advance militarily. The composition of these irregular forces was diverse, encompassing special forces (Spetsnaz⁵), mercenaries, pro-Russian local militias, private military corporations, and organized crime networks, collectively marshaling approximately 25,000 individuals against Ukrainian forces on Russia's behalf (Gardner, 2015: 10).

Owing to the elusive nature of hybrid warfare and the obfuscation caused by Russia's disinformation campaigns, ascertaining which irregular force entities performed specific tasks can be challenging. Nevertheless, some documented activities include occupying strategic positions such as the Crimean Parliament,

⁵ Proper noun of Russian special forces; it means special purposes units in Russian language.

Simferopol Airport, Belbek Airport, certain Simferopol's Council of Ministers buildings, and Donetsk and Luhansk airports in Eastern Ukraine. However, their operations extended beyond merely seizing control of strategic locations. Irregular forces also set up roadblocks and checkpoints, disrupted communication and internet infrastructure, and incapacitated Ukrainian law enforcement and local authorities from taking effective action (Kilinskas, 2016: 152-153; Mulford, 2016: 102).

These actions, in particular, an attack on the Ukrainian Navy at the Sevastopol Port, underscore the importance of irregular forces in the Ukrainian Crisis. Typically, such operations would be executed by a conventional army, yet, during the Ukrainian Crisis, irregular forces exhibited characteristics more commonly associated with conventional forces (Kilinskas, 2016: 153-155). This mimicry of conventional military activities can be seen as a strategic measure by Russian officials to obscure their involvement and limit the presence of Russian regular forces on Ukrainian territory unless necessary.

Among the constellation of irregular forces operating in Crimea, a group colloquially termed the 'little green men' stands out due to its unique characteristics. This unit, which primarily communicated in Russian, was noted for its use of Russian military uniforms and equipment and its explicit support for pro-Russian separatists. The unit first appeared on February 27, 2014, taking control of strategically significant buildings in Simferopol (Veljovski, Taneski, & Dojchinovski, 2017: 299). Simultaneously, the Crimean Parliament was seized by the 'little green men,' with a parliamentary session subsequently convened under the auspices of armed control. This session resulted in the dismissal of Anatoli Mogilev and the installation of Sergei Valeryevich Aksyonov, a pro-Russian figure associated with organized crime, as the new president of Crimea (Cin, 2019: 87-88; Gök, 2019: 151). The detachment of Crimea from Ukraine was subsequently actualized via a referendum, and within two days, the Crimean Parliament announced the peninsula's incorporation into Russia.

From the initial appearance of the "little green men" in Crimea, Russian President Vladimir Putin staunchly denied their association with the Russian armed forces or any form of Russian employment. According to Putin, these soldiers were essentially patriotic militias expressing their resistance to what they perceived as a

fascist Ukrainian government. Furthermore, Putin contended that Russia did not supply the equipment and uniforms worn by these little green men. Instead, he suggested, they had seized weapons from Ukrainian soldiers and procured their military uniforms from local clothing outlets. After a series of persistent denials and a web of disinformation campaigns, Putin ultimately conceded to the involvement of Russian special forces in the Crimean events on April 17, 2015 (Snegovaya, 2015: 17).

Despite the significant role of the little green men in the Ukraine Crisis, it is essential to underscore that most of their operations were limited to the Crimean Peninsula. In contrast, the armed conflict in Eastern Ukraine was primarily propelled by pro-Russian and separatist militias up until the summer of 2014 (Clark, 2020b: 8; Reisinger & Golts, 2014: 8). These militias conducted several operations in the Donbas region, including the capture of strategically essential buildings such as Donetsk City Hall, direct engagement with Ukrainian law-enforcement officers, occupation of Donetsk and Luhansk Airports, and the utilization of proprietary broadcasting channels like *dnr-news.com* and *novorus.info* to propagate anti-Ukrainian government sentiments (Müür, Pruulmann-Vengerfeldt, & Sazonov, 2016: 1; Renz & Smith, 2016: 29; Mulford, 2016: 102). These separatist militias were backed by Russia and certain Ukrainian oligarchs who had profited during the Yanukovych government and held considerable unease towards the politics of the new anti-Russian government. These oligarchs also maintained commercial relationships with Russia and thus sought to curry favor with the Kremlin by supporting local militias (Horbulin, 2017: 41).

Despite overlapping interests between the militias and Russia concerning Ukraine, controlling these militias presented a considerable challenge. Certain right-wing factions within the militias accused Vladimir Putin of treachery, citing insufficient support for the Novorossiia Project⁶. The shooting down of Malaysia

⁶ Novorossiia means 'New Russia' in Russian language. The term, which first appeared 250 years ago, was the name of a new Russian province (*guberniya*) whose political centre was Odessa. Later, Novorossiia *guberniya* had expanded and included different regions. Even if its exact borders are not known, Russian written sources refer to Bessarabskaya, Khersonskaya, Tavricheskaya, Yekaterinoslavskaya, the Region of the Don Army, and Stavropol regions as Novorossiia. In 2014, the term of Novorossiia had been reutilized as historical, religious, and separatist geographical project. On the strength of the term of Novorossiia, Russian separatists and Russian officials have sought to emphasize the historical past of the Donbass region with Tsarist Russia. On 24 May 2014,

Airlines Flight 17 (MH17) by pro-Russian militias using a Russian-made SA-11 anti-aircraft missile underscored the potential danger that uncontrolled militias posed to the international community and civilians alike (Mulford, 2016: 102). Separatist militias in the Donetsk and Luhansk regions declared their secession from Ukraine, a move not favored by Russia. The Kremlin preferred these regions to have a special status. In contrast, Kyiv contended that this would lead to their separation (Gardner, 2015: 11). Ultimately, in line with the Minsk II Agreement, the Ukrainian Constitution underwent reforms to accommodate a more decentralized structure, resulting in Donetsk and Luhansk receiving interim local self-governance status (Minsk II, 2015).

Another irregular force element that acted on behalf of Russia in the Ukraine Crisis was organized crime networks. Post-Soviet Ukraine grappled with many mafia families and crime clans, mainly due to the legacy of the Soviet Union's deeply entrenched mafia state. Organized crime networks were particularly prevalent in Crimea and, more notably, the Donbas region. Since the mid-1990s, organizations such as Seilem, Sheviov, and Bashmaki have remained active in Crimea (Williams & Picarelli, 2002: 47-55). Additionally, the Donetsk clan, one of the largest criminal organizations, dominated the Donbas region (Zimmer, 2005). These networks played a pivotal role in Russia's hybrid warfare strategy.

Due to the extensive involvement of many individuals in Crimea and Donbas in these crime networks, Russia gained the upper hand. Leaders of these organized crime networks pledged support for separatists and Russian special forces in exchange for financial gain. For instance, Solntsevo, one of Donbas's most influential and dangerous criminal networks, supported separatists and special forces during conflicts. Additionally, they spread fear and terror by targeting patriotic Ukrainians who supported the Ukrainian government. Another motivation for the criminal organizations' backing of separatists was the economic benefits a politically unstable Ukraine offered. These organizations exploited the Sevastopol Port of Crimea and Odesa Harbour of Ukraine for illicit activities such as drug smuggling, human

Federal State of Novorossiia Union of People's Republics has been established as a confederation by the merger of Donetsk People's Republic and Luhansk People's Republic. Federal State of Novorossiia Union of People's Republics is considered as a de facto state. For more detail, see also O'Loughlin, J., Toal, G. and Kolosov, V. (2017). 124-144; Toal, G. (2017).

trafficking, arms smuggling, and exporting stolen vehicles to other countries (Mulford, 2016: 99).

Through the examination of Sergei Valeryevich Aksyonov's journey, from leading the Seilem crime organization and overseeing smuggling operations in Sevastopol Port to becoming the Prime Minister of Crimea post-referendum, the importance of these networks becomes more evident (Kilinkas, 2016: 156).

The final element of irregular forces utilized by Russia in Ukraine comprised private military corporations (PMCs). As per the assessment of Russian analysts, PMCs offer two key advantages: they are both cost-effective and deniable. These analysts propose that Russia deploy PMCs in its strategic operations (Clark, 2020b: 23). To date, ten PMCs have been identified as being contracted by Moscow. These corporations include RSB-Group, Antiterror, MAP, MS Group, Centre R, ATK Group, Slav Corps, PMC Wagner, E.N.O.T., and Cossacks (Bryjka, 2019).

PMC Wagner, with its contingent of 5,000 soldiers, is particularly notable. This corporation is owned by a Russian businessman, Yevgeny Prigozhin, known for his close association with Vladimir Putin. PMC Wagner was engaged in combat against Ukrainian soldiers alongside paramilitary forces (Gök, 2019: 204). Moreover, it is essential to note that Russia's deployment of PMCs extends beyond Ukraine, with evidence of their use in other regions, such as Africa and Syria (Cordesman, 2021: 29).

Russia employs a multidimensional strategy known as hybrid warfare, which involves minimizing dependency on conventional military force and instead prioritizing cyber warfare, propaganda, economic pressure, and covert operations. During the annexation of Crimea and the battles in Eastern Ukraine, these strategies allowed Russia to accomplish its political goals while reducing worldwide public opposition. Within this particular framework, Russia's actions serve as a notable illustration of how a nation-state can proficiently utilize hybrid warfare.

CHAPTER THREE

THE HYBRID WARFARE OF THE ISLAMIC STATE OF IRAQ AND SYRIA (ISIS)

3.1. THE STRUCTURE OF ISIS

Throughout history, conventional and irregular forces have been utilized blurrily or separately in different wars. Although both state and non-state actors deploy their troops on the battlefield, state actors become much more deadly through the broad spectrum of their methods and resources. On the other hand, the development of modern technologies and the increment of their attainableness make non-state actors more fatal, as well (Reichborn-Kjennerud & Cullen, 2016: 2). According to many scholars, ISIS is one of the best cases to illustrate this situation. Andrea Beccaro (2018) claims that ISIS can be identified better as an insurgent group, while Florence Gaub (2015) argues that it is a political-military entity. According to Cronin, ISIS is a pseudo-state governed by a conventional army (Cronin, 2015: 88). It should be noted that whether it is a purely terrorist organization is still a matter of debate.

Of course, this debate is not because ISIS declared itself a state. ISIS waged effective guerrilla warfare and increased terrorist activities as expected. Conversely, it also conducted conventional war alongside unprecedented cyber warfare of non-state actors (Wither, 2016: 75). ISIS has acted as a state rather than a terrorist organization on the territory in which it was captured. Also, the management of the organization reminded of a state; the management authorization was shared by four councils⁷: Shura Council, Advisory Council, Military Council, and Security Council (Turkoglu, 2018: 79). Another thing that distinguishes ISIS from other jihadist organizations, such as Al-Qaeda, was its purpose to achieve territorial gains. In contradistinction to other jihadist organizations, ISIS did not have an ambiguous

⁷ Abu Bakr al Baghdadi was the Caliph so both the political and religious leader of ISIS. It does not mean that the caliph possessed all the power of organization. Shura Council had the authority to dethrone the caliph. However, it was only possible in theory because the Caliph was appointing all members of the Shura Council. For more information, see also Glenn, C. (2015). Al Qaeda v ISIS: Leaders & Structure. Retrieved 12 May 2021, from <https://www.wilsoncenter.org/article/al-qaeda-v-isis-leaders-structure>.

purpose aimed only at destabilizing its opponents. While Al-Qaeda presented the ceaselessness of terrorism and war to its militants, ISIS promised more realistic opportunities such as a territory to live in, institutions to organize daily life, and the Caliphate to glorify Islam (Bektaş & Gündoğdu, 2019: 32-35). In contrast to ISIS, Al-Qaeda is not exceptionally skilled in hybrid warfare. This outcome may result from generational disparities in leadership and expertise, but it may also suggest that effective hybrid warfare requires more outstanding organization and stability than traditional violent terrorism (LSE IDEAS, 2017: 6).

ISIS was more than a purely terrorist organization, not just because it offered its soldiers and believers a territory to live in. Furthermore, it pretended to be a state to regulate public services, law, and economy. ISIS, which described itself as a state, managed to discharge the responsibilities and duties of being a state at the macro and micro levels. For instance, ISIS's administration collected taxes and picked up street garbage. Also, ISIS assumed the mantle of giving marriage certificates, regulating market prices, arranging school exams, and registering. ISIS had allowed institutions and government offices in the captured areas to continue to operate under its rule by changing their names and structures. The Diwan of Agriculture of ISIS is an example of this exercise; it was the modified form of the Iraqi government's Directorate of Agriculture (Cambanis, et al., 2019 111).

When it is considered that ISIS had more than 30,000 soldiers, a monthly income of more than 2 million American dollars (Beccaroa, 2018: 210), and a territory where approximately 8 million people live (Hashim, 2019: 27), it would be a reductive interpretation to have ISIS down as just a terrorist organization. Nevertheless, it would be unrealistic to say that ISIS was a sovereign state. Here, the concept of a hybrid threat has a vital place in fitting ISIS into a theoretical framework because ISIS is a hybrid threat that meets the eye by mobilizing military and non-military capabilities alongside terrorist and guerrilla tactics (Lushenko & Williams, 2016: 11). In 2007, Frank G. Hoffman enounced that terrorist acts are part of hybrid warfare (Hoffman, 2007: 29). Thus, the usage of regional and global terrorist activities implemented by ISIS must not lead to a misconception, it does not demonstrate that ISIS was a terrorist organization. On September 28, 2014, former US President Barack Obama also indicated that ISIS is not just a terrorist network; it

is a hybrid threat (Croft, 2014). Moreover, ISIS's hybrid warfare has threatened regional countries such as Iraq, Syria, Turkey, Libya, and the world. Therefore, ISIS must be regarded as a global hybrid threat, not a regional one (Troy, 2020: 385). Suicide attacks which are known as SVBIED (Suicide Vehicle Borne Improvised Explosive Device) in European countries such as France, Germany, and Spain, and global access to ISIS's propaganda videos are confirmations of this reality.

To sum up, ISIS has been a hybrid actor or threat that conducted hybrid warfare against its enemies in the Middle East but also against all enemies around the world. For an aggressor to be a hybrid threat, its methods and means also must incorporate hybridity.

3.2. ORIGINS OF ISIS

ISIS' origins may be dated back to the year 2002 when Abu Musab al-Zarqawi founded it under the name of the Organisation of Monotheism and Jihad. Nonetheless, under the influence of al-Zarqawi's expedition to Afghanistan during the 1980s, where he engaged in the Soviet-Afghan War and established connections with Osama bin Laden, the group transitioned into an affiliate of Al-Qaeda in Iraq in 2004, assuming the designation Al-Qaeda in Iraq (AQI) (Weiss & Hassan, 2015: 1-86; Warrick, 2015:1-196). Once known as the Mujahideen Shura Council, the group underwent a rebranding process and adopted the Islamic State of Iraq (ISI) to align with its territorial advancements in Iraq. The group accepted the new name for its operations between 2006 and 2013. Subsequently, with the rippling effects of the Arab Spring that extended to Syria and the emergence of a power vacuum, the Islamic State of Iraq (ISI) expanded its territorial control within Syria. It underwent a rebranding, adopting the name Islamic State of Iraq and Syria (ISIS). After the seizure of Mosul in 2014, the organization declared a caliphate, having employed the name for an approximate duration of one year. The group eliminated the geographical markers from its title to assert its claim as the caliphate representing all Muslims globally, thus rebranding itself as the Islamic State (IS) (Cockburn, 2015).

Abu Bakr al-Baghdadi, along with the organization's founder Abu Musab al-Zarqawi, emerged as a highly recognized and dominant figure. In 2010, he inherited

the leadership role inside the organization once called the Islamic State of Iraq (ISI). Taking advantage of the political crisis in Syria during the year 2013, ISI, under his strategies, extended its territory to Syrian soil. Thus, the organization took the name “Islamic State of Iraq and Syria” (ISIS) or “Islamic State of Iraq and the Levant” (ISIL) (BBC News, 2019).

In 2014, the capture of Mosul by ISIS signaled a significant turning point for the organization, ultimately leading to the proclamation of a “caliphate” in June of the same year. Abu Bakr al-Baghdadi declared himself as the caliph of all Muslims. Last time, the organization adopted the name Islamic State (IS). In 2014, the IS militants gained control over Mosul and successfully took over other major urban centers, including Raqqa, Fallujah, and Tikrit. In 2015, the IS made significant progress in territorial expansion, successfully seizing control of various urban centers, including Ramadi, Palmyra, and Sirte (Wilson Center, 2019). The IS experienced its peak between 2015 and 2016; however, towards the conclusion of 2016, its momentum began to diminish. The loss of Raqqa and Mosul in 2017 significantly defeated the IS organization. The geographical government of the caliphate ended with the loss of the village of Baghuz in eastern Syria in 2019. While the material foundation of the organization has been decimated, it would be incorrect to assert that its intellectual influence has been entirely removed from the region (Who was Abu Bakr al-Baghdadi?, 2019).

One of the key factors contributing to the emergence of ISIS and its subsequent operations was the notable power vacuum that existed in the region during and after 2003. The withdrawal of the United States forces from Iraq resulted in a diminished Iraqi state within the region. Following the initiation of the Arab Spring in 2010, the consequential aspects swiftly extended to adjacent nations, ultimately resulting in the involvement of Syria in a state of internal conflict by 2011. The two countries where ISIS achieved territorial advancements were already contending with internal unrest and endeavoring to establish a stable political course. In the context of the prevailing power vacuum, leaders of ISIS strategically profited from significant entities and nations, such as the European Union, NATO, and the US, by closely monitoring regional developments from afar, thereby bolstering their position (Mabon & Royle, 2017: 1-27).

While the victories of IS can be attributed to the implementation of hybrid warfare methods, it is not the first non-state entity that employs hybrid warfare strategies. Organizations and groups, including Hezbollah, Al-Qaeda, and Chechen Fighters, have employed hybrid warfare tactics. Indeed, Hoffman's introduction of hybrid warfare was exemplified by his analysis of Hezbollah's conflict with Israel in Lebanon. The active operations of ISIS from 2003 to 2014 attracted considerable international attention due to many factors (Piotrowski, 2015: 1-2). However, the achievements of the organization, its impact on the global community, and its acquisition of territory are closely linked to the implementation of its proficient hybrid warfare tactics.

3.3. WHY DOES ISIS WAGE HYBRID WARFARE?: POWER ASYMMETRY

Rob De Wijk argues that hybrid warfare offers asymmetric advantages to hybrid threats that are relatively weaker. According to him, hybrid warfare is a fighting strategy employed by entities lacking technological, military, economic, and cultural superiority as a means to overcome their inherent disadvantages (Wijk, 2012: 359-360). Furthermore, Hoffman's introduction of the hybrid warfare idea aimed to provide an explanation and comprehension of the strategies employed by relatively less powerful non-state actors such as Hezbollah, Taliban, and Al-Qaeda, which enabled them to accomplish successes against stronger nation-states (Renz, 2016: 3). Consequently, a preliminary explanation for the utilization of hybrid warfare by ISIS may lie in their strategic objective to equalize the power dynamics by utilizing asymmetrical methods.

While making this deduction is not entirely unreasonable, it is crucial to recognize the possibility of exceptions. To illustrate, despite Russia's various hybrid warfare tactics in Crimea and the Donbas regions, it would be erroneous to assert that Russia is militarily, economically, or technologically inferior to Ukraine. Waging hybrid warfare may not inherently expose the vulnerability of the hybrid actor. However, it provides the aggressor with a method to accomplish goals without facing the casualties of conventional conflict. Hybrid warfare facilitates the effective allocation of scarce resources (Özer, 2018: 39-51). From this perspective, the

utilization of hybrid warfare by ISIS might be attributed to their desire to exploit their limited resources efficiently.

Despite resorting to hybrid warfare cannot be definitively accepted as conclusive evidence of a hybrid actor's vulnerability concerning its adversary, it is important to bear in mind that actors might employ hybrid warfare to counterbalance some of their disadvantages. ISIS has effectively leveraged its economic vulnerabilities through the use of hybrid warfare, thereby capitalizing on this aspect as a strategic advantage. The confusing characteristics of hybrid warfare, along with its ability to conduct operations on multiple levels, have enabled ISIS to use its economic limitations and weaknesses in conventional military capabilities for its benefit. The organization experienced growth in its economic capabilities, strengthened its expenditures in the military sector, and started to enhance its utilization of the potential presented by hybrid warfare in a more efficient manner (Mumford, 2016: 9-10).

The effectiveness of ISIS's hybrid warfare strategy is dependent not only upon its increasing economic ability but also on the use of hybrid tactics that, in turn, contribute to its economic growth. A correlation can be observed between the increase in ISIS's economic influence and the effectiveness of its hybrid warfare strategies. In order to secure its economic independence, the organization has implemented diverse non-traditional funding approaches, encompassing activities like extortion, bank theft, people trafficking, and the management of oil and gas reserves (Beccaroa, 2018: 210-211). In 2014, ISIS obtained a total of 20 million dollars in ransom revenues through the facilitation of repatriation for individuals from different nationalities. Moreover, by capitalizing on the sales of its regulated oil reserves, it managed to amass a daily revenue of one million dollars (Berman, 2014).

In conclusion, the imperative for the organization to broaden and strengthen its financial resources has compelled it to turn to hybrid warfare and acts of aggression. The utilization of hybrid warfare confers notable benefits that contribute significantly to the attainment of economic objectives by ISIS.

3.3. HYBRID METHODS OF ISIS

3.3.1. Activities in Cyberspace

Historically, the sphere of activity of jihadist organizations such as Al-Qaeda (the predecessor of ISIS) or Boko Haram remained mainly limited to the physical globe. The main goal of jihadist organizations was to destabilize the hostile country by spreading fear in the target country. To do this, they have carried out several attacks in the physical sphere. Aircraft hijacking, crashing hijacked aircraft into fixed targets, using biological and chemical weapons, attacks on critical infrastructures and diplomatic representations, and bomb attacks in crowded areas such as subway stations, train stations, and airports are some examples of trumpeted methods of jihadist organizations. However, advancing technologies and internet access worldwide have allowed non-state organizations such as ISIS to move towards cyberspace activities and the physical sphere (Ozden, 2021: 20-21).

Cyber warfare has been taking the most crucial place in ISIS's hybrid warfare campaign because cyber warfare of ISIS includes a broad spectrum that consists of the disinformation campaign, propaganda, online training of mujahids, hacker attacks, the usage of social media, online employment of soldiers, and promulgating of the so-called Caliphate's creed.

ISIS has been so concerned about cyberspace acts that many scholars have argued that it sought to maintain a virtual caliphate. A virtual caliphate was a backup plan that allowed ISIS to keep spreading its radical ideology through online tools in the event of a decisive defeat in Syria and Iraq. Therefore, it could become a permanent threat without a territory (Votel, Bembeneck, Hans, Mouton, & Spencer, 2017: 1-5). Another practical usage of the virtual Caliphate enhanced the accessibility to foreign fighters and supporters (Troy, 2020: 397). Through the virtual Caliphate, ISIS has recruited many foreign fighters and mainly utilized them in three ways. First, it summoned the supporters to its soil and trained them to use in military conflicts. Second, the foreign fighters were used to spread the Caliphate's creed to the world. These fighters have spoken about the correctness and virtues of ISIS's rule on social media platforms and invited people to join their war. Lastly, ISIS did not

call for all its followers to gather within its territories. The group's cyber efforts were facilitated by digital mentors who successfully transformed numerous individuals into combatants by utilizing online training modules. The individuals who received digital training carried out many activities on behalf of the organization, particularly in various parts of Europe.

Moreover, it is also worth mentioning that ISIS's adaptation demonstrated that today's technologies and conditions have started to shape solid jihadist communities. The Jihadi community transformed into a more adaptive and resilient online jihadi community (Gambhir, 2016: 30).

3.3.2. Disinformation Campaign and The Manipulation of Information Flow

One of the essential characteristics of hybrid actors is their efficiency levels in the methods and tools they use to disseminate and control information. The more active tools and techniques, the easier it is to influence the international and domestic community. The Russian Federation revealed a successful example and delayed or prevented the world from understanding what was happening in Ukraine. When comparing ISIS to state actors, it might be expected that ISIS would have limited effectiveness in conducting misinformation campaigns and exerting control over the dissemination of information. Nevertheless, while examining the limited availability of means and resources accessible to ISIS, it becomes apparent that the group has achieved unprecedented success as a non-state entity.

Since it was not easy for ISIS to spread information that could manipulate the international community and the mainstream media, ISIS's employees mainly aimed at smaller targets. For instance, ISIS used several media outlets to receive support and warriors from different countries. The Al-Hayat Media Center, broadcasted in different languages, was the essential ISIS media outlet for employing foreigners. It contained many materials, such as videos, photographs, news, and infographics. The materials presented by the Caliphate's media apparatus demonstrated signs of selective editing and manipulation. The Caliphate's overarching strategic approach was centered on cultivating a profound sense of empathy and alignment among

foreigners. The Mujatweet HD video series was one of the best examples of the materials uploaded to get ambitious foreigners' support. In the series, the lifestyles of ISIS militants have been encouraged. Also, it was emphasized that the people living under the Caliphate were happy by offering carefully selected sections of their lives.

Moreover, the media department of the Caliphate was casting its militants from European countries, so these militants were demanding support by mentioning the pleasing life in ISIS's territory and the virtues of fighting on behalf of the Caliphate (Barret, 2014: 55-56). Indeed, ISIS has recruited many foreign fighters through its information manipulation. Between 2014 and 2016, the number of soldiers fighting for ISIS reached 30,000, and from 1979 to 2015, the number of foreign warriors fighting in Afghanistan was around 26,000. This is the success of the cyberspace warfare of the Caliphate (Yalçinkaya, 2017: 16-17).

On the other hand, ISIS's information manipulation campaign was not unidirectional. It implemented its informational operations against not only its adversaries but also fighters of the Caliphate. In informative operations against fighters, the power of the Caliphate was mainly underlined. Besides, the number of soldiers killed by ISIS forces was published. So, it aimed to increase the motivation of the Caliphate's fighters by reminding them of the capacity of ISIS (LSE IDEAS, 2017: 7).

It also must be noted that non-state actors' media usage tends to become more savage and egregious because they do not feel responsible for complying with international law. In this way, non-state actors manipulate information and the international community more quickly by creating asymmetric advantages for themselves (Ganor, 2012: 14).

3.3.3. Propaganda

The Caliphate endeavored to spread an anti-Western narrative, but the organization's administrative staff argued that mainstream media is deferential to Western governments. As ISIS could not use mainstream media, it has put lots of effort into becoming an alternative to mainstream media tools through multilingual mass media (periodicals and newspapers) and propaganda videos. Even though ISIS

was not the first extremist organization to carry out propaganda against the West, its behest set it apart from previous extremist organizations such as al-Qaeda and al-Shabaab. The Caliphate has systematically and consistently tried to find a solution to reach a broad audience (Yarchi, 2019: 56).

As a result of these systematic and continuous efforts, the propaganda methods of the organization changed after mid-2015 because the Caliphate aimed to have more proponents by reaching a broad audience. Before 2015, ISIS worked to threaten its enemies through images of violence such as beheadings and mass executions, so propaganda products mostly contained vandalism and brutality. However, these uncivilized propaganda products had unsettled enemies of the Caliphate and potential supporters. Thus, ISIS's media department resorted to redesigning the contents of propaganda videos to earn more sympathy. The new videos included images of the welfare level of people in captured areas, the supply of food and beverages, the happiness of people, and the kids who go to school (Jasper & Moreland, 2016).

As seen from this example, ISIS was not an organization that made uncontrolled propaganda. The Caliphate established a Media Council as a media ministry to superintend media activities. The Council contained many organizations such as Al-Hayat Media Center⁸, Ajnad Foundation⁹, Al-Furqan Islamic Heritage Foundation¹⁰, Amaq News Agency¹¹, and Al-Beyan¹² (Salihi & Göksun, 2018: 19-21). Although the Caliphate possessed media outlets, social media platforms were vital propaganda tools. It has used the most important social media platforms such as YouTube, Twitter, and Facebook to recruit, fundraise, and commercialize (Doğru, 2017: 143). Using these platforms for propaganda has yielded some asymmetric advantages in other respects. The spread of propaganda was complicated to prevent as both personnel of the Caliphate and sympathizers served to spread propagandistic

⁸ The center was publishing the journals of Dabiq (English), Dar Al-Islam (French), Al-Manba (Russian), Konstantiniyye (Turkish), and Rumiyyah (English, French, German, Russian, Turkish, Indonesian, Bosnian, Kurdish, Uigur, Kurdish and Pashto Arabic).

⁹ The foundation recorded organization's anthems, quranic recitations, and soundtracks.

¹⁰ The organization was mostly responsible for announcing official statements of ISIS's senior staff, as well as preparing archive videos. On the 29th of June 2014, the official announcement of so-called caliphate was made through this foundation.

¹¹ The official news agency of organization.

¹² The radio channel transmitted in Iraq and Syria. This organization was transmitting all day with targeting FM frequencies.

media. For instance, Twitter suspended the organization's main account¹³, but 55,000 sympathizers continued making propaganda on behalf of ISIS in 2015 (Gaub, 2015: 2).

Besides, the Caliphate forced prisoners to appear in propaganda videos criticizing the West. In 2012, the British photojournalist John Cantlie¹⁴ was kidnapped by militants in Syria, and then he showed up in several videos. In these videos, he criticized Western states, especially the United States and Britain, and said that ISIS was more powerful than Britain. Mr. Cantlie also accused the Western media of distorting and manipulating facts (Cumhuriyet, 2014).

ISIS has an unusual and sophisticated propaganda understanding from other non-state organizations. For example, it even prepared an animated movie¹⁵ targeting children on Telegram and YouTube (BBC, 2017). Another unique propaganda method of the organization was using unmanned aerial vehicles (UAVs). It is common knowledge that some extremist groups have previously used drones for surveillance and attacks on the battlefield. However, the Caliphate used drones not only for surveillance and aggression but also for preparing propaganda videos, delivery of armaments, and detection of fire (Jasper & Moreland, 2016: 5). ISIS has filmed pre-attack reconnaissance and ground operations through drones and then published videos to demonstrate its operational capability (Archambault & Veilleux-Lepage, 2020: 956).

3.3.4. Hacker Attacks

ISIS's hacker attacks have mainly caused psychological suffering to its adversaries rather than physical ones. Nevertheless, it must not be understood as its

¹³According to statement of Twitter officials, they suspended over 125,000 accounts which promoted terrorism and extremism until the first months of 2016. Most of these accounts were related to ISIS. For more information, see also https://blog.twitter.com/en_us/a/2016/combating-violent-extremism.html.

¹⁴The British journalist John Cantlie and American journalist James Foley were kidnapped in Syria on the 22nd of November 2012. James Foley was murdered, and John Cantlie was displayed some propaganda videos. However, he has not been appeared since 2016. His fate is unknown. For more information, see also <https://www.bbc.com/news/uk-54270679>.

¹⁵This animation movie which was titled *The Ruler and The Brave* started to be animated in 2017. It has told the story of a society of brave people against the tyrant in their country. In fact, these brave people symbolized ISIS's militants. In this way, ISIS made itself look like heroes who fight against injustice and tyranny.

hacker attacks were inoperative and feeble. The Caliphate's cyber-attacks have induced fear and moil among its enemies' soldiers and their families. Several hacker groups organized cyber-attacks on the side of ISIS such as Cyber Caliphate, Cyber Caliphate Army, Sons Caliphate Army, Islamic Cyber Army, and the Kalashnikov E-Security Team (Özden, 2021: 95-96). The Cyber Caliphate hacker group was well-known because it has taken the blame for operating significant hacker attacks. In 2013, Abu Hussain al-Britani¹⁶, a British Pakistani black hat hacker, created this hacker group and trained new hackers to increase the cyber power of ISIS. Until he died in August 2015, the Cyber Caliphate had carried out many significant attacks on the organization's adversaries (Giantas & Stergiou, 2018: 10-12).

The Cyber Caliphate was believed to become suspicious of significant cyber crimes supporting ISIS. One of the most critical crimes was hacking the US Central Command (CENTCOM) 's Twitter and Facebook accounts and YouTube channels. The hacker group replaced the profile photo of the Twitter account with an image that read “I love ISIS” and “CyberCaliphate.” Moreover, threatening messages against US military personnel that say, “American soldiers, we are coming, watch your back!” and “ISIS is already here, we are in your PCs, in each military base.” were tweeted out. Besides, the timing of the hack was well planned because it occurred when President Barrack Obama was holding a press conference in Washington about cybersecurity (Ackerman, 2015).

The US was not the only state targeted by the Cyber Caliphate, after a few months, a global French television network called TV5Monde was also attacked by the group. TV5Monde's websites and social media accounts were taken over, and its eleven channels were blacked out for two days. On the network's Facebook page,

¹⁶ In 2012, Abu Hussain al-Britani was jailed for six months because he leaked out private e-mails and phone numbers of British Prime Minister Tony Blair and her family. When he got out of jail, he went to Syria to join ISIS. After a short time, he became the chief terror cybercoach of the organization owing to his computer skills. In 2013, he established the Cyber Caliphate hacker group to organize cyber-attacks on behalf of ISIS. He was the prime suspect for hacker attacks on the CENTCOM and TV5Monde network. In the summer of 2015, he was killed by US air bombardment. After he died, the effectiveness of the Cyber Caliphate has reduced. For more information, see also Hamid, N. (2018). The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain. *Combating Terrorism Center*, 11(4), 1-37. Retrieved from <https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/> and Ackerman, S., MacAskillin, E., & Ross, A. (2015, August 27). Junaid Hussain: British hacker for Isis believed killed in US air strike. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike>.

attackers published some documents that claimed that ISIS had IDs, CVs, and passports of French soldiers who participated in anti-ISIS operations. Also, they threatened French soldiers and their families with Facebook posts that wrote, “Soldiers of France, stay away from the Islamic State! You have the chance to save your families, take advantage of it” (Chrisafis & Gibbs, 2015; CBS News, 2015).

3.4. CONVENTIONAL FORCES

The Caliphate did not have a conventional army as robust as nation-states, even when it was at the peak of its power. Nevertheless, it has displayed its danger to international security by blurring conventional forces with guerilla tactics and terrorism (Wither, 2016: 75). ISIS had no capacity to keep an army of hundreds of thousands of men available; its army consisted of 30,000 soldiers when its largest period. Only two-thirds of soldiers were full-time and ideologically devoted to the organization. However, the organization's armed forces were capable of organizing all-inclusive military operations, despite its smallness (Mumford, 2016: 25). Besides, the Caliphate's armed forces had fundamental features of a conventional army such as employing motorized infantry¹⁷, armored forces, semi-professional artillery¹⁸, hierarchical military command, and control, also, conducting intelligence and surveillance activities, wearing an army uniform, and having intense firepower (Maurer, 2018: 233-238).

ISIS's military victories against Iraq and Syria armies in 2014 have become more of an issue in forming conventional forces of the organization. Iraq and Syria, struggling with internal and external problems during this period, suffered significant defeats from ISIS. After its unexpected military success, ISIS captured many weapons, vehicles, and other military stuff from both states' military forces. Furthermore, the organization's victories provided military equipment and territory to shelter, refresh, plan, and make military production. In addition, both its

¹⁷Those troops mostly used main battle tanks such as Soviet T-54/55s, T-62s, and T-72s, US M60s, and M1-Abrams type. These tanks were captured from ISIS's adversaries.

¹⁸ Semi-professional artillery's fire power consisted of improvized missile launch facilities, multiple rocket launchers, mortars, light artillery weapons, howitzers and heavy armored artillery such as the US M198 (155 mm) and the Soviet 2S3 (152 mm).

conventional forces and military elite found a place to deploy, so the military structure of conventional forces thrived (Hashim, 2019: 27).

In the early years of its existence, the military leadership had not had enough experience in traditional conflicts. In 2010, however, former Iraqi Baathist¹⁹ officers were assigned to the military decision-making process to increase success in conventional conflicts. Those officers, who had seen service in a conventional army and had been involved in many conflicts, shared their military training, knowledge, and experience with ISIS militants (Gaub, 2015: 1). High-profile Baathists were also among those officers such as Ayman Sabawi, who is the son of Saddam Hussein's uterine brother, and Raad Hassan, who is Saddam's cousin. Those officers brought along not only their military knowledge but also their networks. The utilization of communication networks established by former Baathist officers during their stay in high-level administration has demonstrated significant advantages for ISIS. ISIS has engaged in many espionage and intelligence operations using these networks. (Coles & Parker, 2015).

Many samples of the Caliphate's militants behaved as if they were members of a conventional army instead of a guerilla force in many conflicts in Iraq and Syria. For instance, it applied traditional infantry tactics in northern Iraq by attacking with extensive artillery fire on the Kurds' Peshmerga. Also, in 2015, ISIS troops combined infantry assaults with irregular attacks during the battle of Ramadi to run behind the defense line of Iraqi Security Forces (Beccaroa, 2018: 5). ISIS has captured the weapons deployed by traditional militaries, which is another reason for its success in military conflicts. It has received most of its conventional weapons from captured Iraqi and Syrian military installations (Majumdar, 2015). Thus, it has an amount of

¹⁹ At its simplest, Baathism stands for Arab nationalism, pan-Arabism, and united Arab society in a single state without foreign intervention. Salah al-Din Bitar and Michel Aflaq were masterminds of the Baathist idea which has been represented by two Arab countries; Iraq and Syria. Later, socialism was interpreted as social justice by Baathists and added to Baathism. On April 4-6, 1947, The Baath Party was founded with a congress in Damascus by Bitar and Aflaq. Baathism's idea was transferred to Iraq by Shi'i students. However, in 1966, Iraqi regional branches of the Baath Party had a falling out with Syrian regional branches because of the Syrian coup d'état which was organized by a union of the party's Military Committee and the Regional Command against the National Command of the Arab Socialist Baath Party. Saddam Hussein was one of the important representatives of Baathists in Iraq. He was in charge of the secretary-general of the Iraqi Baath Socialist Party between 1989–2003. The Iraqi Baath Socialist Party was firstly evaporated with the US occupation and then abolished in 2003. In Syria, Bashar al-Assad is still in charge as the leader of the Syrian Baath Party. For more information, see also Devlin, J. F. (1991). 1396-1407 and Slevin, P., & Chandrasekaran, R. (2003, May 12).

weaponry typically employed by traditional armies. ISIS often exhibited the weaponry it had captured, intending to spread fear in its adversaries, a strategy that yielded positive outcomes. The weaponry of ISIS and its prospective applications have been extensively deliberated upon by numerous Western news networks (Warrick, 2022; Hénin, 2015). Some weapons in the possession of ISIS include weapons taken from the Iraqi and Syrian military. T-55, T-62, and T-72 Ural model tanks, BRDM-2 Armored Vehicles, and MT-LB armored vehicles. Humvees, BMP-1 Infantry Fighting Vehicles, 122mm 2S1 Gvozdika self-propelled Artillery, 82 mm B-backlash-10 Gun, 105mm backlash M40 rifle, M79 Osa rocket launchers, RBG-6 grenade launcher, multiple rocket launchers, M198 Howitzers, Type 59-1 Field gun, D-30 Howitzers as well as anti-aircraft weapons, anti-tank missiles, and MiG fighter aircraft (TRISA; CTID, 2014: 8; Bender, Rosen, & Wilson, 2016).

Other significant examples of ISIS's success in conventional combats were the seizure of Kobane and the assault on the Baiji oil refinery. The organization's cyber unit shared some images of ISIS militants capturing Kobane house-by-house with artillery support in 2014 and drone images of the Baiji assault 2015. Both scenes impressed military analysts because militants were moving like a conventional army rather than a guerilla power. The ability of these well-trained troops to act disciplined and coordinated has attracted many military analysts' attention (Jasper & Moreland, 2016: 7).

Finally, it is essential to highlight that the army of ISIS demonstrated maneuverability commonly observed in traditional military forces. The unexpected nature of the maneuver operation in Al-Anbar in 2012 can be regarded as a compelling indication of this phenomenon (Beccaroa, 2018: 6). The US army's withdrawal from Iraq allowed the Caliphate to increase its maneuverability as they were aware of the extremely low probability of airstrikes (Whiteside, 2016: 12). However, it does not mean that the Caliphate's maneuverability was comparable to traditional armies. It mainly deployed SVBIEDs²⁰ against its adversaries rather than classic maneuver operations. Those sorts of military tactics, which do not require maneuverability and close contact with a battalion, have substantiated that some part

20 Suicide Vehicle-Borne Improvised Explosive Device

of former Baathists' military doctrine had been adopted by the Caliphate (Barfi, 2016: 19).

3.5. NON-CONVENTIONAL METHODS: TERRORISM AND INSURGENCY

Many politicians, military analysts, and academics accepted that ISIS is not a pure terrorist group. President Obama argued that ISIS is a terrorist organization as well as a hybrid danger with territorial ambitions (Jacobs & Lasconjarias, 2015: 5). Although ISIS is not exclusively a terrorist group, it has utilized terrorist actions, one of the defining criteria of a hybrid actor, to gain an advantage over its adversaries. ISIS's ability to deploy terrorist acts as a successful hybrid warfare technique is further facilitated by its decentralized nature. It has created a structure that can reach pain receptors from the political and social spheres to coordinate terror attacks against adversaries without waiting for instructions. This structure has expanded ISIS's flexibility across the Middle East and Turkey, resulting in more lethal terrorist attacks in these regions (Doğru, 2017: 138-142).

ISIS not only planned terrorist activities but also rationalized their conduct with the theory of just war²¹ and promoted the concept of “just terror.” They utilized Rumiya Magazine for justification efforts, and in the second issue of the magazine, for the first time, the framework of the notion of just terror was outlined, as well as advice on the use of knives in terrorist attacks (Mahzam, 2017: 8-10). The magazine's five issues are dedicated to Just Terror Tactics (Rumiya 2, Rumiya 3, Rumiya 4, Rumiya 5, and Rumiya 9) to define and instruct ISIS militants on just terror. The third issue discusses the use of trucks and other vehicles for murderous purposes when other issues of the magazine, information is offered on the selection of targets, theft, vehicle attacks, and hostage-taking within the context of justified terrorism (Azani & Dotti, 2021: 22; Welch, 2018: 193-194). Therefore, it is possible

21 The just war theory analyzes whether the use of force for political reasons is acceptable. In this perspective, there are two crucial pillars upon which the righteous war stands. The first principle, *jus ad bellum*, stresses that war should be launched for justifiable causes, whereas the second principle, *jus in bello*, emphasizes being right in war and, hence, conducting a restrained war. The goal of the doctrine of just war is not to legalize war, but rather to restrain it. Respect for diversity, necessity, and proportionality are essential criteria of *jus in bello*, according to the philosophy of just war, even in conflict conditions. For more information, see also, Ereker, (2019, October).

to say that ISIS used the magazine not just to justify terrorist attacks but also to train its militants.

Although ISIS has evolved from a terrorist group to a more structured and systematic hybrid actor over time, it has utilized terrorist and insurgent tactics regularly and effectively in its operations. Suicide bombers were one of the most influential and terrifying weapons utilized by ISIS in their terrorist strikes. ISIS has carried out suicide bombings and vehicle assaults in other European nations in addition to Iraq and Syria. Between 2013 and 2018, ISIS terror attacks in the Middle East and beyond resulted in the deaths of around 28,442 people (McCarthy, 2019). The terrorist attack that transpired in Paris on November 13, 2015, resulting in the loss of 130 lives and causing injuries to 413 individuals, was executed by ISIS (Armstrong, 2016). Besides, ISIS's 2016 attack on the Brussels Zaventem airport, which resulted in the deaths of 32 people, is another example of the shocking terrorist operations it has carried out in Europe (Euronews, 2022).

The fact that ISIS militants believe that dying on the path of jihad will open the gates of heaven for them has facilitated the use of suicide strikes, one of the most efficient forms of terrorism. In the first five months of 2016, ISIS committed around 500 suicide strikes in Iraq, Libya, and Syria (Lushenko & Williams, 2016). According to Katherine R. Seifert and Clark R. McCauley, between 2003 and 2010, ISIS militants organized a total of 1,779 suicide attacks (Seifert & McCauley).

Scott Casper and Scott Moreland have linked ISIS's terrorist actions to three operations. Firstly, the severe violence demonstrated by ISIS when it conquered some regions and executed, destroyed holy places, and intimidated Western foes by distributing films of executions is among the regional operations of ISIS (Jasper & Moreland, 2016). ISIS has used its severe violence and terrorist actions to create unrest by spreading fear among its enemies. The fact that ISIS releases films of particularly violent beheadings on multiple platforms is one illustration of their aggressive propaganda. Throughout the era, however, ISIS abandoned this tactic in favor of a policy emphasizing the pleasure and prosperity of the people living under the Caliphate (LSE IDEAS, 2017: 7).

Secondly, ISIS's philosophy of devastation reflects its transitional operations. In accordance with these operations, ISIS carried out numerous acts of damage in

rural and urban areas, including the poisoning of water, the placement of booby traps in hospitals, the destruction of generators, and the devastation of agricultural lands. Finally, ISIS has also conducted adaptive operations that quickly adjust to changing conditions. ISIS militants, for instance, use refugee routes to enter Europe via Turkey and Greece to carry out and organize terrorist acts in Europe (Jasper & Moreland, 2016).

Furthermore, ISIS has also successfully implemented the technology into non-conventional tactics. They have integrated the scope and aims of the weapons employed with their own goals and terrorist assaults. From this perspective, ISIS' utilization of captured drones for terrorist strikes has given a new dimension to non-state actors' terrorist actions. ISIS is not the first non-state entity to utilize flying drones (UAVs). As an illustration, it has been observed that Hezbollah has employed drones six times in its engagements with Israel. Nevertheless, ISIS has demonstrated innovation and adaptation in the utilization and rationale behind drone deployment.

In contrast to ISIS, Hezbollah has demonstrated a tendency to employ drones solely for reconnaissance missions and bomb strikes. On the other hand, ISIS has developed propaganda videos employing drones to intimidate Western powers it deems to be its opponents. From August 2014 to March 2015, drones were deployed to provide aerial assistance for the continuing conflicts on the ground, for propaganda videos, and for reconnaissance flights in four different operations around Raqqa, Falluja, and Kobani (Bunker, 2015: 9-15; Tadjdeh, 2014).

ISIS has not only employed sophisticated weaponry in its terrorist strikes but has also resorted to conventional techniques. ISIS employs ambushes, mines, and booby traps, among other classic means of terrorism. ISIS has left booby traps and minefields as it withdraws from the Iraqi and Syrian territory it once controlled but later lost. Therefore, they impeded the maneuverability of their adversaries and led them to suffer significant casualties (Fordham, 2014). ISIS has employed terrorist acts, which are one of the essential parts of hybrid warfare, especially for non-state actors, in a very successful manner by combining traditional with novel terror tactics. With the addition of terrorist attacks and insurgency actions, the ISIS military forces, whose size has surpassed 30,000 and which have been effective in conventional

fights against the Iraqi and Syrian forces, have become one of the deadliest actors in the region.



CHAPTER FOUR

A COMPARATIVE ANALYSIS OF HYBRID THREATS: RUSSIAN AND ISIS CASES

This thesis delineates the conceptual framework of hybrid warfare while simultaneously uncovering its application and resultant impacts in contemporary conflicts through case analyses. It seeks to enrich our understanding of the hybrid warfare concept by examining selected cases. The chosen cases are Russia's hybrid warfare campaigns in Crimea and the Donbas region and the hybrid warfare conducted by ISIS during its rise in Iraq and Syria.

Two principal reasons underpin the selection of these cases. The first stems from the stark contrast between Russia and ISIS as actors. Although both are identified as hybrid aggressors employing hybrid warfare methods, Russia is a state actor, while ISIS is a non-state actor. Hence, how state and non-state actors resort to hybrid warfare, their objectives, and the methods employed exhibit differences and similarities. By selecting these cases, the aim is to highlight what these similarities and differences entail.

The second significant reason for choosing these cases is the proximity of the conflicts' onset dates. Russia annexed Crimea on March 21, 2014 (Grant, 2015: 68-77), while ISIS, having renamed itself from its previous iterations, began to employ hybrid warfare tactics in Syria and Iraq starting in April 2013 (Hashim, 2014: 1-11). These cases were chosen to understand the conjunctural conditions of the period and to explore if there is a correlation between these conditions and the reasons why the actors engaged in hybrid warfare.

The analysis focuses on the hybrid warfare strategies employed by Russia and ISIS, examining their similarities and differences across various levels, including philosophical, strategic, operational, methodological, and tactical. The comparison has been categorized into six major categories, each aiming to uncover similarities and differences in the hybrid warfare strategies employed by the two actors.

4.1. PSYCHOLOGICAL WARFARE AND PROPAGANDA TOOLS

The utilization of social media platforms for disinformation campaigns and psychological damage by both Russia and ISIS is widely acknowledged; nonetheless, their objectives in employing these platforms differ significantly. Russia employs social media to obscure its acts, intending to evade international consequences. Conversely, ISIS has utilized social media platforms to disseminate its activities to a worldwide audience, creating widespread international impact. Therefore, whereas Russia uses social media as a defense mechanism against global criticism, ISIS employs it to magnify its influence on the worldwide platform.

The ISIS social media posts that garnered the most notable attention were the videos featuring Western detainees who were coerced into speaking on camera before their execution. These movies rapidly disseminated around the internet, leading to global recognition and comprehension of the impact wielded by ISIS. The group carefully employed these videos as a demonstration of dominance over the Western world and as a means to validate their presence (Bronk & S. Anderson, 2017: 96-97).

ISIS initially posted execution videos and footage of raids on social media platforms to increase the organization's fame. Nevertheless, they ultimately dropped this strategy. They adopted a new approach by distributing videos that portrayed the contentment of individuals residing within the Caliphate instead of using execution videos to intimidate its adversaries. This strategic move aimed to acquire a more significant number of supporters via social media and enlist some of them into their organization (Awan, 2017: 140-141).

ISIS aimed to utilize these videos not only to recruit soldiers but also to grow its population. According to estimations, ISIS managed to convince more than 3,000 individuals from Western countries to go to the territories it controlled, primarily by utilizing social media platforms (Blaker, 2016: 3-5). Moreover, it is widely recognized that ISIS used social media platforms as a means to gather financial contributions. Although the donations collected through social media and other means are minimal compared to other sources of income like oil, drug smuggling, and ransom, they nonetheless hold considerable significance. On September 24,

2014, it was revealed that ISIS officials received a sum of 2 million dollars from donors in the Gulf region (FATF, 2015: 18-20).

Russia used social media platforms to broadcast disinformation, avoid global inquiry, provoke the Russian-speaking minority in Crimea and Donbas, spread pro-Russian news and narratives, and weaken Ukraine's reputation in the international arena (B. Mueller, Jensen, & Valeriano, 2023: 11-15).

When Russia annexed Crimea in 2014, it initially denied any involvement in the attacks carried out by a group of soldiers referred to as “little green men.” However, it was later revealed that these soldiers were Russian special forces. Russia fraudulently claimed that these uniformed individuals, whose military affiliation was intentionally concealed, had no connection to the Russian army. The Russian media portrayed these warriors as “polite people.” Russia propagated its disinformation campaign by disseminating the narrative through social and conventional media platforms that these were indigenous self-defense groups unconnected to the Russian military (Besemeres, 2016: 356-357). Hence, Russia managed to evade any negative diplomatic implications for the operations carried out by these units. Nevertheless, it is essential to acknowledge that this tactic was utilized within the Russo-Ukrainian War that commenced in 2014. By contrast, in the second Russo-Ukrainian War that began in 2022, the Kremlin publicly dispatched armed forces and did not avoid international scrutiny (Boer, 2023: 17-23).

In addition, the Kremlin has endeavored to strengthen President Putin's reputation and undermine the Ukrainian government by providing financial support to social media trolls. An extensively documented instance of this phenomenon is a collective called the “Olgino trolls,” named after the geographical location in St. Petersburg, where they conducted their activities and were financially supported by Russia. This organization has engaged in spamming news stories and blog posts that contain negative opinions about Russia. They have inundated these platforms with comments that aim to refute the content. (Mejias & Vokuev, 2017: 1033-1035). In addition, these trolls have employed multiple social media platforms, specifically Facebook and Twitter, to distribute posts that commend the Donetsk People's Republic (DNR) or the Luhansk People's Republic (LNR) and propagate fabricated

accounts of mistreatment by the Ukrainian government, intending to undermine global backing for Ukraine (Walker, 2015).

The Kremlin used not only social media manipulations but also other strategies to improve President Putin's global reputation and undermine the Ukrainian government. They have successfully utilized both social and traditional media to provoke the Russian-speaking community in Eastern Ukraine against the Ukrainian government. In 2014, there were discussions on social media platforms stating that the protests at Maidan, which Western supporters started, were supported by the United States. Additionally, it was claimed that the Ukrainian government was trying to construct a neo-Nazi administration. The main topic was the assertion that the forthcoming neo-Nazi regime would specifically target the Russian-speaking community in Ukraine, with an impending threat of genocide. The objective behind disseminating such propaganda was to incite the Russian-speaking population to revolt against the Ukrainian government (Horvath, 2015: 3-5).

Both Russia and ISIS have utilized the internet and social media extensively during their hybrid wars. Although it cannot be asserted that each employed the internet in entirely distinctive manners, observable disparities in their approaches and goals are apparent. A notable gap lies in the fact that Russia has used the internet to conceal its endeavors, whereas ISIS has sought to disseminate its operations globally.

4.2. CYBER ATTACKS

Cyber attacks play a prominent role in the hybrid warfare strategies employed by ISIS and Russia. Both parties have sought an edge over their adversaries by using cyber attacks alongside physical assaults. Although these attacks have shared characteristics, their scopes are significantly different.

For example, the individuals carrying out cyber attacks on behalf of Russia were not official government employees but rather chosen patriotic Russian citizens. This is done to facilitate the repudiation of any association in case the identities of the hackers implicated in the assaults are disclosed. Conversely, ISIS has not hidden its affiliation with the hackers carrying out the attacks and has openly declared its financial support for multiple cyber collectives. The organization formed a hacker

group called Cyber Caliphate, responsible for conducting numerous cyber attacks (Piazza & Guler, 2019: 3-5).

Upon comparing the cyber-attacks executed by the two entities, it becomes evident that Russia's attacks exhibit a higher level of sophistication and have a broader scope. Russian hackers have not only focused their efforts on infiltrating the infrastructure of the Ukrainian government and military but have also orchestrated deliberate attacks on the infrastructure of Ukraine's private communications businesses. During 2015 and 2016, Ukrainian energy infrastructure was targeted by Russian hackers through the deployment of malicious software and phishing emails. Following the 2015 attack, 225,000 individuals experienced a power outage lasting several hours (Lee, Assante, & Conway, 2016).

In addition to targeting telecommunication businesses, Russian hackers also transmitted menacing messages to Ukrainian soldiers and their families to undermine the soldiers' resolve to engage in combat. The extent of the cyber assaults carried out by Russian hackers extended beyond Ukraine exclusively. Amidst the turmoil in Ukraine, the online platforms of three NATO nations - Germany, Estonia, and Poland - that had openly shown their backing for Ukraine were also subjected to cyber attacks by Russian hackers (Limnell, 2018: 68-71).

Russian cyber attacks encompass intricate operations that aim at a broader scope beyond mere infrastructure and websites. Indeed, Russian hackers endeavored to interfere with the system through the initiation of cyber assaults on Ukraine's Central Election Commission only 48 hours before the 2014 Ukrainian Presidential Elections. During the election night, they persisted in their efforts to manipulate the election outcomes by launching further attacks (Kramer & Higgins, 2017: 1-6)—Russian hackers' endeavors to disrupt elections extended beyond Ukraine only. In the 2016 US Presidential Elections, Russian hackers successfully breached the email accounts belonging to the Democratic National Committee (DNC) and multiple prominent Democratic Party leaders. The emails were subsequently disclosed via WikiLeaks and other platforms (Mueller, 2019: 38-50).

ISIS's cyber attacks have been aimed at causing psychological harm rather than physical harm, in contrast to Russia. ISIS hackers, like their Russian counterparts, also spread menacing messages to undermine soldiers' resolve to

engage in combat. Nevertheless, ISIS has not targeted the infrastructure of any telecommunications businesses, or if they have, their attempts have not yielded substantial outcomes. As a result, their main focus has been on orchestrating assaults aimed at websites and social media accounts.

The Cyber Caliphate hacker group executed a prominent attack by compromising the social media accounts of the US Central Command (CENTCOM). The CENTCOM Twitter account was used to make posts that threatened US soldiers to pressure the US administration to cease its attacks on ISIS (Giantas & Stergiou, 2018: 10-12).

The Cyber Caliphate directed its attacks on both the United States and France, leading to a two-day blackout of TV5Monde, the French national television channel. Furthermore, the social media accounts affiliated with this channel were compromised, resulting in the unauthorized disclosure of the identities of soldiers purportedly engaged in combat against ISIS. In addition to these posts, there were also messages of danger directed towards French soldiers and their families, intending to undermine the morale and motivation of the French military (Tsaourias, 2016: 456).

Both actors employ cyber attacks as a means of hybrid warfare. However, it is noteworthy that ISIS's operations predominantly serve to further its psychological warfare strategies. These attacks have been significantly less extensive in comparison to those in Russia. Conversely, Russian hackers have conducted assaults with practical and verifiable goals, such as manipulating election outcomes. Russian hackers have staged sophisticated operations, such as the ones on Ukraine's electrical system, that are capable of causing physical harm to their opponents and their infrastructure.

4.3. REGULAR FORCES AND TACTICS

Another notable distinction between ISIS and Russia is their possession of regular forces and the tactical strategies deployed in conflict utilizing these forces. Attempting to assess the influence of regular troops on hybrid warfare by comparing the military personnel and equipment of Russia, a state player, with that of ISIS, a

non-state actor, would not yield realistic results. Hence, it is crucial to examine how each participant employs their regular forces and the consequences of such utilization.

Due to its status as a terrorist organization, ISIS initially lacked any conventional military forces. Nevertheless, it may be said that ISIS insurgents started to embrace a more systematic framework after the enlistment of ex-Iraqi soldiers in 2010, who imparted their military expertise and instruction to the group (Coles & Parker, How Saddam's men help Islamic State rule , 2015). Following 2010, the regular units of the organization rapidly formed a structure that incorporated traditional features commonly found in conventional armies, including the ability to maneuver quickly and engage in infantry attacks (Lewis, 2014: 13-16).

While the group's militants started functioning like a conventional army, comparing their military capabilities with those of any nation is not practical. Even at its peak, the organization had approximately 3000 soldiers, and not all were assigned to regular units (NBC News, 2015).

On the other hand, any endeavor to compare the military apparatus of ISIS and Russia would be devoid of significance. ISIS acquired guns and ammunition by taking control of military sites and confiscating the weaponry of captured soldiers in Syria and Iraq (Byman, 2016: 148). Despite the organization's notable successes in Iraq and Syria, its military arsenal remains relatively modest compared to a conventional army.

The regular forces of the organization, albeit weaker in terms of both people and military equipment compared to a state actor, played a crucial part in ISIS's hybrid warfare. These units were used in battles and in conjunction with guerrilla operations, which increased the efficiency of these assaults (Cockburn, 2014: 62-68).

Given Russia's substantial military force and superior equipment, it can be inferred that Russian regular troops were more proficient than ISIS forces during the conflicts in Eastern Ukraine and the invasion of Crimea. Nevertheless, the actuality diverges. Russian regular troops have demonstrated significantly worse effectiveness in warfare compared to regular units of ISIS.

The limited impact is not due to the regular forces being inadequate but rather stems from the Kremlin's intention to prevent negative repercussions from the

international community. Consequently, Russia has employed its forces sparingly in combat. Russia sent the 18th Army Brigade to the Donetsk and Luhansk regions to influence the trajectory of the conflict. The size of this brigade is approximately 4000 soldiers. Nevertheless, it refrained from carrying out extensive assaults. However, its operations were limited to battalion tactical groups that only assisted pro-Russian insurgents in the region (Reisinger & Golts, 2014: 5). Evidently, the solitary brigade dispatched by Russia in the region surpasses the entire army of ISIS in terms of size.

Russia has predominantly employed its regular forces to coerce Ukraine, the European Union, and NATO allies through intimidation. From 2014 to 2015, spanning 20 months, Russia carried out eight significant military drills. A number of these drills were conducted near the Ukrainian border, showcasing their preparedness for conflict and their potential to act militarily in Ukraine if the need arises. Russia strategically deployed its forces around the Eastern Ukrainian border to instill fear and demonstrate its preparedness for potential action (Luhn, 2014).

Within this framework, it can be asserted that Russia's regular forces have been predominantly employed for psychological intimidation and attrition of their adversaries. At the same time, actual combat operations have been kept to a minimum. However, despite possessing significantly smaller regular forces, ISIS has yet to show hesitation in deploying them in combat. Through the strategic coordination of these forces with guerrilla strikes, ISIS successfully attained significant territorial and strategic advancements in both Iraq and Syria. ISIS publicly deployed regular forces, but Russia's hesitance to involve its troops in combat can be ascribed to concerns about global repercussions and the aim to evade a potential confrontation with NATO. Russia's hybrid warfare strategy revolves around the crucial aspects of deniability and evading international repercussions.

4.4. ASYMMETRIC TACTICS

Hybrid warfare necessarily incorporates the employment of asymmetric techniques. Hence, it is valid to claim that both Russia and ISIS have employed asymmetric strategies in their hybrid attacks. However, significant differences become evident when these uneven approaches are examined more closely.

A notable disparity between Russia and ISIS lies in their use of SVBIEDs. ISIS has effectively utilized SVBIEDs in both offensive and defensive capacities. This demonstrates the organization successfully integrating its current expertise in this field into its hybrid warfare strategy.

The employment of SVBIEDs by ISIS in its strikes, particularly in Raqqa, has attracted significant attention due to their unique methods. The organization utilized rocket launchers and machine gun-equipped SVBIEDs in Raqqa, a strategy that intensified the effectiveness of their attacks. ISIS strategically employs SVBIEDs as a vital component in their asymmetric warfare strategies. It is estimated that ISIS conducted 482 SVBIED attacks in Mosul between October 19, 2016, and July 12, 2017. The available data indicates that no other battle has exhibited such a notable frequency of SVBIED (Suicide Vehicle-Borne Improvised Explosive Device) employment. This underscores the importance of SVBIED deployment in the organization's asymmetrical tactics. (Spence & Geroux, 2021). However, there is no substantiated information indicating that Russia has orchestrated any SVBIED attacks.

Nonetheless, the organization has endeavored to transform its uneven disadvantages into benefits by integrating various assault strategies, armaments, and military divisions. ISIS has a strategic approach involving synchronizing many weapons and technologies. For example, during its attacks in Raqqa, the organization employed SVBIEDs, unmanned aerial vehicles (UAVs), and guerrilla units concurrently. UAVs would detect targets in the vicinity and guide teams for SVBIED assaults during these missions. After the SVBIED bombings, ISIS fighters would surreptitiously enter the area to launch their assaults. During these strikes, ISIS stationed snipers close to the areas of fighting, offering remote assistance to the guerrilla fighters (Ashour, 2021: 53-68).

ISIS employed many asymmetric tactics beyond the utilization of SVBIEDs. The organization has successfully operated over a large geographical area by using suicide bombers and engaging in other acts of violent terrorism. ISIS orchestrated almost 500 suicide strikes in Iraq, Syria, and Libya within the initial five months of 2016. It is believed that ISIS conducted terrorist attacks in the Middle East and Europe, causing the deaths of around 30,000 military personnel and civilians (Glum,

2016). The ISIS assaults in Paris and Belgium have specifically emphasized the organization's position as a global menace (Cruickshank, 2017). Through the incorporation of acts of terror into its asymmetric strategies, ISIS has aimed explicitly at its adversaries and transformed into a worldwide security concern.

ISIS has effectively employed asymmetrical warfare strategies, resulting in devastating outcomes, not only in traditional battlefields and rural communities but also in cities with high populations. The excavated fortifications constructed by ISIS within urban areas have played a substantial role in their tactics for both defending and attacking. In Syria, ISIS excavated trenches around strategically significant buildings to bolster its defensive measures. These trenches were also utilized to avoid aerial bombardments. ISIS militants employed a tactic of burning oil in the trenches they excavated to generate a smokescreen, thus diminishing the impact of airstrikes, particularly those carried out by the United States.

Moreover, the presence of snipers strategically located within these trenches has resulted in a significant number of deaths. The trenches have played a particularly vital role in ISIS's defence. The group constructed a trench spanning 500 kilometres, stretching from Sinjar to Kirkuk. This trench served as a defensive barrier, effectively safeguarding the territory it had seized from the Peshmerga forces (Gündüz, 2017: 6-7).

ISIS has also utilized human beings and civilian structures as instruments of its asymmetric tactics. The organization employed war prisoners and local civilians as human shields in both Iraq and Syria to impede attacks targeting them. Furthermore, ISIS flags were raised on buildings and structures where civilians resided to deceive airstrikes. The organization pursued two objectives: firstly, to minimize casualties by accurately targeting the airstrikes; secondly, to provoke resentment among the local population towards the West by causing civilian deaths in the airstrikes, thus gaining support for the organization (Iraq: Feared ISIS Use of 'Human Shields,' Executions, 2016).

Similar to ISIS, Russia has also employed asymmetric tactics. Nevertheless, Russia's classification as a sovereign nation and its possession of substantial military and financial capabilities have impacted the specific strategies utilized.

Russia has deployed special forces soldiers in the Crimea and Donbas regions, in contrast to ISIS. The Spetsnaz, a specialized military unit, has participated in several military campaigns, including the initial takeover of Crimea. Despite Russia's consistent denial, it was eventually revealed that these forces in the region consisted of soldiers from the Russian army (BBC, 2014).

A notable distinction between Russia and ISIS lies in the influence exerted by Russian intelligence agencies on the conflict. Russia is a nation that has been present in Eurasia for a long time and has well-established institutions, which means it has a strong intelligence network. Before the commencement of the Russo-Ukrainian conflict, Russian intelligence was already engaged in activities within Ukraine, acting in opposition to Russian objectives. Personnel from the Federal Security Service (FSB) and General Staff of the Armed Forces of the Russian Federation (GRU) actively took part in anti-government demonstrations in Ukraine to instigate the local population against the government. In addition, FSB and GRU operatives remained present in the region during the wars, carrying out various actions such as collecting intelligence, engaging in espionage, stealing information, and conducting other intelligence-related operations (Kılıçoğlu, 2022).

Russia has extensively employed Private Military Companies (PMCs) as a critical asymmetric strategy in the Ukraine War. Ukraine has functioned as a primary area of conflict where Russia has conducted trials and evaluations to determine the advantages of PMCs. Several private military companies (PMCs), such as Wagner, Vengia, E.N.O.T., Convoy, and others, have been involved in the Russo-Ukrainian war (Katz, G. Jones, Doxsee, & Harrington, 2020). The primary rationale behind the deployment of these groups is the convenient ability to disclaim their connections to Russia plausibly. Moreover, comprised of seasoned military personnel, these factions have played pivotal roles in combat situations. PMCs have carried out activities with the assistance of the Russian military during the annexation of Crimea and the battles in the Donbas region. The Wagner Group significantly influenced the Eastern Ukraine hostilities from 2014 to 2015 (Lohmus, 2023: 23-31).

4.5. NATURAL RESOURCES AS HYBRID MEANS

A notable distinction between Russia and ISIS lies in Russia's ownership and strategic use of substantial oil resources to exert influence in international relations. Russia holds the position of being the second-largest global producer and exporter of natural gas. Furthermore, Russia is a prominent nation in oil production and exporting (Russia - Countries & Regions -IEA, 2023). Russia's ability to exert more assertive actions in foreign policy and exploit economic ties to its benefit is facilitated by Ukraine's and European countries' reliance on Russian natural gas (Davis, 2016: 176).

Russia has effectively leveraged Ukraine's energy dependence to its advantage in their economic relations. Following the Orange Revolution in 2004, which resulted in the pro-Western Yushchenko government coming into power, Russia strategically employed the rise in natural gas prices to exert pressure. In 2004, Ukraine procured natural gas from Russia at \$50 per thousand cubic meters. However, after the Orange Revolution, the costs surged by a factor of five, resulting in the worth of the equivalent quantity of natural gas escalating to \$250. The upward trend in natural gas prices persisted, and by 2014, the Kremlin upped the price for a thousand cubic meters of natural gas to \$500.

Furthermore, although the Kremlin had previously granted leniency in Ukraine's plan for repaying its debt, shortly after the revolution, it insisted on an immediate payment in cash for the outstanding natural gas arrears. The increased prices and the requirement to promptly settle energy bills owed to Russia worsened Ukraine's economic challenges. As mentioned earlier, the scenario caused a disturbance in Ukraine's economic and political equilibrium, exacerbating the detrimental consequences of Russia's economic sanctions and military interventions in Ukraine (Newnham, 2018: 10-12).

The Kremlin's utilization of Ukraine's reliance on natural gas as a diplomatic instrument went beyond the simple act of increasing natural gas prices. Russia halted natural gas supply to Ukraine twice during the winter months of 2006 and 2009. Both disruptions occurred throughout political tension between the two governments while Ukraine actively pursued pro-Western policies. The Kremlin's involvement in

Ukraine's foreign policy has been inferred from this action. The interventions were strategically timed over winter to maximize effectiveness (Dragneva & Wolczuk, 2016: 688-695).

Russia strategically employs its dominance over energy resources as a diplomatic instrument, not only to exert pressure on Ukraine but also to exert influence over Western countries and NATO. More precisely, Russia seeks to influence Western countries' selection of natural gas suppliers by utilizing the Nord Stream natural gas pipelines. Russia's Energy Strategy 2035 roadmap highlights the intention to monopolize Europe's energy imports. Russia views the management of energy resources as crucial for maintaining and increasing its influence in foreign affairs. Its objective is to sustain Europe's reliance on Russian natural gas. Russia utilizes this technique as a prominent instrument in its interactions with the West and NATO, increasing apprehensions regarding Europe's energy security (Ozawa & Iftimie, 2020).

Nonetheless, it is only partially accurate to claim that ISIS utilized natural resources to apply pressure or implement policies. The organization predominantly leveraged the natural gas and oil reserves in the territories it seized in Iraq and Syria to fund its hybrid warfare. In 2014, ISIS took possession of the Al-Omar oil field in Syria, which had a daily oil production capacity of 75,000 barrels. The group utilized the resources obtained from this well to bolster its military capabilities (Tonkuş & Sağlam, 2014). To manage the resources it acquired effectively, ISIS established a Ministry of Resource Distribution, facilitating the transfer of resources to relevant units. In 2015, it was estimated that ISIS generated over 2 billion dollars in revenue from natural resources (Levallois, Cousseran, & Kerrello, 2017).

Within this framework, it can be asserted that natural resources play a crucial role for both Russia and ISIS in their execution of hybrid warfare. Nevertheless, distinct disparities become apparent when examining their specific means of application. ISIS has utilized the natural resources it has seized to fund its military activities, whereas Russia employs these riches as a tool for conducting its foreign policy.

4.6. TERRITORIAL ACQUISITION AND GEOPOLITICAL INFLUENCE ASPIRATION

Both Russia and ISIS have aimed to gain territorial control and enhance their geopolitical power through hybrid warfare. While the political outcomes they sought through territorial gains differ, their desire to acquire land and strengthen geopolitical influence is common (Gurganus & Rumer, 2019; Stanford University, 2021; Wright, 2017).

One of Russia's primary reasons for annexing Crimea was the region's geographic alignment with Russia's political objectives. The occupation enabled Russia to take control of the Sevastopol port, strategically positioning the Black Sea Fleet and securing significant regional dominance (Charron, 2016: 225-235). Moreover, Russia has attempted to counter Ukraine's Western pivot by annexing Crimea and conducting covert operations in Donbas, aiming to maintain regional stability in its favor (Lawrence, 2022: 198-205).

On the other hand, ISIS's motivation for territorial expansion in Iraq and Syria was primarily ideological and religious. They sought to establish an Islamic Caliphate to spread their interpretation of Islam worldwide, believing the caliphate must possess land. Additionally, ISIS needed territorial control to claim political legitimacy and military power. For a time, ISIS operated as a state, using social media propaganda to demonstrate its provision for the people under its caliphate (Cambanis et al., 2019: 111).

Despite the different political outcomes each actor desired from territorial gains, it should not be interpreted that they did not want the same outputs. For example, both actors aimed to seize management of economic resources as a result of territorial gains; by taking Crimea, Russia not only gained control of the strategically important Sevastopol port but also other vital ports like the Feodosiya Port (Grant, 2015: 68-77). Moreover, the control over regions in Crimea rich in agriculture and natural resources also passed to Russia (Cahill & Palti-Guzman, 2023: 3).

ISIS, meanwhile, captured natural resources, particularly oil reserves, generating substantial financial resources. The group used the oil wells in Syria and Iraq to finance its hybrid warfare, and by controlling agricultural lands in these areas,

ISIS increased its income. Given the lack of official declarations by ISIS as a formal organization, it is difficult to determine the precise amount of revenue earned. Nevertheless, an autonomous investigation has ascertained that ISIS's income from oil hit its zenith approximately in the midst of 2015. ISIS's monthly oil revenues during this period were reported to be around \$40 million (Crane, 2015). Thus, the effective use of economic resources bolstered their influence and regional operational capabilities.

Regardless of the political and military outcomes Russia and ISIS planned, it can be said that they used hybrid warfare to increase territorial gains, strengthen geopolitical positioning, capture strategic points, and seize economic resources in the regions where they were effective.

CONCLUSION

The complicated nature of hybrid warfare and its place in modern wars are thoroughly examined in this thesis. Since the end of the Cold War, it has been evident that traditional explanations of warfare are inadequate for comprehending and elucidating contemporary conflicts. This has prompted researchers and academics to propose several theories to clarify these modern conflicts. The thesis's chapter on the conceptual framework elaborates on the nature of these concepts. One of the newer concepts among these suggestions is hybrid warfare. Frank Hoffman, regarded as the conceptual creator of this concept, has maintained that comprehension of hybrid warfare is required to explain conflicts in the twenty-first century. This concept is essential when considering how complicated and multifaceted today's conflicts are.

Modern wars primarily differ from conventional warfare in that they take on cyber, economic, psychological, and diplomatic aspects in addition to physical ones. Therefore, states and non-state actors must design their strategies in a flexible and adaptable way to accommodate this complex structure that is evolving on the battlefield. Because of its flexibility and adaptability, hybrid warfare is a concept that makes it possible to understand the complexity of battlefields.

Modern technologies have significantly shaped the nature of modern warfare. It is not appropriate to confine our discussion of contemporary technologies to developments in the armaments industry. The emergence of cyberspace, widespread internet usage, and the spread of social media platforms have revealed crucial components in figuring out state and non-state actors' conflict strategies. During conventional warfare, aggressors would use gunfire to destroy transportation systems, energy networks, and infrastructure, but today, cyberattacks can target similar goals. It makes attacks more economical and covert.

Due to this transformation, the aggressor and the target now have another path to pursue. Disinformation campaigns and information warfare are essential components of this change. Hybrid aggressors use this transition by disseminating misleading information to deceive the public, demoralize the opponent, and further their political objectives. The modern era's ease of access to information has also

made it easier to manipulate information, simplifying disinformation tactics. Such disinformation campaigns include Russia's capacity to hide its involvement as the secret hand behind the takeover of Crimea for a set amount of time. However, the widespread expansion in the use of social media is one of the main reasons ISIS could recruit foreign warriors from many countries and propagate the idea of a caliphate throughout the world.

One of the critical inquiries around hybrid warfare is whether its rise is an unavoidable outcome of shifts in battlefields, doctrines, or technology or a preferred tactic due to its benefits. It appears impractical to give a straightforward and unambiguous response to this topic. Without a doubt, the changes taking place in the 21st century have established the basis for the concept of hybrid warfare, while the ambitions of various actors to acquire unequal advantages have played a role in the evolution of hybrid warfare. Hence, hybrid warfare is simultaneously a catalyst and a consequence.

Actors employ hybrid warfare for a multitude of reasons. The reasons for this can vary based on several aspects, such as the actor's political motives, geographical position, institutional power, compliance with international law, and apprehensions regarding international sanctions.

When analyzing the motivations behind players employing hybrid warfare, a prominent factor is the intention to counteract the disadvantages of power disparity. Hoffman's explanation of hybrid warfare primarily draws on the 2006 Hezbollah-Israel war, highlighting the frequent utilization of this idea by less powerful factions. This claim is substantiated by the strategies employed by the Chechens in their conflicts with the Russians throughout both the first and second Chechen Wars. The hybrid warfare tactics utilized by ISIS, first in Iraq and Syria and subsequently in nearby nations like Turkey and even in regions beyond, such as Europe, support this same approach.

Nevertheless, Russia's behavior during the annexation of Crimea in 2014 has demonstrated that this viewpoint on hybrid warfare is overly simplistic. Although Russia has superior capabilities to Ukraine in various sectors, and the power imbalance favored Russia, it refrained from engaging in conventional warfare and instead employed hybrid tactics. Hybrid warfare can exhibit different characteristics

based on the political motives and capabilities of the aggressor involved. Various underlying factors drive Russia's implementation of hybrid warfare against Ukraine and Western governments.

A key reason for employing hybrid warfare is to avoid the influence of global public opinion. Russia, unlike Hezbollah, the Chechens, and ISIS, has demonstrated a propensity for concealing its identity during its assaults.

One significant factor that led Russia to employ hybrid warfare during the annexation of Crimea and its involvement in the hostilities in Eastern Ukraine was its concern about world public opinion and the implementation of sanctions. Hybrid warfare encompasses tactics, including traditional military operations, cyberattacks, disinformation campaigns, economic and diplomatic sanctions, covert operations, and backing for separatist organizations. Russia's use of hybrid warfare is driven by the need to avoid or minimize the possible repercussions of international law and sanctions, all while pursuing political goals.

Russia effectively employed disinformation tactics to mitigate international response during the annexation of Crimea. Instead of engaging in direct military engagement, Russia assisted separatist groups and deployed specialized units in Crimea and Eastern Ukraine while simultaneously denying their presence. The commencement of an overt conflict by Russia against Ukraine in 2022, together with its subsequent economic and political ramifications, highlights the apparent benefits that hybrid warfare provides to the attacking party. Since the commencement of the war in 2022, Russia has been confronted with many economic and political sanctions. Conversely, Crimea was incorporated promptly with minimal global reaction, leading to Russia encountering significantly fewer sanctions.

The concept of hybrid warfare can be highly elusive, contingent upon the aggressor's level of expertise, making its detection exceptionally challenging. Actors can disperse their attacks over numerous years. The intricate characteristics of hybrid warfare render it difficult to ascertain the source of the strike. Occasionally, the intended recipient may remain oblivious to the fact that they are being subjected to an assault. Hybrid warfare can provide favorable outcomes not only against opponents but also against the aggressor's populace. Conventional conflicts are undesirable, as they negatively impact the soldiers engaged in combat and the

country's general population. Extended and arduous battles can potentially diminish leaders' political influence and legitimacy. Neither the Russian populace nor Western governments completely grasped the fact that Russia was launching an attack until the annexation of Crimea was executed correctly.

Actors often choose hybrid warfare because of its cost-effectiveness compared to conventional military engagements. The adaptable hybrid warfare strategy, which combines traditional and nontraditional components, enables actors to attain optimal effectiveness while utilizing limited resources. Conventional wars necessitate the coordination of substantial military campaigns and the massive utilization of people and material resources. Conversely, hybrid warfare can produce significant results with reduced expenses and a smaller workforce. Utilizing hybrid warfare tactics, including cyberattacks, dissemination of false information, and psychological manipulation via social media and digital platforms, can significantly undermine the strength of an adversary. These elements can occasionally bolster traditional military actions or substitute them during various stages of warfare.

The evolving nature and complex characteristics of contemporary conflicts have made traditional approaches inadequate for comprehending these conflicts. The notion of hybrid warfare aims to provide a complete framework for comprehending the intricate character of contemporary conflicts. Nevertheless, this strategy has also prompted objections against hybrid warfare. Specific authors contend that it is simply a captivating term that attempts to capture and elucidate all aspects within its scope. A considerable contingent of critics argue that the notion of hybrid warfare is not novel, contending that it simply redefines conflict tactics that have been present throughout history.

It is accurate to point out that the components associated with hybrid warfare have been utilized in several historical conflicts. Historically, guerilla attacks have been employed with conventional assaults for millennia. Psychological warfare, as stated in the works of Sun Tzu, is a significant method of attrition. Nevertheless, as suggested, the primary distinction between historical instances and hybrid conflicts resides in their “hybrid” characteristics. Hybrid warfare is the outcome of the capacity to combine several methods of attack into a single entity and employ them concurrently. These offensive strategies are intentionally adaptable and are executed

at various strategic, tactical, and operational levels based on the progression of the battle, an intricate and diverse notion that poses challenges in defense. Consequently, hybrid warfare has gained more popularity than previous war concepts in comprehending and interpreting contemporary battles.

Gaining comprehension and deciphering contemporary conflicts is equally crucial to strategizing effective countermeasures. Identifying a hybrid attack can be challenging, and it may already be too late when the intended victim becomes aware of it. Hence, actors and the international community must implement various steps to counter hybrid warfare.

The primary stage would involve augmenting awareness through educational approaches to initiate this process. The effective response to hybrid warfare necessitates the augmentation of societal knowledge across all sectors, extending beyond solely military personnel. It is imperative to organize these trainings to include politicians, military people, civil society organizations, and all segments of the public. Given the diverse capabilities of hybrid aggressors, offering a comprehensive array of training programs is imperative. Undoubtedly, imparting identical training to every stratum of society is impracticable and superfluous. As an illustration, military personnel can get training on using regular and irregular military units in hybrid warfare. At the same time, the general population can be educated on identifying misinformation operations and propaganda activities, bolstering cyber security, and improving social media literacy. Government officials, however, can receive training in recognizing hybrid attacks, understanding international law, mastering crisis management, and developing strategic planning skills.

States must incorporate military and civilian defense measures to combat hybrid warfare effectively in this environment. Hybrid warfare blurs the distinction between military and civilian domains, expanding the fight's scope beyond purely military aspects and incorporating civilians into the struggle. Hence, it is imperative to amalgamate military and civilian defense. For example, joint training and exercise programs can unite civilian and military personnel. By doing so, both parties can enhance their comprehension of each other's requirements and capabilities and develop the ability to collaborate effectively. Implementing standardized units to facilitate communication between civil and military institutions and constructing

communication networks are further steps to be used. In addition, creating crisis management centers, which assemble specialists from many fields, can expedite the development of prompt and efficient resolutions in times of crisis.

Addressing hybrid warfare requires collaborative efforts involving individual governments and other relevant actors. The international community must enhance legal and normative structures, precisely delineate hybrid warfare strategies, and impose sanctions on them. Specifically, it is necessary to establish regulations for international laws about cyberattacks, provide clear definitions and penalties for cybercrimes, and improve the ability to monitor actions in cyberspace. Furthermore, enhancing media and communication rules is imperative to thwart disinformation campaigns effectively. There is a need to establish international rules and standards to combat hybrid warfare methods effectively. This requires more international collaboration and coordination to address this issue. Implementing these legal and normative frameworks will serve as a robust means of protection against hybrid warfare and as a deterrent to individuals or groups involved in such actions.

States must use military and civilian defensive strategies to combat hybrid warfare, as hybrid warfare erases the distinction between military and civilian domains. It broadens the scope of the fight beyond the military domain, encompassing citizens as active participants in the conflict.

In conclusion, hybrid warfare is crucial for comprehending and analyzing contemporary conflicts. This notion, which has garnered attention for almost two decades, has showcased its impact, utilization, and possible dangers to the global community through instances such as ISIS and Russia. As a result, the notion has swiftly become a prominent topic on the agenda of international security groups such as NATO. Hence, it is crucial for the international community to fully grasp the complexities of hybrid warfare and implement countermeasures accordingly.

REFERENCES

Abdyraeva, C. (2020). (Rep.). OIIP - Austrian Institute for International Affairs.

Abu Bakr al-Baghdadi: IS leader appears in first video in five years . (2019, April 30). *BBC News*.

Ackerman, S. (2015, January 12). US Central Command Twitter account hacked to read 'I love you Isis'. *The Guardian*. Retrieved June 6, 2021, from <https://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack>, 12.06.2023.

Afineevsky, E. (Director). (2015). Winter on Fire: Ukraine's Fight for Freedom [Motion Picture].

Angstrom, J. (2017). Escalation, Emulation, and the Failure of Hybrid Warfare in Afghanistan. *Studies in Conflict and Terrorism*. 40(10): 838–856.

Aoi, C., Futamura, M. and Patalano, A. (2018). Introduction 'hybrid warfare in Asia: its meaning and shape. *The Pacific Review*. 31(6): 693–713.

Archambault, E. and Veilleux-Lepage, Y. (2020). Drone imagery in Islamic State propaganda: flying like a state. *International Affairs*, 96(4), 955–973.

Armstrong, M. (2016, July 29). *Terrorist attack victims in Western Europe* . Retrieved from Statista : <https://www.statista.com/chart/4554/terrorist-attack-victims-in-western-europe/>, 12.06.2023.

Arslan, H. (2021). Hibrit savaş 2014 yılı Rusya'nın Ukrayna müdahalesi (Master's Degree). Milli Savunma Üniversitesi.

Ashour, O. (2021). *How ISIS Fights: Military Tactics in Iraq, Syria, Libya and Egypt*. Edinburg: Edinburgh University Press.

Asymmetric Warfare Group. (2016). *Russian New Generation Warfare Handbook*. Florida : Asymmetric Warfare Group.

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy* , 138–149.

Azani, E. and Dotti, F. (2021). The Islamic State's Web Jihadi Magazine Dabiq and Rumiya. More than just propaganda. *International Institute for Counter-Terrorism*, 1-28.

Bachmann, S. and Gunneriusson, H. (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.

Barfi, B. (2016, February). The Military Doctrine of the Islamic State and the Limits of Ba'athist Influence. *Combating Terrorism Center*, 9(2), 18-24.

Barret, R. (2014). *Media Operations*. New York: Soufan Group.

Beccaroa, A. (2018). Modern Irregular Warfare: The ISIS Case Study. *Small Wars & Insurgencies*, 29(2), 207–228.

Bektaş, M. H. and Gündoğdu, A. Y. (2019). IŞİD'in Hibrit Savaş Stratejileri: Hibrit Savaş Konsepti Perspektifinden Analizi. *International Journal of Politics and Security*, 1(1), 25-56.

Bender, J., Rosen, A. and Wilson, J. (2016, Jan 17). These are the weapons Islamic State fighters are using to terrify the Middle East. *Business Insider* .

Besemeres, J. (2016). Russian disinformation and Western misconceptions. In J. Besemeres, *A Difficult Neighbourhood* (pp. 356-379). ANU Press.

Bıçakçı, S. (2019, November). Hibrit Savaş. Güvenlik Yazıları Serisi, 33. https://trguvenlikportali.com/wpcontent/uploads/2019/11/HibritSavas_SalihBicakci_v.1.pdf, (20.12.2020).

Blaker, L. (2016). The Islamic State's Use of Online Social Media. *Military Cyber Affairs*, 1(1), 1-9.

Boer, L. d. (2023, May 30). Disinformation in a Time of War: A Critical Discourse Analysis of Russian Disinformation Strategies During the Russo-Ukrainian War of 2022. Euroculture.

Boot, M., Brahimi, A., Kemp, W., Tobias, J. and Weiss, T. G. (2015). Chapter One: The Changing Character of Conflict. *Armed Conflict Survey*. 1(1): 11-68.

Boyer, Y. and Lindley-French, J. (2012). *The Oxford Handbook of War*. (Y. Boyer and J. Lindley-French, Eds.) New York: Oxford University Press Inc.

Bronk, C. and S. Anderson, G. (2017). Encounter Battle: Engaging ISIL in Cyberspace. *The Cyber Defense Review*, 2(1), 93-108.

Bryjka, F. (2019, August 14). Russian "Contractors" In the Service of the Kremlin. Retrieved from Warsaw Institute: "<https://warsawinstitute.org/russian-contractors-in-the-service-of-the-kremlin/>" , 12.06.2023.

Bunker, R. J. (2015). Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications. *Strategic Studies Institute*,, 1-55.

Byman, D. (2016). Understanding the Islamic State— A Review Essay. *International Security*, 40(4), 127-165.

Cahill, B. and Palti-Guzman, L. (2023). The Role of Gas in Ukraine's Energy Future. *Center for Strategic and International Studies*, 1-9.

Calışkan, M. (2019). Hybrid warfare through the lens of strategic theory. *Defense & Security Analysis*. 35(1): 40-58.

Cambanis, T., Esfandiary, D., Ghaddar, S., Hanna, M. W., Lund, A. and Mansour, R. (2019). *Hybrid Actors: Armed Groups and State Fragmentation in the Middle East*. New York: The Century Foundation Press.

Cendrowicz, L., Harding, L. and Luhn, A. (2014, April 10). Satellite images reveal Russian military buildup on Ukraine's border. *The Guardian*. Retrieved May 3, 2021

Center for Strategic & International Studies. (2015). The Russian Military Forum: Russia's Hybrid War Campaign: Implications for Ukraine and Beyond [Video]. Retrieved from "<https://www.csis.org/events/russian-military-forum-russias-hybrid-war-campaign-implications-ukraine-and-beyond>" , 12.06.2023.

Charron, A. (2016). Whose Is Crimea? Contested Sovereignty and Regional Identity. *Region*, 5(2), 225-256.

Chrisafis, A. and Gibbs, S. (2015, April 9). French media groups to hold emergency meeting after Isis cyber-attack. *The Guardian*. Retrieved June 7, 2021, from <https://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers>, 12.06.2023.

Cilluffo, F. J. and Clark, J. R. (2012). Thinking About Strategic Hybrid Threats—In Theory and in Practice. *PRISM*. 4(1): 46-63.

Cin, G. (2019). Güvenlik Problemlerinin Hibrit Savaş Kapsamında İncelenmesi: Doğu Ukrayna ve Kırım Örnekleri(2014-2015) (Master's Degree). T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü.

Clark, M. (2020). Russian Hybrid Warfare. Institute for the Study of War.

Clark, M. (2020). The Russian View of Future War: Unconventional, Diverse, and Rapid. Institute for the Study of War.

Cockburn, P. (2014). *The Rise of Islamic State: ISIS and the New Sunni Revolution*. New York: Verso.

Cohen, A. (2019, February 28). As Russia Closes In On Crimea's Energy Resources, What Is Next For Ukraine? Retrieved from Forbes: "<https://www.forbes.com/sites/arielcohen/2019/02/28/as-russia-closes-in-on-crimeas-energy-resources-what-is-next-for-ukraine/?sh=7124616429cd>", 12.06.2023.

Coles, I. and Parker, N. (2015, December 11). How Saddam's men help Islamic State rule . *Reuters* .

Connell, M. and Vogler, S. (2016). *Russia's Approach to Cyber Warfare*. Washington: CNA Analysis & Solutions.

Cordesman, A. H. (2021). The Biden Transition and U.S. Competition with China and Russia: The Crisis Driven Need to Change U.S. Strategy. Center of Strategic & International Studies.

Costea, C. A. (2020). Rusya'nın Ukrayna'daki Hibrid Savaşı (2014-2018). Ankara: SETA Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı.

Cramers, P. A. and Caliskan, M. (2018). What Do You Mean by Hybrid Warfare? A

Content Analysis on the Media Coverage of Hybrid Warfare Concept. *Horizon Insights*. 4: 23-36.

Crane, K. (2015). *The Role of Oil in ISIL Finances*. RAND Cooperation.

Croft, S. (2014, September 28). President Obama: What makes us America. *CBS News*. Retrieved May 14, 2021, from <https://www.cbsnews.com/news/president-obama-60-minutes/>, 12.06.2023.

Cronin, A. K. (2015). ISIS Is Not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat. *Foreign Affairs*, 94(2), 87-98.

Cullen, P. J. and Reichborn-Kjennerud, E. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. Multinational Capability Development Campaign.

Çalışkan, M. and Cramers, P. A. (2018). What Do You Mean by "Hybrid Warfare"? A Content Analysis on the Media Coverage of Hybrid Warfare Concept. *Horizons Insights*, 4, 23-35.

Danyk, Y., Maliarchuk, T. and Briggs, C. (2017). Hybrid War: High-tech, Information and Cyber Conflicts. *Connections*. 16(2): 5-24.

Davis, C. M. (2016). The Ukraine conflict, economic–military power balances and economic sanctions. *Post-Communist Economies*, 28(2), 167-198.

Dayspring, S. M. (2015). *Toward a Theory of Hybrid Warfare: The Russian Conduct of War During Peace*. Master's Thesis. California: Naval Postgraduate School. Retrieved from "https://calhoun.nps.edu/bitstream/handle/10945/47-931/15Dec_Dayspring_Stephen.pdf?sequence=1&isAllowed=y", 12.06.2023.

Doğru, A. (2017). Hybrid Warfare, Daesh and Turkey's Stance. *ANKASAM | Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, 1(2), 130-161.

Dragneva, R. and Wolczuk, K. (2016, June). Between Dependence and Integration: Ukraine's Relations With Russia. *Europe-Asia Studies*, 68(4), 678-698.

Ereker, F. A. (2019, October). Haklı Savaş. *Güvenlik Yazıları Serisi*(18).

EUR-Lex: Access to European Union Law. (2018). Retrieved from Joint Communication To The European Parliament, The European Council And The Council Increasing resilience and bolstering capabilities to address hybrid threats: "<https://eurlex.europa.eu/legalcontent/GA/TXT/?uri=CELEX:52018JC0016>", 12.06.2023.

Euronews. (2022, December 10). Retrieved February 2023, from 2016 Brussels bombings: Ten men go on trial over airport and metro attacks: <https://www.euronews.com/2022/12/05/brussels-attacks-ten-men-go-on-trial-over-2016-terror-bombings-in-belgian-capital>, 12.06.2023.

European Leadership Network. (2016). Major Russian exercises have been conducted since 2014 in its European territory and adjacent areas.

Fabian, S. (2019). The Russian hybrid warfare strategy – neither Russian nor strategy. *Defense & Security Analysis*, 35(3): 308-325.

FATF. (2015). *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*. Paris: Financial Action Task Force.

Fordham, A. (2014, October 21). Ambushes, Mines And Booby Traps: ISIS Militants Change Tack. *National Public Radio*.

Freedman, L. (2014). Ukraine and the Art of Limited War. *Survival*. 56(6): 7-38.

Galeotti M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?, *Small Wars & Insurgencies*. 27:2: 282-301.

Gambhir, H. (2016). *The Virtual Caliphate: ISIS's Information Warfare*. Washington: Institute for the Study of War .

Ganor, B. (2012). The Hybrid Terrorist Organization and Incitement. In A. Baker (Ed.), *The Changing Forms of Incitement to Terror and Violence: The Need for a New International Response* (pp. 13-19). Jerusalem Center for Public Affairs, Jerusalem .

Gardner, H. (2015). Hybrid Warfare: Iranian and Russian Versions of "Little Green Men" and Contemporary Conflict. *NATO Defense College*: 1-16.

Gaub, F. (2015). Hybrid tactics: ISIL & Co. European Union Institute for Security Studies.

General Staff of the Armed Forces of the Russian Federation. (2010). The Military Doctrine of the Russian Federation.

Georgieva, T. and Petkov, P. (2018). Expert Framework for Measuring the Institutional Capabilities to Counter Hybrid Threats. *Information & Security: An International Journal*. 39(3): 237-256.

Gerasimov V., "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," trans. Robert Coalson, *Military-Industrial Kurier*, 27 February 2013, accessed 27 October 2015, <http://www.theatlantic.com/education/archive/2015/10/complexacademicwriting/412255/>, 12.06.2023.

Giantas, D. and Stergiou, D. (2018). From Terrorism to Cyber-terrorism: The Case of ISIS. *Social Science Research Network*, 1-32. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927, 12.06.2023.

Giegerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict. *Connections*. 15(2): 65–72.

Giles, K. (2019). “Hybrid Threats”: What Can We Learn From Russia? Federal Academy for Security Policy.

Gök, A. (2021). Hibrit savaşlar Rusya'nın Afganistan (1979) ve Ukrayna (2014) askeri müdahaleleri ile israil-lübnan savaşları (1982, 2006) örnek olayları ışığında tarihsel-mukayeseli bir inceleme (PHD Degree). Yıldırım Beyazıt Üniversitesi.

Grant, T. D. (2015, January 15). Annexation of Crimea. *The American Journal of International Law*, 109(1), 68-95.

Gurganus, J. and Rumer, E. (2019, February 20). *Russia's Global Ambitions in Perspective*. Retrieved from Carnegie Endowment for International Peace : <https://carnegieendowment.org/2019/02/20/russia-s-global-ambitions-in-perspective-pub-78067>, 12.06.2023.

Gündüz, İ. (2017). The Islamic State of Iraq and Al-Sham and Its Urban Warfare Tactics. *The Foreign Military Studies Office*, 1-16.

Haines, J. R. (2016, March). How, Why, and When Russia Will Deploy Little Green Men – and Why the US Cannot. *Foreign Policy Research Institute*. "<https://www.fpri.org/article/2016/03/how-why-and-when-russia-will-deploy-little-green-men-and-why-the-us-cannot/>" , 12.06.2023.

Hammes, T. X. (2007). Fourth Generation Warfare Evolves, Fifth Emerges . *Military Review*. 14-23.

Harding, L. (2010, April 21). Ukraine extends lease for Russia's Black Sea Fleet. *The Guardian*. Retrieved from "<https://www.theguardian.com/world/2010/apr/21/ukraine-black-sea-fleet-russia>" , 12.06.2023.

Hashim, A. S. (2014, December). From Al-Qaida Affiliate to The Rise of Islamic Caliphate: The Evolution of the Islamic State of Iraq and Syria (ISIS). *S. Rajaratnam School of International Studies (2014)*, 1-16.

Hashim, A. S. (2019). The Islamic State's Way of War in Iraq and Syria: From its Origins to the Post Caliphate Era. *Perspectives on Terrorism*, 13(1), 22-31.

Hénin, N. (2015, November 16). I was held hostage by Isis. They fear our unity more than our airstrikes. *The Guardian*.

Hoffman, F. G. (2009a). Hybrid Warfare and Challenges. *Joint Force Quarterly*. 34-39.

Hoffman, F. G. (2009b). Hybrid vs. compound war. The Janus choice: Defining today's multifaceted conflict. *Armed Forces Journal*.

Hoffman, F. G. (2009c). Further Thoughts on Hybrid Threats. *Small Wars Journal*. Retrieved December 18, 2020, from "<https://smallwarsjournal.com/jrnl/art/further-thoughts-on-hybrid-threats>" , 12.06.2023.

Hoffman, F. G. (2010). 'Hybrid Threats': Neither Omnipotent Nor Unbeatable. *Orbis*. 54(3): 441-455.

Hoffman, F. G. (December 2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, Virginia: Potomac Institute for Policy Studies.

Horbulin, V. (2017). *The World Hybrid War: Ukrainian Forefront*. (J. Lugovska, A. Krapivnik and R. Shultz, Trans.) Kharkiv: National Institute for Strategic Studies Ukrainian Institute for the Future.

Horvath, R. (2015). The Euromaidan and the crisis of Russian nationalism. *The Journal of Nationalism and Ethnicity*, 1-21.

Hybrid threats as a concept. (n.d.). Retrieved 12 3, 2020, from Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats: "<https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>", 12.06.2023.

Iraq: Feared ISIS Use of 'Human Shields,' Executions. (2016, November 4). Retrieved December 2023, from Human Rights Watch: <https://www.hrw.org/news/2016/11/04/iraq-feared-isis-use-human-shields-executions>, 12.06.2023.

ISIS-allied hackers claim worrying new attack. (2015, April 9). *CBS News*. Retrieved June 7, 2021, from <https://www.cbsnews.com/news/french-tv-network-tv5-monde-hacked-by-cybercaliphate-in-name-of-isis/>, 12.06.2023.

Jacobs, A. and Lasconjarias, G. (2015). *NATO's Hybrid Flanks - Handling Unconventional Warfare in the South and the East*. Rome: NDC Public Affairs Office.

Jasper, S. and Moreland, S. (2016, October 23). ISIS: An Adaptive Hybrid Threat in Transition. *Small Wars Journal*.

Johnson, R. (2017). The Evolution of Hybrid Threats Through History. In Y. Özel

and E. İnaltekin, *Shifting Paradigm of War: Hybrid Warfare* (pp. 1-9). İstanbul, Yenilevent: Turkish National Defense University Printing House.

Johnson, R. (2018). Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies*. 29(1): 141-163.

Kappeler, A. (2014). Ukraine and Russia: Legacies of the imperial past and competing memories. *Journal of Eurasian Studies*: 107-115.

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

Kasapoglu, C. (2015). (Rep.). NATO Defense College. Retrieved December 9, 2020, from "<http://www.jstor.org/stable/resrep10269>", 12.06.2023.

Katz, B., G. Jones, S., Doxsee, C. and Harrington, N. H. (2020, September). The Expansion of Russian Private Military Companies.

Kılıçoğlu, M. E. (2022). Russia's Military Preparations in the Region Leading to Russo-Ukrainian War of 2022. *Dergi Park*, 6(2), 383-418.

Kilcullen, D. (2013). *Out of the Mountains: The Coming Age of the Urban Guerrilla*. New York: Oxford University Press.

Kilinskas, K. (2016). Hybrid Warfare: an Orientating or Misleading Concept in Analysing Russia's Military Actions in Ukraine? *Lithuanian Annual Strategic Review*, 14: 139-158.

Lawrence, P. (2022, December). Russia's War in Ukraine: State Patriotism or Economic Gain? *Journal of Global Faultlines*, 9(2), 198-211.

Levallois, A., Cousseran, J.-C. and Kerrello, L. (2017). *The financing of the 'Islamic State' in Iraq and Syria (ISIS)*. the European Parliament, Policy Department. Belgium : Directorate-General for External Policies .

Lewis, J. D. (2014). *The Islamic State: Counter Strategy for a Counter-State* . Washington : Institute for the Study of War.

Liang, Q. and Xiangsui, W. (1999). *Unrestricted warfare*. PLA Literature and Arts Publishing House Arts Beijing.

Lohmus, E. H. (2023). The Role of the Wagner Group in the Russo-Ukrainian War.

Lowe, K. (2012). Hybrid War in Vietnam. In W. Murray and P. R. Mansoor, *Hybrid Warfare Fighting Complex Opponents from the Ancient World to the Present*. New York: Cambridge University Press.

LSE IDEAS, L. S. (2017). *Global Strategies Hybrid Warfare in the Middle East*. London: London School of Economy.

Luhn, A. (2014, August 4). Russia holds huge military exercises near Ukraine border. *The Guardian* .

Lushenko, P. and Williams, A. (2016). Defeating the Islamic State: Reconciling Pressure and Precision High Value Targeting. *Counter Terrorist Trends and Analyses*, 8(9), 10-15.

Mabon, S. and Royle, S. (2017). *The Origins of ISIS: The Collapse of Nations and Revolution in the Middle East*. London: I.B.Tauris & Co. Ltd.

Mahzam, R. (2017). Jihadist Propaganda & Information Warfare in Cyberspace. *Counter Terrorist Trends and Analyses*, 9(3), 8-14.

Majumdar, D. (2015, September 15). Russia's Lethal T-90 Tank vs. ISIS' Captured M1 Abrams: Who Wins? *The National Interest* .

Mansoor, P. R. (2012). Introduction: Hybrid Warfare in History. In P. R. Mansoor and W. Murray, *Hybrid Warfare Fighting Complex Opponents from the Ancient World to the Present* (pp. 3-4). New York: Cambridge University Press.

Maurer, T. (2018). ISIS's Warfare Functions: A Systematized Review of a Proto-state's Conventional Conduct of Combat Operations. *Small Wars & Insurgencies*, 29(2), 229-244.

May, L. (2007). *War Crimes and Just War*. Washington: Cambridge University Press.

McCarthy, M. C., Moyer, M. A. and Venable, B. H. (2019). *Deterring Russia in the Gray Zone*. Strategic Studies Institute, US Army War College

McCarthy, N. (2019, December 10). *The Rise And Fall Of ISIS*. Retrieved from Statista: <https://www.statista.com/chart/20255/the-rise-and-fall-of-isis/>

McCulloh, T. and Johnson, R. (2013). *Hybrid Warfare*. Florida: Joint Special Operations University Press.

Mearsheimer, J. J. (2014). Why the Ukraine Crisis Is the West's Fault. *Foreign Affairs*: 1-12.

Mejias, U. A. and Vokuev, N. E. (2017). Disinformation and the media: the case of Russia and Ukraine. *Media, Culture & Society*, 39(7), 1027– 1042.

Mölder, H. and Sazonov, V. (2018). Information Warfare as the Hobbesian Concept of Modern Times — The Principles, Techniques, and Tools of Russian Information Operations in the Donbas. *The Journal of Slavic Military Studies*, 31(3): 308-328.

Mueller, B. G., Jensen, B. and Valeriano, B. (2023). Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative Futures. *Center for Strategic and International Studies (CSIS)*, 1-25.

Mulford, J. P. (2016). Non-State Actors in the Russo-Ukrainian War. *Connections*, 15(2): 89-107.

Mumford, A. (2016). *The Role of Counter Terrorism in Hybrid Warfare*. NATO's Centre of Excellence for Defence Against Terrorism (COE DAT).

Murray, W. (2012). The American Revolution: Hybrid War in America's Past. In W. Murray and P. R. Mansoor, *Hybrid warfare : fighting complex opponents from the ancient world to the present* (pp. 72-104). New York: Cambridge University Press.

Müür, K., Pruulmann-Vengerfeldt, P. and Sazonov, V. (2016). Russian Information Campaign Against Ukrainian State and Defence Forces. 1-130. (V. Sazonov, K. Müür and H. Mölde, Compilers) Latvia: The NATO StratCom Centre of Excellence.

NATO. (2016, July 09). Retrieved from Warsaw Summit Communiqué: "https://www.nato.int/cps/en/natohq/official_texts_133169.htm"

NATO. (2016, July 9). *Warsaw Summit Communiqué*. NATO: https://www.nato.int/cps/en/natohq/official_texts_133169.htm, 12.06.2023.

Nemeth, W. J. (2002). *Future war and Chechnya: A case for hybrid warfare*. Unpublished PhD Thesis. California: Naval Postgraduate School.

Newnham, R. E. (2018, July). Russia vs the West: The Economic Battle for Ukraine. *Journal of Ukrainian Politics and Society*, 1-26.

News, N. (2015, February 15). ISIS By the Numbers: Foreign Fighter Total Keeps Growing. *NBC News* .

O'Loughlin, J., Toal, G. and Kolosov, V. (2017). The rise and fall of “Novorossiia”: examining support for a separatist geopolitical imaginary in southeast Ukraine. *Post-Soviet Affairs*, 33(2): 124-144.

Ozawa, M. and Iftimie, I. A. (2020). *Russia's energy policy*. Roma : NATO Defense College.

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

Parker, G. (2005). Cambridge Savaş Tarihi. (F. Tayanç and T. Tayanç, Trans.) İstanbul: Türkiye İş Bankası Kültür Yayınları.

Parkes, R. (2019). *Protecting Europe: The EU's response to hybrid threats* (Rep.) (Fiott D., Ed.). European Union Institute for Security Studies (EUISS).

Pawlak, P. and Petkova, G. (January). State-sponsored hackers: hybrid armies? European Union Institute for Security Studies.

Pearce, J. C. (2019). “Hybrid” and “Information”: New Labels, Old Politics. In O. Fridman, V. Kabernik and J. C. Pearce (Eds.), *Hybrid Conflicts and Information Warfare : New Labels, Old Politics* (pp. 249-257). Colorado: Lynne Rienner Publishers Inc.

Piotrowski, M. A. (2015). Hezbollah: The Model of a Hybrid Threat. *The Polish Institute of International Affairs* .

Pomerantsev, P. (2014). How Putin Is Reinventing Warfare. *Foreign Policy*.
"<https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/>"

Rácz, A. (2015). *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. Helsinki : The Finnish Institute of International Affairs.

Rácz, A. (2015). *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. Helsinki : The Finnish Institute of International Affairs.

Ratsiborynska, V. (2016). When Hybrid Warfare Supports Ideology: Russia Today. *NATO Defense College*, 133: 1-20.

Reeves, S. and Wallace, D. A. (2015). The Combatant Status of the 'Little Green Men' and Other Participants in the Ukraine Conflict. *International Law Studies*. 91: 361.

Reichborn-Kjennerud, E. and Cullen, P. (2016). What is Hybrid Warfare. *Norwegian Institute for International Affairs (NUPI)*.

Reinares, F. (2016). *Al-Qaeda's Revenge: The 2004 Madrid Train Bombings*. Washington, DC: Woodrow Wilson Center Press.

Reisinger, H. and Golts, A. (2014). Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence. *NATO Defense College*: 1-12.

Reisinger, H. and Golts, A. (2014). *Russia's Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defence*. NATO Defence College .

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics*. 22(3): 283–300.

Renz, B. and Smith, H. (2016). Russia and Hybrid Warfare - Going Beyond the Label . *Aleksanteri Papers*, 1-52.

Renz, B. and Smith, H. (2016). Russia and Hybrid Warfare - Going Beyond the Label. *Aleksanteri Papers*.

Renz, B. and Smith, H. (2016). Russia and Hybrid Warfare: Going Beyond the Label. Helsinki : Aleksanteri Institute.

Rumsfeld, D. (2005). *The National Defense Strategy of the United States of America*. Washington DC: Department of Defense.

Russia - Countries & Regions -IEA. (2023). Retrieved December 2023 , from International Energy Agecy: <https://www.iea.org/countries/russia>, 12.06.2023.

Rühle, M. (2019). (Rep.). NATO Defense College.

Sackur, S. (2011, September 7). *2004: Madrid train attacks*. Retrieved February 2023, from BBC News: <https://www.bbc.com/news/av/world-europe-14666717>, 12.06.2023.

Salihi, E. and Göksun, Y. (2018). *DEAŞ'ın Medya Stratejisi*. İstanbul: SETA.

Sazonov, V. and Müür, K. (2016). Russian Information Warfare against Ukraine I: Online News and Social Media Analysis. Russian Information Campaign Against Ukrainian State and Defence Forces. Latvia: The NATO StratCom Centre of Excellence.

Schmidt, C. K. (2020, July 6). Evaluating Russia's Grand Strategy in Ukraine. Retrieved from E-International Relations: <https://www.e-ir.info/2020/07/06/evaluating-russias-grand-strategy-in-ukraine/>

Schnauffer, T. A. (2017). Redefining Hybrid Warfare: Russia's Non-linear War against the West. *Journal of Strategic Security*. 10(1): 17-31.

Schoen, T. and Krijger, A. (2019). EU: Between an American rock and a Russian hard place. *Atlantisch Perspectief*, 43(1): 26-30.

Schroefl, J. and Kaufman, S. J. (2014). Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War. *Studies in Conflict & Terrorism*. 37: 862–880.

Seifert, K. R. and McCauley, C. R. (n.d.).

Sinnreich, R. H. (2012). That Accursed Spanish War: The Peninsular War, 1807-1814. In W. Murray and P. R. Mansoor, *Hybrid warfare : fighting complex opponents from the ancient world to the present* (pp. 104-151). New York: Cambridge University Press.

Smith, H. (2019). *NATO and the EU: The essential partners* (Rep.) (Lindstrom G. & Tardy T., Eds.). NATO Defense College.

Snegovaya, M. (2015). Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare. Institute for the Study of War.

Spence, J. and Geroux, J. (2021, September 15). *Urban Warfare Project*. Retrieved December 2023, from Modern War Institute: <https://mwi.westpoint.edu/urban-warfare-project-case-study-2-battle-of-mosul/>, 12.06.2023.

Stanford University. (2021, April). Retrieved from Center for International Security and Cooperation : <https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state>, 12.06.2023.

Stavridis, J. (2016, December). *Maritime Hybrid Warfare is Coming*. Retrieved December 14, 2020, from U.S. Naval Institute Proceedings: "<https://www.usni.org/magazines/proceedings/2016/december/maritime-hybrid-warfare-coming>", 12.06.2023.

Stoker, D. and Whiteside, C. (2020). "Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking," *Naval War College Review*: 73(1), Article 4. Available at: "<https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/4>", 12.06.2023.

Svetoka, S. (2016). *Social Media as A Tool of Hybrid Warfare*. Riga: NATO Strategic Communication Centre of Excellence.

Tadjdeh, Y. (2014, August 28). Islamic State Militants in Syria Now Have Drone Capabilities. *National Defense Magazine* .

Thornton, R. (2015). The Changing Nature of Modern Warfare. *The RUSI Journal*. 160(4): 40-48.

Toal, G. (2017). *Near Abroad: Putin, the West, and the Contest over Ukraine and the Caucasus*. New York: Oxford University Press.

Tonkuş, S. and Sağlam, B. (2014, July 5). IŞİD "enerji" depoluyor . *Anadolu Ajansı*.

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K. and McCue, M. (2018). *Addressing Hybrid Threats*. Swedish Defence University.

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K. and McCue, M. (2018). *Addressing Hybrid Threats*. Swedish Defence University.

Troy, J. (2020). The containment of the Islamic State: A realist case to engage a hybrid actor. *Contemporary Security Policy*, 41(3), 385-406.

Tzu, S. (2009). *The Art of War*. (L. Giles, Trans.) Pax Librorum Publishing House.

Ukraine Import Partner Share from Russian Federation in Percentage 2012-2018. (n.d.). Retrieved April 21, 2021, from World Integrated Trade Solution: "<https://wits.worldbank.org/CountryProfile/en/Country/UKR/StartYear/2012/EndYear/2018/TradeFlow/Import/Partner/RUS/Indicator/MPRT-PRTNR-SHR>" , 12.06.2023.

Ulu, H. (2019). Doktrinden Pratiğe Rusya'nın Hibrit Savaşı Ukrayna ve Suriye örnekleri (Master's Degree). Necmettin Erbakan Üniversitesi.

Vandiver, J. (2014, September 4). SACEUR: Allies Must Prepare for 'Hybrid Warfare'. Stars and Stripes. Retrieved April 8, 2021, from "<https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464>" , 12.06.2023.

Veljovski, G., Taneski, N. and Dojchinovski, M. (2017). The danger of “hybrid warfare” from a sophisticated adversary: the Russian “hybridity” in the Ukrainian conflict. *Defence & Security Analysis*: 33(4), 292-307.

Votel, J. L., Bembenek, C., Hans, C., Mouton, J. and Spencer, A. (2017). *Virtual caliphate: Defeating ISIL on the physical battlefield is not enough*. Washington : Centre for a New American Century.

Walker, S. (2015, April 2). The Russian troll factory at the heart of the meddling allegations. *The Guardian* .

Waltz, E. (1998). *Information Warfare Principles and Operations*. London: Artech House.

Warrick, J. (2015). *Black Flags: The Rise of ISIS*. New York: Doubleday.

Warrick, J. (2022, July 11). ISIS planned chemical attacks in Europe, new details on weapons program reveal. *The Washington Post* .

Weiss, M. and Hassan, H. (2015). *ISIS: Inside the Army of Terror* . New York : Regan Arts.

Weissmann, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security*. 5(1): 17-26.

Welch, T. (2018). Theology, heroism, justice, and fear: an analysis of ISIS propaganda magazines Dabiq and Rumiyah. *Dynamics of Asymmetric Conflict*, 11(3), 186-198.

Whiteside, C. (2016). New Masters of Revolutionary Warfare: The Islamic State Movement (2002-2016). *Perspectives on Terrorism*, 10(4), 4-18.

Wierzbowska-Miazga, A. and Sarna, A. (2014, March 6). Russian economic pressure on Ukraine. Retrieved April 22, 2021, from Centre for Eastern Studies: "<https://www.osw.waw.pl/en/publikacje/analyses/2014-03-26/russian-economic-pressure-ukraine>", 12.06.2023.

Williams, P. and Picarelli, J. (2002). Organized Crime in Ukraine: Challenge and Response. National Criminal Justice Reference Service.

Wills, M. (2019). *Chinese Dominance in the South China Sea: An Effective Use of Hybrid Warfare(JCSP 44–PCEMI 44)*. Toronto, ON: Canadian Forces College.

Wither, J. K. (2016). Making sense of hybrid warfare. *Connections*. 15(2): 73–87.

Wright, R. (2017). *The Jihadi Threat: ISIS, al-Qaeda, and Beyond*. Wilson Center. United State Institute of Peace.

Yalçinkaya, H. (2017). *IŞİD'in Yabancı Savaşçıları ve Yarattığı Tehdit: Türkiye'nin Tecrübesi (2014-2016)*. Ankara : ORSAM.

Yalçinkaya, H. (2019, November). Savaşın Değişimi ve Kuramsal Tartışmalar. *Güvenlik Yazıları Serisi*, 43.

Yamaguchi, N. (2012). An Unexpected Encounter with Hybrid Warfare: The Japanese Experience in North China, 1937–1945. In W. Murray and P. R. Mansoor, *Hybrid Warfare Fighting Complex Opponents from the Ancient World to the Present*. New York: Cambridge University Press.

Yarchi, M. (2019). ISIS's media strategy as image warfare: Strategic messaging over time and across platforms. *Communication and the Public*, 4(1), 53-67.

Yıldız, G. (2017). How Postmodern is Hybrid Warfare: Revisiting the Modern Euroasian Military History. In Y. Özel and E. İnaltekin(Eds.), *Shifting Paradigm of War: Hybrid Warfare*. İstanbul: Turkish National Defense University Printing House.

Zimmer, K. (2005, April 12). What Happened to 'Unity, Consent and Revival?' The Donetsk Clan before and after the Ukrainian Presidential Elections. Retrieved from Wilson Center: <https://www.wilsoncenter.org/event/what-happened-to-unity-consent-and-revival-the-donetsk-clan-and-after-the-ukrainian>, 12.06.2023.

‘Little green men’ or ‘Russian invaders’? (2014, March 11). *BBC*.

(2014). *Threat Tactic Reports: Islamic State of Iraq and the Levant*. TRISA; CTID.

