NEVŞEHİR
HACI BEKTAŞ VELİ
ÜNİVERSİTESİ
Ara, bul.

Sosyal Bilimler Enstitüsü Dergisi
Cilt: 15 Sayı: 3 Eylül 2025
E-ISSN: 2149-3871

HYBRID WAR: INTERNATIONAL SECURITY AT THE INTERSECTION OF TRADITIONAL AND MODERN WARFARE

HİBRİT SAVAŞ: GELENEKSEL VE MODERN SAVAŞIN KESİŞİM NOKTASINDA ULUSLARARASI GÜVENLİK

Şeref ÇETİNKAYA
İstanbul Üniversitesi, Türkiyat Araştırmaları Enstitüsü,
Avrasya Araştırmaları ABD,
seref.cetinkaya@istanbul.edu.tr
ORCID: 0000-0002-6446-2322

Geliş Tarihi:
13.04.2025

Kabul Tarihi:
24.09.2025

Yayın Tarihi:
28.09.2025

Anahtar Kelimeler
Hibrit Savaş,
Güvenlik,
Uluslararası Güvenlik,
Geleneksel Savaş,
Modern Savaş

Keywords
Hybrid Warfare,
Security,
International Security,
Traditional Warfare,
Modern Warfare

ABSTRACT

Hybrid warfare is a multifaceted and dynamic form of conflict that employs a combination of both traditional and modern warfare methods. This type of warfare is not limited to wars between states, but can also be waged by non-state actors, terrorist organisations and cyberattackers. By integrating traditional military confrontations with the technological and asymmetric elements of modern warfare, the scope of hybrid warfare expands, resulting in a more complex threat structure. This paper aims to analyze the impacts of hybrid warfare on international security. It examines how hybrid warfare integrates traditional military strategies with modern components such as cyberattacks, disinformation campaigns, and economic sanctions, and what consequences this has for international security organizations, states, and non-state actors. Special attention is given to the positions of international security organizations like NATO and the EU in the face of hybrid warfare, and how hybrid warfare may shape the future security architecture. As hybrid warfare introduces new security threats into the contemporary conflict environment, the paper also discusses what measures states and international organizations can take to counter these threats. Ultimately, it concludes that hybrid warfare affects global power balances and could lead to transformations in international security and international relations.

ÖZ

Hibrit savaş, hem geleneksel hem de modern savaş yöntemlerinin bir arada kullanıldığı, çok boyutlu ve dinamik bir çatışma biçimidir. Bu savaş türü, yalnızca devletler arası savaşlarla sınırlı kalmayıp, devlet dışı aktörler, terör örgütleri ve siber saldırganlar tarafından da uygulanabilmektedir. Geleneksel savaşın cephe çatışmaları, modern savaşın teknolojik ve asimetrik unsurlarıyla birleştirilerek, hibrit savaşın kapsamı genişlemekte ve daha karmaşık bir tehdit yapısı ortaya çıkmaktadır. Bu makale, hibrit savaşın uluslararası güvenlik üzerindeki etkilerini analiz etmeyi amaçlamaktadır. Hibrit savaşın, geleneksel askeri stratejiler ile modern siber saldırılar, dezenformasyon kampanyaları ve ekonomik yaptırımlar gibi unsurları nasıl entegre ettiği, uluslararası güvenlik örgütleri, devletler ve devlet dışı aktörler üzerinde ne tür sonuçlar doğurduğu kapsamlı bir şekilde ele alınmıştır. Özellikle NATO ve AB gibi uluslararası güvenlik örgütlerinin hibrit savaş karşısındaki durumu ve hibrit savaşın gelecekteki güvenlik mimarisini nasıl şekillendirebileceği üzerinde durulmuştur. Hibrit savaş, günümüz çatışma ortamında yeni güvenlik tehditleri doğururken, devletlerin ve uluslararası örgütlerin bu tehditlere karşı ne tür önlemler alabileceği de bu çalışmada tartışılmaktadır. Buna göre hibrit savaşın, küresel güç dengelerini etkilediği, uluslararası güvenlik ve uluslararası ilişkilerde dönüşüme neden olabileceği sonucuna varılmıştır.

DOI: https://doi.org/10.30783/nevsosbilen.1675508
Atıf/Cite as: Çetinkaya, Ş. (2025). Hybrid War: International security at the intersection of traditional and modern warfare. *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi, 15*(3), 1920-1934.

Introduction

Hybrid warfare has emerged as one of the most complex and multidimensional security threats of the 21st century. As a form of conflict that combines traditional military operations with modern tactics and technologies, hybrid warfare has exerted significant effects on international relations and security strategies. This type of warfare is not limited to engagements between states; it is also employed by non-state actors (e.g. terrorist organizations), and also cyber aggressors. In this context, hybrid warfare occupies the intersection of traditional and modern forms of warfare, generating both new challenges and opportunities for the global security architecture. One of the secondary objectives of this study is to identify and analyze these challenges and opportunities.

The primary aim of this article is to explore the relationship between traditional and modern warfare, and to analyze their convergence under the concept of hybrid warfare, with particular attention to its implications for international security. This study offers a comprehensive examination of how hybrid warfare integrates traditional military strategies with technological and information-based tactics, the consequences of this fusion for international security organizations, states, and non-state actors, and how these dynamics might shape future security environments.

Hybrid warfare appears to be a concept that reflects fundamental changes in the nature of modern conflicts. By transcending the boundaries of classical security paradigms, it has prompted a major shift in global security policies. Understanding the nature of hybrid warfare is of vital importance for states and international organizations to develop more effective strategies against asymmetric threats. Elements such as Cyberattacks, disinformation campaigns and economic sanctions pose significant threats not only in the military sphere, but also in the economic, political and social spheres. Therefore, academic research on hybrid warfare contributes to the reshaping of international security policies and strengthens the preparedness of states to confront such threats.

In this article, the concepts of traditional and modern warfare are examined in a comparative framework, alongside the hybrid warfare model. The first section discusses traditional warfare through the lens of interstate wars, the laws of armed conflict, and the role of conventional weaponry. Modern warfare, in contrast, is analyzed in relation to cyberattacks, information warfare, and technological innovations. Subsequent sections focus on how hybrid warfare synthesizes these two forms of conflict, creating complex and multifaceted threats. Additionally, the article investigates the implications of hybrid warfare for international security, especially in relation to major security institutions such as NATO and the EU. Finally, the components of hybrid warfare and its potential impacts on the future international security architecture are discussed. This evaluation is based on a thorough literature review and document analysis, employing a qualitative research design.

By existing at the intersection of traditional and modern warfare, hybrid warfare has created a new paradigm in international security. This article seeks to explore the historical roots, core components, and security implications of hybrid warfare comprehensively. Understanding hybrid warfare will assist in the development of more effective responses to future security threats and contribute to the formulation of more efficient strategies in international relations. The analyses presented throughout the article aim to illuminate the transformations caused by hybrid warfare and foster a deeper understanding of its long-term impact on international security.

Traditional and Modern Concepts of Warfare and Their Transformation

The concept of war occupies an interdisciplinary domain and therefore encompasses numerous definitions. The Roman statesman Cicero defined war as an instrument for achieving peace and justice. According to Cicero, there must be a just cause to wage war, and the ultimate objective should be the restoration of peace. In this way, a war may be waged justly, and the victor may achieve an honorable triumph (Ören, 2022, p. 188). Similarly, the ancient Greek historian Thucydides emphasized necessity in his definition of war. He argued that the Peloponnesian War was inevitable due to Sparta's perceived threat from the growing power of Athens. Thus, the fear instilled in Sparta by Athens' rise made war unavoidable (Gilpin, 2020, p. 425). Thucydides developed a notion of human nature to explain behavior during crises such as war, plague, and massacre, positing that fear and self-interest underlie both individual political behavior and relations between states (Zagorin, 2008). Hugo

Grotius, on the other hand, defined war as a condition wherein parties seek to resolve disputes through the use of force (Grotius, 2011, p. 17).

Carl von Clausewitz, in his seminal work *On War* (1832), attempted to answer the question of what war entails, drawing on the consequences of the Napoleonic Wars. He identified three essential criteria for an act of aggression to be considered war: violence, instrumentality, and political purpose (Rid, 2012). According to Clausewitz, war is an act of force intended to compel the enemy to submit to one's will, thus inherently violent in nature. Secondly, war possesses an instrumental character—its purpose is political, and war serves as a means to achieve that end. Lastly, war must be driven by a political objective. Using these criteria, Clausewitz sought to develop a theory capable of explaining the multifaceted and evolving nature of war—what he called its "chameleon-like" character. Clausewitz's theories remain foundational Western military thought and are closely associated with the concept of traditional warfare (Andersen, 2012; Wilkie, 2009).

Traditional warfare is generally understood as warfare between nation-states, characterized by conflicts between national armies within defined territorial boundaries. Its defining features include the use of conventional weapons, formal armies, and open battlefield engagements. States utilize military force to protect or expand their territorial sovereignty, and such wars typically occur between two or more states within a specific geographical area (Creveld, 1991). According to Weigley, traditional warfare is marked by intense firepower, state-centric organization, industrial capacity, and formal military structures (Weigley, 1977, p. 280).

Traditional warfare is also constrained by a set of legal norms. Laws of war and international humanitarian law prescribe rules of engagement for warring parties. The Geneva Conventions, for instance, aim to ensure the protection of civilians during armed conflict (Henckaerts & Doswald-Beck, 2005). Thus, traditional warfare adheres to specific legal and ethical standards and emphasizes the maintenance of sovereignty within international relations.

The study of war through a traditional lens dominated scholarly discourse until the end of the Cold War, a period strongly influenced by realist theory. Within this framework, concepts such as military power and state-centric security were prioritized. However, the end of the Cold War—along with globalization and technological developments—prompted significant changes in security and warfare studies. During this time, critiques of the traditional understanding of war emerged, challenging its relevance in the face of contemporary threats (Gök, 2021, p. 19). Notably, a study by Lind et al. in 1989 introduced a distinction between traditional and new wars, highlighting that warfare could transcend geographic boundaries, blur the lines between civilians and combatants, and render the distinction between wartime and peacetime increasingly ambiguous (Lind et al., 1989, pp. 22-26).

Prominent scholars of new or modern warfare, such as Creveld, Kaldor, and Keegan, have argued that with the end of the Cold War, direct military confrontations between states declined, while insurgencies and internal conflicts involving non-state actors increased. The diversification of both actors and methods prompted these scholars to study warfare from a dual framework: traditional and modern (Gök, 2021, p. 24). According to Kaldor, traditional wars involved formal state armies, whereas modern wars feature a wider array of actors including non-state entities, private military companies, mercenaries, warlords, and paramilitary groups. Furthermore, modern wars differ in terms of economic structures. While traditional wars were financed through state taxation and borrowing, modern war economies are deeply embedded in the globalized economic system (Kaldor, 2013, pp. 2–3).

Modern warfare thus transcends the parameters of traditional warfare, emphasizing technological advances, information warfare, and cyber operations. Since the mid-20th century, military strategies have been reshaped by innovations such as nuclear weapons, drones, and cyberwarfare—now considered defining characteristics of modern conflicts (Arquilla & Ronfeldt, 1993).

The role of non-state actors and asymmetric threats has also increased in modern warfare. Terrorist organizations and mercenaries complicate the dynamics of conflict beyond state-centric paradigms. Modern warfare (similar to many traditional wars) often includes information operations and psychological warfare, targeting societal morale and fostering internal polarization (Rid, 2012). As a result, modern warfare encompasses a much broader strategic spectrum than traditional warfare.

Moreover, modern warfare incorporates elements such as cyberattacks, which target state infrastructure, and information warfare designed to manipulate public opinion (Kott et al., 2015). Armed forces today are no longer focused solely on physical battles but must also contend with cybersecurity, economic manipulation, and disinformation (Smith, 2008). For example, cyberattacks are now capable of crippling critical state infrastructure, as seen in the 2007 Estonian cyberattack, which disrupted government operations and financial systems. Similarly, information warfare has evolved with the rise of social media, enabling the rapid spread of disinformation to shape public opinion on a global scale. These developments signify a fundamental shift in the nature of warfare—towards a model increasingly reliant on technology and knowledge-based operations.

The Emergence of Hybrid Warfare: The Fusion of Traditional and Modern Approaches

The concept of hybrid warfare was first introduced in a 2002 master's thesis written in the United States. Major William J. Nemeth of the U.S. Army examined the Chechen War and argued that traditional tactics had merged with modern science and technology to form a new type of warfare, thereby emphasizing the evolving nature of conflict (Gök, 2021, p. 32).

Hybrid warfare represents a multidimensional and dynamic form of conflict in which modern warfare methods are integrated with traditional approaches. This form of warfare spans a wide spectrum, including not only conventional military confrontations but also cyberattacks, disinformation campaigns, economic coercion, and the use of proxy forces (Hoffman, 2009). While traditional warfare relies on open, state-versus-state battles, hybrid warfare transcends this framework, incorporating covert operations, non-state actors, and asymmetric tactics (Murray & Mansoor, 2012). This situation has become more pronounced in the post-Cold War era, in regional conflicts and counter-terrorism operations, and has significantly expanded its sphere of influence today.

The evolution of communication technologies in the 21st century has further shaped the character of hybrid warfare. A prominent example is the 2006 Lebanon War, during which Hezbollah combined conventional and asymmetric tactics in its fight against Israel (Hoffman, 2007; Biddle & Friedman, 2008). Hezbollah constructed complex tunnel networks and bunkers that played a key role in disabling Israeli armored vehicles and tanks (Johnson, 2012, p. 20). Strategic terrain was identified and captured for defensive advantage, and intense combat ensued in these areas (Kaplan, 2023, p. 399). Simultaneously, Hezbollah disseminated images of civilian casualties from Israeli airstrikes through both social and traditional media to shape international public opinion. By portraying Israel as using disproportionate force, Hezbollah gained an asymmetric advantage in the global information space (Kalb & Saivetz, 2007, p. 46). Despite losses on both sides, the conflict was widely perceived in the region as a military failure for Israel (Kahraman, 2019, p. 147). This case clearly demonstrated the effectiveness of hybrid tactics employed by non-state actors.

The rise of hybrid warfare is closely linked to the necessity of modernizing certain aspects of traditional warfare. Both states and non-state actors have leveraged technological advancements to extend the battlefield beyond conventional parameters. Hybrid strategies target not only physical battlegrounds but also internal societal dynamics. Media manipulation and disinformation campaigns, for example, aim to fragment societies and weaken public resilience (Waltz, 2018).

Another distinctive feature of hybrid warfare is its emphasis on ambiguity and psychological disruption. By blurring the boundaries of traditional conflict, it aims to outmaneuver conventional defense mechanisms. Hybrid warfare combines military operations, cyberattacks, and disinformation within a unified strategic framework, thereby increasing the complexity of the conflict environment (Mumford, 2013). This synthesis contributes to the transformation of hybrid warfare into a highly adaptive and multi-layered threat that surpasses the limits of both traditional and modern forms of warfare. In order to counter such threats effectively, states must develop capacities not only in conventional military domains but also in cybersecurity, strategic communication, and economic resilience (Johnson, 2018).

One of the factors that makes hybrid warfare particularly intricate is its simultaneous use of multiple domains of conflict. For instance, Russia's 2014 annexation of Crimea was carried out through a combination of military force, cyber operations, media manipulation, and diplomatic pressure. This demonstrated that hybrid warfare can be waged effectively in both physical and virtual arenas (Galeotti, 2016). After all, while military force, diplomatic pressure, and media manipulation are not entirely new to warfare, the way they are integrated today with modern technologies like cyber operations is what makes hybrid warfare so complex. In the past, these tools were used separately or in isolation, but now they work in tandem, amplifying each other's impact. During the 2014 Ukraine crisis, Timothy Thomas observed that Russia deployed its information operations effectively across both social and traditional media. As part of its deception efforts, internet trolls and other cognitive tools were used to conduct psychological operations aimed at confusing and delaying enemy decision-making. Additionally, Russia initially denied its military presence in Crimea, spreading conspiracy theories to shape both domestic and international perceptions (Kaplan, 2023, pp. 406–407).

In sum, hybrid warfare—through its combination of traditional and modern strategies—has emerged as a central phenomenon in contemporary international security. Its strategic framework encompasses not only military power but also the domains of information, economics, and diplomacy, thus creating a broader and more complex threat landscape.

Components of Hybrid Warfare

Hybrid warfare brings together the elements of traditional and modern warfare, creating a multidimensional battlefield and a complex security threat perception. Its primary objective (similar to traditional warfare) is to weaken the target state by simultaneously employing military, cyber/informational, and economic tools. In this context, it is appropriate to briefly examine the three core components of hybrid warfare.

Military Elements: Conventional Forces, Special Units, and Proxy Actors

The military dimension of hybrid warfare is characterized by the coordinated use of conventional armed forces, special operations units, and proxy actors. Regular armies are often deployed in a limited and selective manner, allowing states to avoid direct military engagement and thereby providing strategic flexibility. As traditional military involvement is scaled back and special forces come to the forefront, the conflict assumes an asymmetric character, becoming more complex and ambiguous for the target state (Galeotti, 2016).

Special forces and proxy groups are typically employed in low-intensity conflicts and covert operations. These actors enable states to achieve military objectives without overt deployment of their national forces. For instance, during the Syrian civil war, various states chose to support proxy groups instead of directly involving their own armed forces in the conflict (Mumford, 2013). Such military components also serve the strategic goal of plausible deniability, enabling states to evade legal responsibility and public accountability.

The use of proxy forces amplifies the asymmetric nature of hybrid warfare and complicates the legal assessment of conflict under international law. By circumventing formal declarations of war and direct engagements, states are able to intervene in foreign conflicts through indirect means, thereby challenging the traditional norms of sovereignty and accountability (Hoffman, 2007). Accordingly, the military tools of hybrid warfare enable strategic gains without triggering formal interstate war.

In short, although special forces are part of traditional warfare, their prominence in hybrid warfare stems from their ability to conduct less visible and more targeted operations. In traditional warfare, special forces play a more limited role, but in hybrid warfare, these forces are used in a wider range of activities, such as cyberattacks, intelligence gathering, intervention in local conflicts, and cooperation with proxy forces.

Cyber and Information Elements: Cyberattacks, Disinformation Campaigns, and Media Manipulation

Among the most defining features of hybrid warfare are cyber operations and information warfare. Cyberattacks target critical information infrastructure and aim to disrupt communication channels and strategic decision-making processes. Today, cyberwarfare has become an indispensable element of hybrid strategies, with states increasingly developing the capability to damage, steal, or manipulate digital assets belonging to rival actors (Rid, 2012). A well-known example is the series of cyberattacks carried out against Estonia in 2007, which serve as a notable case of hybrid cyber aggression (Tikk, Kaska & Vihul, 2010). Although Estonia held Russia responsible for these attacks, Russia has never accepted these allegations.

Disinformation campaigns and media manipulation are used to shape public perception and manage popular sentiment. These tactics are especially effective when deployed via social media platforms, where they aim to incite distrust, deepen polarization, and generate chaos within the target society (Jowett & O'Donnell, 2015). For example, the widespread claims regarding Russia's interference in the 2016 U.S. Presidential Election highlight the potential of disinformation campaigns to influence democratic processes (Bennett & Livingston, 2020).

Media manipulation has significant psychological effects, going beyond traditional battlefield operations by undermining societal trust and destabilizing internal political orders. These manipulative strategies exploit the ambiguity of hybrid warfare, seeking to demoralize adversaries and provoke public confusion. As such, information and cyber components lie at the heart of hybrid warfare, and are now considered fundamental to modern strategic planning (Miskimmon, O'Loughlin & Roselle, 2013).

Economic Elements: Sanctions, Energy Leverage, and Trade Wars

The economic dimension of hybrid warfare involves the use of financial instruments to achieve strategic objectives without resorting to conventional force. Economic sanctions are one of the most commonly used tools, designed to weaken the target state's economy and isolate it from the international arena. Through sanctions, states can compel behavioral changes in adversaries without engaging in direct military confrontation (Pape, 1997).

Energy leverage is another critical economic tactic. States may manipulate the supply of energy resources to pressure target states, threaten their energy security, and extract political concessions. Russia's use of gas supply disruptions as leverage against Ukraine is a prominent example of hybrid energy coercion (Goldthau & Sitter, 2015; Pirani, 2007).

Trade wars also represent an important economic element within hybrid warfare strategies. By disrupting the economic interests of rival states, countries aim to weaken their adversaries' economic resilience and strategic posture. For instance, the ongoing trade conflict between the United States and China illustrates how economic instruments can be used as tools of hybrid confrontation with global consequences (Baldwin, 2020; Irwin, 2017).

The economic tools of hybrid warfare necessitate that states develop security strategies that go beyond traditional military responses. Regardless of whether a state is acting offensively or defensively, failure to integrate economic resilience into national security planning can leave it vulnerable to hybrid threats.

The Impact of Hybrid Warfare on International Security

Hybrid warfare has exposed the limitations of traditional security paradigms, significantly challenging the ability of international security systems to adapt to evolving threat landscapes. Conventional understandings of security tend to focus on inter-state wars and clearly defined threats. However, hybrid warfare transcends these frameworks by combining military and non-military tools in complex and unpredictable ways. As a result, both states and international organizations have often found their existing defense strategies insufficient to counter hybrid threats. Hybrid warfare is a strategy that can be found not only in today's conflicts but also in the past. For example, Russia's annexation of Crimea in 2014 presented an example of conflict that transcended traditional notions of warfare by combining elements such as military force, cyberattacks, media manipulation and diplomatic pressure. However, older conflicts such as the Cold War and terrorism demonstrate early forms of hybrid warfare involving non-state actors and proxy forces. While 9/11 provided important lessons regarding threats from non-state actors, hybrid warfare has revealed a more complex security dynamic shaped not only by terrorism but also by new threats such as cyberattacks and disinformation. Therefore, hybrid warfare requires a more integrated approach that transcends old security concepts and combines traditional and modern threats.

The Inadequacy of Traditional Paradigms and the Emergence of New Security Approaches

Traditional security paradigms largely center on protecting national borders and preserving state sovereignty. In contrast, hybrid warfare reaches beyond these confines by employing economic tools, cyber operations, and information warfare to interfere with the internal affairs of sovereign states. This reveals the inadequacy of relying solely on military force in response to hybrid threats. Rather, hybrid warfare targets systemic vulnerabilities and necessitates the development of comprehensive and integrated approaches (Hoffman, 2007).

Hybrid warfare has also brought significant transformations to regional security dynamics. Particularly in regions such as the Middle East, Eastern Europe, and Southeast Asia, hybrid tactics have reshaped local power balances. In response, states have been compelled to formulate hybrid security doctrines. For instance, Russia's hybrid campaign against Ukraine fundamentally altered the security architecture of Eastern Europe, prompting NATO and the EU to strengthen their regional presence and encouraging countries in the region to reassess their national defense strategies (Galeotti, 2016). In this sense, although NATO's activities under the RAP were initially developed as a response to Russia's traditional military threats, over time they have expanded to include non-traditional threats such as cyberattacks, hybrid warfare and disinformation.

By merging traditional and modern war strategies, hybrid warfare emerges as a multidimensional threat, transforming the nature of the international security environment. Faced with such threats, states and international organizations have been forced to move beyond conventional security frameworks and to develop more flexible and multidimensional security strategies. The complexity of hybrid warfare requires that military, civilian, and technological elements be fused within a single strategic framework.

The inherently multifaceted structure of hybrid warfare compels states to create integrated strategies that incorporate not only military tools but also political, economic, cyber, and information-based components. NATO, for example, has restructured its deterrence and defense doctrines to address hybrid threats, taking concrete steps to enhance the cyber defense capabilities of its member states (NATO, 2015). Likewise, the European Union has developed a comprehensive strategy aimed at strengthening resilience against information warfare and improving cyber defense mechanisms (European Commission, 2016).

Key elements of these strategies include reinforcing cybersecurity, expanding strategic communication capabilities to counter disinformation, and developing efficient crisis management mechanisms. In addition, the asymmetric nature of hybrid threats has emphasized the importance of intelligence sharing and adapting national security doctrines accordingly (Galeotti, 2016).

The concept of hybrid warfare within NATO has largely been discussed in the context of asymmetric threats. The concept of hybrid warfare came to the fore in discussions in NATO's 2010 Strategic Concept, which analysed the Alliance's strategic priorities and global security dynamics and redefined its relationship with external actors. However, the term “hybrid warfare” was not explicitly included in the document. In this document, the evolution of warfare through terrorism and cyberattacks was highlighted (Gök, 2021, p. 38). Following this, NATO, as a traditionally state-centric military alliance, had to reassess its approach in the face of hybrid threats. In response, NATO enhanced its cyber defense capabilities and expanded its strategic communication tools to combat information warfare (NATO, 2015).

Another NATO report emphasized the significance of information as a domain of conflict. Although information has always played a crucial role in warfare, hybrid conflicts have elevated its importance to a critical level, where the manipulation of information can serve to intensify or prolong conflict (NATO, 2016).

The annexation of Crimea by Russia, conflicts in the Middle East, the resulting irregular migration crisis, and the rise in terrorist activity across Europe led the European Union to adopt a series of measures to combat hybrid threats. In this context, the EU published a Joint Communication on April 6, 2016, titled *Joint Framework on Countering Hybrid Threats – A European Union Response*, which emphasized the global transformation of the threat environment (European Commission, 2016). According to the document, developments in the Balkans and Southern Europe posed direct threats to EU security and required stronger EU–NATO coordination (Aytuğ & Pozan, 2023, p. 9). However, although hybrid threats are mentioned in this document, the concept of hybrid warfare is not directly addressed. Member states were urged to plan and rapidly implement measures such as threat assessments, early warning systems, and hybrid risk evaluations.

As part of the EU’s efforts to increase situational awareness, the *EU Hybrid Fusion Cell* was established. This cell provides a platform for representatives of EU member states to analyze and assess shared intelligence data, thus functioning as a central intelligence-processing entity. In parallel, the *European Centre of Excellence for Countering Hybrid Threats* was launched to support EU capacities in cybersecurity, strategic communication, civil-military cooperation, energy security, and crisis response (Aytuğ & Pozan, 2023, p. 10).

During the NATO summit in Warsaw in July 2016, a joint declaration was issued by NATO and the EU outlining seven areas of cooperation: countering hybrid threats, expanding and adapting operational cooperation, strengthening coordination in cyber defense, achieving coherent and interoperable defense capabilities, enhancing the defense industrial base, improving coordination of joint exercises, and increasing the resilience of partner countries (European Council, 2016).

The strategies developed by NATO and the EU to combat hybrid threats extend beyond military measures to include economic sanctions, diplomatic engagement, and advanced cyber defense. However, the multidimensional nature of hybrid warfare complicates the efforts of these organizations to implement fully integrated responses. Consequently, NATO and the EU continue to pursue more holistic and flexible strategies aimed at addressing the complex realities of hybrid conflict (Galeotti, 2016).

Hybrid warfare not only presents strategic and operational challenges but also raises significant legal and ethical questions. By its very nature, hybrid warfare blurs the boundaries of existing legal frameworks. While international legal instruments such as the Geneva Conventions regulate traditional forms of warfare, there is considerable ambiguity about how to address cyberattacks, disinformation campaigns, and economic coercion within these legal constructs (Schmitt, 2017). Such traditional legal instruments, focusing on the protection of civilians during war and armed conflict, do not explicitly regulate disinformation or economic sanctions.

This legal uncertainty creates loopholes that make it more difficult to hold actors accountable and to ensure the protection of civilian populations. For example, cyber operations and information warfare often fall into legal gray zones, where their classification under the laws of armed conflict remains contested (Tikk & Kerttunen, 2018). Moreover, the use of non-state actors in hybrid campaigns further complicates the determination of legal responsibility and challenges the status of these actors under international law (Hoffman, 2007).

From an ethical standpoint, the psychological dimensions of hybrid warfare—such as disinformation and manipulation—can lead to deep societal polarization and erode public trust in democratic institutions. These effects underscore the urgent need for the development of new ethical norms and legal frameworks that can better respond to the novel challenges posed by hybrid threats (Rid, 2012).

The Role of Hybrid Warfare in the Future Architecture of International Security

Hybrid warfare is driving significant changes in the nature of modern conflicts and is increasingly occupying a central role in the global security architecture. While both states and international organizations are striving to develop effective strategies to counter hybrid threats, projections suggest that such threats will become even more pervasive in the future. In this context, it is crucial to discuss the future role of hybrid warfare in shaping global security, the importance of international cooperation, and the corresponding policy recommendations.

The complexity and multidimensionality of hybrid warfare have positioned it as a critical determinant in the configuration of the future international security environment. By transcending the boundaries of traditional military doctrines, hybrid warfare allows both state and non-state actors to engage in conflict using increasingly sophisticated tools and strategies. NATO, recognizing the growing importance of hybrid threats, has expanded its defense and deterrence strategies to include hybrid dimensions (Tardy, 2020). This shift underscores the increasingly pivotal role that hybrid warfare is expected to play in future international security strategies.

One of the most salient areas where hybrid warfare will continue to exert influence is cyber warfare. With the global escalation of cyber threats, states and international organizations are being compelled to enhance their cyber defense capabilities and improve their resilience against cyberattacks (Clarke & Knake, 2011). It is anticipated that the cyber component of hybrid warfare will further alter the global balance of power and significantly impact the dynamics of international relations (Singer & Friedman, 2014).

Hybrid warfare often involves complex threats that a single state may struggle to counter effectively on its own, thereby increasing the importance of international cooperation and coordination. Institutions such as the United Nations (UN) and the European Union (EU) have intensified their collaborative efforts to develop more effective global responses to hybrid threats (European External Action Service, 2018). These cooperative initiatives emphasize the need for increased information sharing, joint exercises, and strategic planning, in order to effectively address the multidimensional nature of hybrid warfare (Bachmann & Gunneriusson, 2015).

Global collaboration also plays a critical role in responding to the asymmetric nature of hybrid threats. In particular, the increasing prominence of cyberattacks and disinformation campaigns necessitates the development of collective defense mechanisms. NATO's *Cooperative Cyber Defence Centre of Excellence* serves as an example of how member states are working to improve resilience against cyber threats (Lindsay, 2013). Similarly, legal and ethical dilemmas posed by hybrid warfare require coordinated international legal responses and standardized regulatory frameworks (Schmitt, 2017).

To mitigate the effects of hybrid warfare on international security and develop effective counterstrategies, several policy recommendations can be proposed. First, enhancing intergovernmental cooperation is vital for the prevention and management of hybrid threats. States should formulate hybrid warfare doctrines at both the regional and global levels, and establish joint defense mechanisms tailored to these challenges (Vershbow & Speranza, 2019). Second, strengthening national cybersecurity infrastructure will be crucial in countering one of the most critical aspects of hybrid warfare. States must integrate cybersecurity into their national security agendas and develop robust defense mechanisms in this domain (Libicki, 2009). In this regard, public-private partnerships should also be encouraged, as the private sector plays an increasingly central role in cybersecurity (Buchanan, 2020).

Third, the capacity for strategic communication must be improved to combat disinformation effectively. This involves not only enhancing cyber defenses but also bolstering the ability of states to resist and respond to information warfare. The international community must collaborate to take swift and coordinated action against disinformation campaigns (Starbird et al., 2019).

In parallel, the evolving nature of hybrid threats calls for a careful reassessment of existing international legal frameworks. Current norms may not adequately cover emerging challenges such as cyberattacks, disinformation campaigns, and economic coercion. Therefore, there is a growing need for states and international institutions to explore and develop regulatory mechanisms that reflect the specific dynamics of hybrid conflict (Schmitt & Vihul, 2017).

Conclusion

Hybrid warfare has fundamentally transformed the dynamics of modern conflict and has exerted a profound influence on global power relations. Hybrid strategies that combine traditional and non-traditional methods – including cyberattacks, information operations, economic sanctions and the use of proxy forces – are adding a new layer of complexity to the international security environment and challenging traditional responses and norms. Hybrid warfare has emerged as a strategy that goes beyond open and direct military conflict, aiming to infiltrate the internal affairs of target states through multi-layered and often covert tactics, thereby shifting in the balance of power.

The evolution of hybrid warfare has revealed the limitations of traditional security paradigms and necessitated a shift toward more adaptive, multidimensional approaches. States must strengthen their military capabilities alongside cyber defence, strategic communications, economic resilience and legal frameworks to counter both conventional and hybrid threats. In this regard, the long-term effects of hybrid warfare on international relations are likely to be far-reaching and enduring. Hybrid strategies are already reshaping international law, diplomacy, and collective security arrangements, laying the groundwork for a new phase in the conduct of global conflict.

The rise of hybrid threats has made the international security environment increasingly volatile and unpredictable. As a result, both states and international organizations are engaged in a continuous process of adaptation. Hybrid warfare has created various challenges for traditional alliances and multilateral cooperation mechanisms, undermining mutual trust between states; this situation is particularly evident in conflict zones where complex and covert tactics are employed. Nonetheless, the imperative to develop more robust and flexible counterstrategies has also highlighted the growing importance of international coordination and collaboration. Hybrid threats cannot be mitigated in isolation; instead, they require collective action and integrated responses.

In conclusion, hybrid warfare is reshaping the global security order by fusing traditional and modern methods of conflict. Its impact is not confined to the battlefield but extends into cyberspace, financial markets, political discourse, and social cohesion. As hybrid threats continue to evolve, states and international institutions must devise new strategic frameworks that reflect the realities of this transformed threat environment. The emergence of hybrid warfare marks the beginning of a lasting transformation in the theory and practice of international security—one that demands both analytical innovation and operational resilience in the face of increasingly blurred lines between war and peace, combatants and civilians, and physical and informational domains.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) did not receive any financial support for the research, writing, and/or publication of this article.

Statements of Publication Ethics

We hereby declare that the study has not unethical issues and that research and publication ethics have been observed carefully.

Ethics Committee Approval Information

I declare that I did not collect data from participants using any survey, interview, focus group study, observation, experiment, or other interview techniques within the scope of the study whose information is given below, that I did not conduct any experiments on humans or animals, etc., and that I did not violate the personal data protection law; I declare as the responsible author that this study is one of the studies that does not require ethics committee approval.

References

Arquilla, J., & Ronfeldt. D. (1993). Cyberwar is Coming!. *Comparative Strategy*, 12 (2), 141-165.

Aytuğ, K. H. & Pozan, İ. F. (2023). Gelişen Hibrit Savaş Ortamında NATO-AB İş Birliği, *Karadeniz Araştırmaları*, 20 (77), 1-27.

Bachmann, S. D., & 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.

Baldwin, D. A. (2020). *Economic Statecraft*: *New Edition*, USA: Princeton University Press.

Bennett, W. L., & Livingston, S. (2020). *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States*. USA: Cambridge University Press.

Biddle, S., & Friedman, J. A. (2008). *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy*. US Army War College Strategic Studies Institute. US Army War College Press.

Brett, W. A. (2012). Clausewitz's Continued Relevance and Foundation for Educating Critical Thinking Skills, Usawc Strategy Research Project, U.S. Army War College, https://apps.dtic.mil, 10/08/2024.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Clarke, R. A., & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco Publications.

Clausewitz, C. V. (1989). *On War*. (Ed. Peter Paret). USA: Princeton University Press.

Creveld, M. L. V. (1991). *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*. Free Press.

European Commission (2016). Joint Framework on Countering Hybrid Threats, https://ec.europa.eu/commission/presscorner/detail/en/memo_16_1250

European External Action Service. (2018). Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats, https://www.eeas.europa.eu/node/46397_en

Galeotti, M. (2016). *Hybrid War or Gibridnaya Voina? Getting Russia's Non-linear Military Challenge Right*. Lulu Press.

Gilpin, R. (2020). Hegemonik Savaş Teorisi, (ed. Esra Diri), *Uluslararası İlişkilerde Anahtar Metinler*, 423-441. İstanbul: DER Yayınları.

Goldthau, A., & Sitter, N. (2015). *A Liberal Actor in a Realist World: The European Union Regulatory State and the Global Political Economy of Energy*. Oxford University Press.

Gök, A. (2021). *Hibrit Savaşlar: Rusya ve İsrail Örnekleriyle*, Ankara: Nobel Yayınevi.

Grotius, H. (2011). Savaş ve Barış Hukuku, (çev. Seha L. Meray), İstanbul: SAY Yayınları.

Henckaerts, J.-M., & Doswald-Beck, L. (2005). *Customary International Humanitarian Law: Volume I: Rules*. Cambridge University Press.

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

Hoffman, F. G. (2009). Hybrid Warfare and Challenges. *Joint Force Quarterly*, 52, 34-39. https://smallwarsjournal.com/documents/jfqhoffman.pdf

Irwin, D. A. (2017). *Clashing over Commerce: A History of US Trade Policy*. The University of Chicago Press.

Johnson, D. E. (2012). *Military Capabilities for Hybrid War. Insights from the Israel Defense Forces in Lebanon and Gaza*, RAND Corporation.

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

Jowett, G. S., & O'Donnell, V. (2015). *Propaganda & Persuasion*, (ed. 6th), Sage Publications.

Kahraman, Ö. (2019). *Suriye Krizi'nde Lübnan Hizbullah'ının Rolü*, Gece Kitaplığı, Ankara.

Kalb, M. & Saivetz, C. (2007). The Israeli-Hezbollah war of 2006: The Media as a Weapon in Asymmetrical Conflict. *Harvard International Journal of Press/Politics,* 12 (3), 43-66.

Kaldor, M. (2013). In Defence of New Wars, *Stability*, 2 (1): 4, 1-16.

Kaplan, F. (2023). "Hibrit Savaş" Teriminin İkinci Lübnan Savaşı ve Rusya'nın Kırım'ı İlhakı Kapsamında İncelenmesi, *Güvenlik Stratejileri Dergisi,* 19 (45), 393-420.

Kott, A., et al. (2015). *Cyber Defense and Situational Awareness*. Springer Press.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Lind, W. S. et al. (1989). The Changing Face of War: Into the Fourth Generation, *Marine Corps Gazette*, 22-26.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare, *Security Studies*, 22 (3), 365-404.

Miskimmon, A., et al. (2013). *Strategic Narratives: Communication Power and the New World Order*. Routledge Publications.

Mumford, A. (2013). Proxy Warfare and the Future of Conflict. *The RUSI Journal*, 158 (2), 40-46.

Murray, W., & Mansoor, P. R. (2012). *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge University Press.

NATO. (2015). NATO's Response to Hybrid Threats. Retrieved from https://www.ndc.nato.int/news/news.php?icode=886

NATO. (2016). *Social Media As A Tool Of Hybrid warfare*, NATO Strategic Communications Centre of Excellence.

Ören, E. (2022). The Just War in Political Thought: from Cicero to Grotius, *Çankırı Karatekin Üniversitesi İİBF Dergisi*, 22 (3), 188-204.

Pape, R. A. (1997). Why Economic Sanctions Do Not Work, *International Security*, 22 (2), 90-136.

Pirani, S. (2007). *Ukraine's Gas Sector*. Oxford Institute for Energy Studies.

Rid, T. (2012). Cyber War Will Not Take Place, *Journal of Strategic Studies*, 35 (1), 5-32.

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Schmitt, M. N., & Vihul, L. (2017). *The Nature of International Law Cyber Norms,* in "International Cyber Norms: Legal, Policy & Industry Perspectives", (ed. Osula & Röigas), NATO Cooperative Cyber Defence Centre of Excellence, 23-47.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Smith, R. (2008). *The Utility of Force in the Modern World.* Vintage Press.

Starbird, K., et al. (2019). Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations, *Proceedings of the ACM on Human-Computer Interaction*, 3 (CSCW), 1-26.

Tardy, T. (2020). *NATO 2030. United for a new era: a Digest*. NATO Defence College Policy Brief 23-20.

Tikk, E., et al. (2010). *International Cyber Incidents: Legal Considerations*. NATO Cooperative Cyber Defence Centre of Excellence.

Tikk, E., & Kerttunen, M. (2018). *Parabasis: Cyber-diplomacy in Stalemate*. Norwegian Institute of International Affairs Publications.

Vershbow A. R. & Speranza, L. M. (2019). *More In The Med: How NATO Can Refocus its Efforts in the South and Italy Can Lead the Charge*. Atlantic Council Report.

Waltz, K. N. (2018). *Man, the State, and War: A Theoretical Analysis*. Columbia University Press.

Weigley, R. F. (1977). *The American Way of War: A History of United States Military Strategy and Policy*, Indiana University Press.

Wilkie, R. (2009). Hybrid warfare: something old, not something new, *Air and Space Power Journal*, 23 (4), 13-17.

Zagorin, P. (2008). *Thucydides: An Introduction for the Common Reader*. Princeton University Press.

GENİŞLETİLMİŞ ÖZET

Hibrit savaş, günümüz uluslararası güvenlik ortamında ortaya çıkan en önemli güvenlik tehditlerinden biri olarak öne çıkmakta olup, karmaşık ve çok boyutlu yapısıyla dikkat çekmektedir. Hem geleneksel hem de modern savaş unsurlarını bir arada barındıran hibrit savaş, uluslararası güvenlik stratejilerini doğrudan etkilemekte ve çeşitli yaklaşımların geliştirilmesini zorunlu kılmaktadır. Bu savaş modeli yalnızca devletler tarafından değil; devlet dışı aktörler, terör örgütleri ve siber saldırganlar tarafından da uygulanabilmektedir. Bu bağlamda hibrit savaş, geleneksel ve modern savaş kavramlarının kesişim noktasında yer almakta ve uluslararası güvenlik mimarisinde yeni zorluklar ve fırsatlar yaratmaktadır.

Bu makalenin temel amacı, geleneksel ve modern savaş kavramları arasındaki ilişkiyi incelemek, bu iki savaş türünün hibrit savaş kavramı altında nasıl birleştiğini ve uluslararası güvenlik üzerindeki etkilerini analiz etmektir. Çalışma kapsamında, hibrit savaşın geleneksel askerî stratejiler ile modern teknolojik ve bilgi temelli savaş taktiklerini nasıl entegre ettiği, bu birleşimin uluslararası güvenlik örgütleri, devletler ve devlet dışı aktörler üzerindeki etkileri ve söz konusu dinamiklerin gelecekteki güvenlik ortamını nasıl şekillendireceği kapsamlı bir şekilde değerlendirilmiştir.

Hibrit savaş, geleneksel güvenlik algılarını aşarak uluslararası güvenlik politikalarında köklü dönüşümlerin önünü açmaktadır. Bu yeni savaş biçiminin doğru bir şekilde anlaşılması, devletler ve uluslararası örgütler için asimetrik tehditlere karşı daha etkili stratejiler geliştirilmesi açısından kritik öneme sahiptir. Siber saldırılar, dezenformasyon kampanyaları, ekonomik yaptırımlar ve vekil güçler gibi hibrit savaş unsurları, yalnızca askerî değil; ekonomik, politik ve toplumsal alanlarda da ciddi tehditler oluşturmaktadır. Bu nedenle, hibrit savaş üzerine yapılan akademik çalışmalar, uluslararası güvenlik politikalarının yeniden şekillendirilmesine ve devletlerin bu tür tehditlere karşı daha hazırlıklı olmalarına katkı sağlayacaktır.

Hibrit savaşın etkileri yalnızca ulusal güvenlik politikalarıyla sınırlı kalmamakta, aynı zamanda küresel güvenlik yönetişimi açısından da yeni sınamalar ortaya çıkarmaktadır. Geleneksel savaş hukukunun tanımlayıcı çerçevesi hibrit tehditler karşısında yetersiz kalmakta; savaş ilanı, saldırı tanımı, sivillerin korunması ve sorumluluğun tespiti gibi konular hibrit savaş senaryolarında gri alanlara çekilmektedir. Bu durum, uluslararası hukuk sisteminin ve Birleşmiş Milletler gibi örgütlerin krizlere etkin ve meşru müdahale kapasitesini sınırlamakta, devletlerin hibrit tehditlere karşı hukuki temelde nasıl hareket edeceği konusunda belirsizlik yaratmaktadır. Bu noktada, hibrit savaşın meşruiyet sorunları da akademik ve politik düzeyde ciddi bir tartışma konusu haline gelmektedir.

Bu çalışmada, geleneksel ve modern savaş kavramları, hibrit savaş kavramı ile karşılaştırmalı olarak ele alınmaktadır. İlk bölümde, geleneksel savaş kavramı; devletler arası çatışmalar, savaş hukuku ve konvansiyonel silahların rolü bağlamında ele alınırken; modern savaş kavramı, siber saldırılar, bilgi savaşı ve teknolojik yenilikler çerçevesinde incelenmiştir. Takip eden bölümlerde, hibrit savaşın bu iki savaş türünü nasıl birleştirdiği ve karmaşık bir tehdit oluşturduğu tartışılmaktadır. Ayrıca, hibrit savaşın uluslararası güvenlik üzerindeki etkileri, özellikle NATO ve AB gibi başlıca uluslararası güvenlik örgütleri bağlamında değerlendirilmektedir. Son olarak, hibrit savaşın unsurları ve bu unsurların gelecekteki uluslararası güvenlik mimarisi üzerindeki muhtemel etkileri tartışılmıştır. Bu değerlendirmeler, literatür taramasına dayanmakta olup, elde edilen veriler nitel araştırma yöntemlerinden biri olan doküman analizi yöntemiyle analiz edilmiştir.

Hibrit savaşın evrimi, uluslararası güvenlikte yeni zorluklar doğurmuş ve geleneksel güvenlik paradigmalarının ötesinde düşünmeyi zorunlu kılmıştır. Devletler, hibrit tehditlere yalnızca askerî güçle değil; aynı zamanda siber savunma, stratejik iletişim, ekonomik dayanıklılık ve hukuki normlar aracılığıyla da karşı koymak zorundadır. Bu bağlamda, hibrit savaşın uluslararası ilişkiler üzerindeki kalıcı etkileri kaçınılmaz görünmektedir. Hibrit savaş stratejileri, uluslararası hukuku, diplomasiyi ve güvenlik iş birliği mekanizmalarını yeniden şekillendirmekte ve gelecekteki çatışmaların doğasını belirlemektedir.

Bununla birlikte, hibrit savaş stratejileri, uluslararası rekabetin karakterini de değiştirmektedir. Geleneksel güç projeksiyonu yöntemleri yerini daha örtük, maliyeti düşük ve siyasi sonuçları daha yönetilebilir araçlara bırakmaktadır. Siber alanın, medya platformlarının ve enerji kaynaklarının birer jeopolitik silaha dönüşmesi, güç mücadelesini yalnızca savaş alanlarına değil, toplumların içine taşımakta; kamuoyunu, seçim süreçlerini ve ekonomik istikrarı hedef alan yeni nesil tehdit türleri ortaya çıkmaktadır. Bu bağlamda hibrit savaş, yalnızca güvenlik mimarisini değil, aynı zamanda egemenlik kavramını, demokratik kurumların işleyişini ve stratejik özerklik anlayışını da yeniden tanımlamaktadır. Dolayısıyla bu makale, hibrit savaşın çok katmanlı doğasını

yalnızca bir güvenlik sorunu olarak değil; aynı zamanda jeopolitik, hukuki ve sosyo-politik boyutlarıyla birlikte kavramsallaştırmaya çalışmaktadır.

Yeni nesil çatışma stratejileri, uluslararası güvenliği daha belirsiz ve öngörülemez hâle getirirken, devletler ve uluslararası örgütler için sürekli bir uyum süreci gerektirmektedir. Hibrit savaş, geleneksel ittifakları zorlamakta, devletler arası güveni zedelemekte ve çok taraflı iş birliği mekanizmalarını zayıflatmaktadır. Bununla birlikte, hibrit tehditlerle başa çıkmak için daha güçlü ve esnek stratejiler geliştirme ihtiyacı, uluslararası güvenlikte iş birliği ve koordinasyonun önemini bir kez daha gözler önüne sermektedir. Sonuç olarak, hibrit savaş, küresel güç dengelerini yeniden şekillendirmekte ve uluslararası güvenlik ile uluslararası ilişkilerde kalıcı bir dönüşüm sürecini tetiklemektedir. Bu dönüşüm, devletlerin ve uluslararası örgütlerin gelecekteki güvenlik tehditlerine karşı hazırlıklı olabilmeleri için yeni stratejik yaklaşımlar geliştirmelerini zorunlu kılmaktadır.