



University of Piraeus

Department of International & European Studies

School of Economics, Business & International Studies

Master Program in American Studies:
Politics, Strategy and Economics

«Hybrid Warfare and American Strategy»

By

Ioannis Morfakidis

Piraeus, Greece, October 2024

Το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος.

A handwritten signature in black ink, consisting of several overlapping loops and lines, positioned on the right side of the page.

Hybrid Warfare and American Strategy

By

Ioannis Morfakidis

Thesis

Submitted to the University of Piraeus

Department of International & European Studies

School of Economics, Business & International Studies

for the degree of

Master Program in American Studies:

Politics, Strategy and Economics

October, 2024

Piraeus, Greece

Approved:

Date:

.....

.....

.....

.....

.....

.....

TABLE OF CONTENTS

Introduction	1
CHAPTER 1: Historical Context and Evolution of Hybrid Warfare	
1.1 Early Examples	5
1.2 The Medieval Period	6
1.3 The American Revolutionary War	7
1.4 The Napoleonic Wars	8
1.5 World Wars	9
1.6 The Cold War	10
1.7 Vietnam War	11
1.8 Post-Cold War Era and the 21 st Century	12
CHAPTER 2: Components of Hybrid Warfare	
2.1 Introduction	15
2.2 Conventional Tactics	15
2.3 Unconventional Tactics	16
2.4 Cyber Warfare	18
2.5 Information Warfare	19
2.6 Economic and Political Pressure	21
2.7 Integration of Components	22
CHAPTER 3: American Strategy and Response to Hybrid Warfare	
3.1 Introduction	25
3.2 Current U.S. Defense Strategy	25
3.3 Doctrine and Policies	28
3.4 Case Studies	30
3.5 Strengths and Weaknesses	33
CHAPTER 4: Challenges in Countering Hybrid Warfare	
4.1 Introduction	37
4.2 Identification and Attribution	38
4.3 Interagency Coordination	39

4.4 Technological and Intelligence Gaps	40
4.5 Legal and Ethical Considerations	42
4.6 Strategic Adaptations and Innovations	43
4.7 International Cooperation and Legal Frameworks	44
4.8 Societal Resilience and Public Awareness	45
CHAPTER 5: U.S. Strategic Adaptations and Recommendations	
5.1 Introduction	47
5.2 Policy Recommendations	47
5.3 Technological Advancements	48
5.4 Training and Education	52
5.5 Resilience and Defense Mechanisms	53
5.6 Developing a Long-Term Strategy	54
5.7 Developing Resilience in Critical Infrastructure	56
5.8 Strengthening International Legal Frameworks	57
CHAPTER 6: Conclusions	
6.1 The Evolution and Relevance of Hybrid Warfare	59
6.2 The U.S. Response to Hybrid Warfare	60
6.3 Hybrid Warfare as the Continuation of War with Other Weapons	61
6.4 The Necessity of Adapting	63
REFERENCES	69

INTRODUCTION

Overview of Hybrid Warfare

War will always be a confrontation in which the intention of the adversaries will be the use of all the means at their disposal, in the most coordinated way possible, to impose their will. Hybrid war does not constitute something new in history and is not different from the war on which Sun Tzu wrote his treatise in the 5th century B.C., or from the wars that philosophers, sociologists, political scientists, historians, strategists, soldiers, etc., have attempted to theorize throughout history. The new in the concept of hybrid war is the growing capacity of international actors to use all tools at their disposal to project power. Paramilitary forces, presence of weapons of mass destruction, terrorist groups, organized crime, failed states are some of the threats that reveal the complexity of Hybrid war¹.

Technology has a huge impact on war, but human, ethics, geography and logistics do as well. It is so complex in its working parts that it is not possible to approach war through one or two perspectives². Recent conflicts highlight the need to remember that the enemy have the capacity to reason creatively.

Hybrid Warfare is a term that covers the need to understand contemporary warfare especially after the collapse of Soviet Union. The first that use this term was General James N. Mattis on September 2005, at the fourth annual Sea Services Forum. In the same year General Mattis and Frank Hoffman wrote an article about the Hybrid War³. According to this article Hybrid Warfare is a combination of novel approaches and a synthesis of the four emerging challengers; the traditional, the irregular, the catastrophic and the disruptive⁴. Frank Hoffman developed later the concept of Hybrid Warfare, in which can take part state and non-state actors.

¹ Juan Jose Terrados, "Hybrid Warfare", *The Three Swords Magazine*, 35/2019, 43.

² Murat Caliskan, "Hybrid warfare through the lens of strategic theory", *Defence & Security Analysis* (2019):1. doi: 10.1080/14751798.2019.1565364.

³ Ibid.

⁴ James N. Mattis and Frank Hoffman, "Future Warfare: The Rise of Hybrid Wars", USNI, no.11 (2005):1-2.

Hybrid Threats

Frank Hoffman defined Hybrid threats as “*the full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.*” Most current definitions of hybrid threats lean heavily on Russian actions in Ukraine and Crimea.

The character of warfare continues to evolve with the ongoing information revolution being a significant factor that offering adversaries new opportunities to exploit the spectrum of conflict beyond the utility of force. Hybrid threats do not follow a set pattern, and can be generated by a wide range of actors creatively using whatever means and measures available to achieve their strategic objectives. The adversary prefers to stay short of the threshold of conventional warfare but may eventually resort to the direct application of force. It should be expected that future threats will evolve in this way, with adversaries tailoring their means and measures to a targeted nation’s vulnerabilities⁵.

Hybrid threats, by their very nature, are about creating effects that influence political decision-making process. These effects can be diffuse, developing over a long period of time and not noticeable until it is too late. This ambiguity means that they can be difficult for governments to identify, attribute or publicly define because the responsible actor, or overall intent, is unclear or deliberately obscured.

Relevance to American Strategy

During Iraq campaign, there was a need for more troops on the ground, whose firepower should be used more against rebels and less against a conventional force. The first official mention of the Hybrid war, was in the Quadrennial Defense Review (QDR) by the U.S Department of Defense. According to the QDR of 2010, the term “hybrid” is used to capture the increased complexity of war, characterized by the multiplicity of actors involved and the blurring of traditional categories of conflict. As a result U.S forces need to prepare for a range of conflicts to confront hybrid approaches. These may involve state adversaries that employ

⁵ Bean Heap, *Hybrid Threats: A Strategic Communication Perspective*, (NATO StartCom COE, 2019), 18.

protracted forms of warfare, possibly using proxy forces to coerce and intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states⁶.

The increased complexity of the war, the multiplicity of actors involved and the blurring between traditional categories of conflict were the reasons that the term “hybrid” used by U.S in the QDR of 2010. Hybrid approaches could be implemented by state actors that employ protracted forms of warfare, possibly using proxy forces to coerce and intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states⁷.

The significance of hybrid warfare in the context of U.S. national security and defense strategy cannot be overstated. As global power dynamics shift and technological advancements accelerate, the United States faces a diverse array of threats that require a nuanced and flexible approach to defense. Traditional military might, while still crucial, is no longer sufficient to address the multifaceted challenges posed by hybrid warfare. Adversaries such as Russia, China, and various non-state actors have increasingly adopted hybrid tactics, compelling the U.S. to rethink and adapt its strategic doctrines to effectively counter these threats.

Research Methodology

This thesis employs a case study methodology, focusing on key state and non-state actors' strategies in hybrid warfare. The case study approach allows for an in-depth exploration of complex, multi-dimensional strategies that cannot be fully captured by quantitative methods alone. This method is particularly suited for understanding the intricacies of hybrid warfare, where diverse tactics such as cyberattacks, psychological operations, and guerrilla warfare are combined in American Strategy.

Controlled comparison is used to analyze different hybrid warfare strategies across time periods and regions. By comparing cases, this method helps identify patterns, isolate variables, and draw more robust conclusions about the evolution and effectiveness of hybrid warfare tactics from U.S. The case studies are selected based on their relevance to the research questions, ensuring they provide meaningful insights into the topic at hand.

⁶ U.S. Department of Defense, Quadrennial Defense Review Report, (Washington DC, 2010), 8.

⁷ Ibid.

Process tracing is applied to follow the sequence of events that led to the development and implementation of hybrid warfare strategies. This method allows for a detailed examination of causal mechanisms, uncovering how specific tactics in American Strategy influenced outcomes in conflicts. It helps in understanding the progression from initial strategic decisions to their execution and impact.

The research also utilizes qualitative content analysis to examine propaganda, media manipulation, and psychological operations—key elements in modern hybrid warfare. By analyzing these aspects, the research provides a deeper understanding of how hybrid tactics influence political and military outcomes in United States, especially in terms of public perception and strategic decision-making.

Thesis Statement

America's potential adversaries are likely to employ a hybrid mix of approaches and capabilities if and when they choose to oppose the United States, its allies, or its partners. This thesis examines the evolution, components, and implications of hybrid warfare, with a particular focus on how the United States has responded and adapted its strategy to this emerging form of conflict. It argues that while the U.S. has made significant strides in recognizing and addressing hybrid threats, there remain critical areas where strategic and operational adaptations are necessary to enhance its resilience and effectiveness.

CHAPTER 1

Historical Context and Evolution of Hybrid Warfare

1.1 Early Examples

Hybrid warfare involves the use of various methods and tactics to achieve strategic ends without resorting to full-scale, conventional warfare. Historically, various empires and states tried to combine military and non-military tactics to exert influence and achieve their objectives, setting the stage for the modern understanding of hybrid threats⁸.

The concept of hybrid warfare can be traced back to ancient and medieval times, where a combination of conventional and unconventional tactics was used to achieve strategic objectives. The Persian Empire, for example, effectively utilized a mix of conventional military power and psychological operations to maintain control over its vast territories. By incorporating local leaders into their administration and using propaganda, the Persians managed to create a stable and loyal empire for years⁹. This blend of direct military force and psychological manipulation laid the foundation for future hybrid warfare strategies.

The Mongol Empire under Genghis Khan represents another early example of hybrid warfare. The Mongols employed psychological warfare and espionage alongside their formidable cavalry forces to conquer and control extensive territories in China and Central Asia. Their use of terror as a psychological weapon, spreading fear and misinformation, weakened the resolve of their enemies before the actual military engagement¹⁰. The Mongols' strategic use of mobility, intelligence, and psychological impact exemplifies the principles of hybrid warfare that continue to be relevant today.

The Mongols also engaged in sophisticated forms of intelligence gathering, utilizing networks of spies and scouts to understand the political and military landscapes of their enemies. This allowed them to exploit weaknesses and strike at opportune moments, often before their enemies could organize a coherent defense. The use of such intelligence operations,

⁸ Heap, *Hybrid Threats: A Strategic Communication Perspective*.

⁹ David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Routledge, 2004).

¹⁰ Thomas J. Barfield, *The Perilous Frontier: Nomadic Empires and China* (Oxford: Basil Blackwell, 1989).

combined with their rapid and mobile cavalry, made the Mongols an unstoppable force during their time. Their ability to blend traditional military prowess with advanced psychological and intelligence tactics marks them as one of the earliest practitioners of what we now recognize as hybrid warfare¹¹.

1.2 The Medieval Period

During the medieval period, the Byzantine Empire demonstrated sophisticated hybrid warfare strategies. The Byzantines combined military strength with diplomacy, intelligence operations, and psychological warfare. They employed mercenaries, forged alliances through diplomatic marriages, and used strategic misinformation to destabilize their adversaries. This multifaceted approach allowed the Byzantine Empire to maintain its dominance and stability in a highly unstable region. The Byzantines' use of diverse tactics to maintain their influence showcases the enduring relevance of hybrid warfare principles¹².

They often used religion as a tool to exert influence over neighboring regions, spreading Orthodox Christianity as a means of soft power. By converting neighboring leaders and populations to Christianity, the Byzantines not only expanded their cultural influence but also created religious bonds that reinforced political alliances. This form of religious diplomacy was particularly effective in the Balkans and Eastern Europe, where Byzantine religious authority was often seen as a counterbalance to the Catholic West. This strategy of using religion as part of their hybrid warfare toolkit allowed the Byzantines to project power far beyond their borders without the need for direct military intervention¹³.

Furthermore, the Byzantine strategy often involved recruiting foreign warriors as mercenaries, ensuring loyalty through payments and political favors. These mercenaries were used not only for direct combat but also for covert operations and sabotage against potential threats. The Byzantines' use of diplomacy was equally sophisticated, involving complex negotiations to secure alliances, and the dissemination of strategic misinformation to create

¹¹ Timothy May, *The Mongol Art of War: Chinggis Khan and the Mongol Military System* (Yardley, PA: Westholme Publishing, 2007), 84.

¹² J. Haldon, *Warfare, State and Society in the Byzantine World, 565-1204* (London: Routledge, 1999).

¹³ Edward N. Luttwak, *The Grand Strategy of the Byzantine Empire* (Cambridge, MA: Belknap Press of Harvard University Press, 2009), 145.

discord among their enemies¹⁴. This comprehensive approach, highlights the complexity and adaptability required in hybrid warfare, a concept that remains crucial in modern conflict scenarios.

1.3 The American Revolutionary War

The American Revolutionary War between 1775 and 1783 is a prime example of early modern hybrid warfare. The American colonists employed a mix of conventional and guerrilla tactics against the British. While the Continental Army engaged in traditional battles, irregular forces used hit-and-run tactics, ambushes, and sabotage against British supply lines and outposts. Additionally, the Americans leveraged propaganda to garner support for their cause, both domestically and internationally. This combination of military and psychological strategies was instrumental in the eventual success of the American revolutionaries¹⁵.

The colonists' use of guerrilla warfare was particularly effective in the dense forests and rugged terrain of North America, where traditional British military tactics were less effective. Local militias, composed of farmers and tradesmen, conducted unexpected attacks and ambushes, disrupting British supply lines and communication networks. These irregular tactics were complemented by a sophisticated propaganda campaign that included pamphlets, newspapers, and speeches aimed at rallying public support and persuading potential allies abroad, such as France, to join the fight against the British. This multifaceted approach exemplifies the core elements of hybrid warfare, blending conventional and unconventional methods to achieve strategic goals¹⁶.

During the war, colonists employed a range of economic tactics, including boycotts of British goods and the establishment of alternative trade networks, to weaken British economic interests in the colonies. These economic pressures, coupled with the disruption of British trade routes by American privateers, significantly strained British resources and contributed to the overall war effort. Additionally, the use of intelligence networks, such as the Culper Spy Ring, played a crucial role in gathering information on British troop movements and plans, which allowed the Continental Army to make informed strategic decisions. These elements of

¹⁴ Ibid.

¹⁵ Robert W. Coakley and Stetson Conn, *The War of the American Revolution* (Washington, D.C.: Center of Military History, United States Army, 2010), 10-12, 22, 53-67.

¹⁶ Ibid.

economic and intelligence warfare illustrate the complexity and depth of the American revolutionary strategy, making it a quintessential example of hybrid warfare¹⁷.

1.4 The Napoleonic Wars

The Napoleonic Wars (1803-1815), further illustrate the use of hybrid strategies. Napoleon's forces combined conventional battles with psychological operations and political maneuvers. Napoleon himself was a master of propaganda, using bulletins and proclamations to maintain the morale of his troops and the support of the French populace. Moreover, the Peninsular War (1808-1814) against Spain highlighted the effective use of guerrilla tactics by Spanish partisans, disrupting French supply lines and communication¹⁸. This blend of direct and indirect tactics showcases the strategic depth of hybrid warfare.

Napoleon's strategic genius lay not only in his battlefield tactics but also in his ability to manipulate information and perception. He crafted a narrative of invincibility through carefully controlled messages to his troops and the public, reinforcing the image of a charismatic and unbeatable leader. Meanwhile, the Spanish guerrillas, or "guerrilleros," employed hit-and-run tactics, leveraging their knowledge of the local terrain to launch surprise attacks on French forces. These guerrilla operations significantly hampered French logistics and stretched their resources thin, contributing to Napoleon's eventual defeat in the Peninsular War. The effective use of propaganda and irregular tactics in this conflict underscores the enduring principles of hybrid warfare¹⁹.

By exploiting the fragmented political landscape of Europe, Napoleon was able to isolate enemies and secure temporary alliances that served his strategic goals. The use of marriage alliances, such as his own marriage to Marie Louise of Austria, was part of this broader diplomatic strategy to legitimize his rule and secure the cooperation or neutrality of potential adversaries. Additionally, Napoleon's Continental System, an economic blockade against Britain, aimed to weaken his most persistent enemy through economic means rather than direct military confrontation. This integration of military, economic, and diplomatic strategies in

¹⁷ John Ferling, *Whirlwind: The American Revolution and the War That Won It* (New York: Bloomsbury Press, 2015), 213.

¹⁸ Charles Esdaile, *Napoleon's Wars: An International History, 1803-1815* (London: Penguin Books, 2008).

¹⁹ *Ibid.*

Napoleon's approach exemplifies the multi-faceted nature of hybrid warfare, highlighting its effectiveness in achieving strategic objectives without relying solely on military force²⁰.

1.5 World Wars

The World Wars marked significant advancements in hybrid warfare techniques. In WWI, the use of propaganda became institutionalized, with nations establishing dedicated departments for psychological operations. The British established the War Propaganda Bureau, while the Germans used leaflets and other media to demoralize Allied troops. This institutionalization of propaganda demonstrated its critical role in modern warfare²¹.

World War I saw the unprecedented use of propaganda to maintain home front morale and undermine enemy resolve. The British War Propaganda Bureau produced posters, pamphlets, and films that depicted the war as a noble cause and demonized the enemy. These efforts were mirrored by the Germans, who distributed leaflets over enemy lines to incite desertion and spread disinformation. The widespread use of propaganda highlighted its potential as a powerful tool in hybrid warfare, capable of shaping public opinion and influencing the course of the war. The strategic deployment of psychological operations in World War I underscores the evolution of hybrid warfare tactics²².

World War II saw the extensive use of hybrid warfare. The Nazi regime utilized a combination of conventional military power, covert operations, and propaganda to achieve its objectives. The Blitzkrieg strategy combined rapid, mechanized attacks with psychological warfare to shock and disorient the enemy. Additionally, resistance movements across occupied Europe employed guerrilla tactics, sabotage, and intelligence operations to undermine German control²³.

The Nazis' Blitzkrieg strategy, or "lightning war," was designed to deliver a swift and decisive blow to the enemy, combining fast-moving infantry, tanks, and air support to create confusion and panic. This approach was supported by psychological operations, including the

²⁰ David G. Chandler, *The Campaigns of Napoleon* (New York: Scribner, 2009), 367.

²¹ Garry S. Messinger, *British Propaganda and the State in the First World War* (Manchester: Manchester University Press, 1992).

²² Ibid.

²³ Peter Calvocoressi, Guy Wint, & John Pritchard, *Total War: Causes and Courses of the Second World War* (Penguin Books, 1989).

dissemination of leaflets and radio broadcasts to demoralize enemy soldiers and civilians. In occupied territories, resistance movements such as the French Maquis and the Polish Home Army conducted sabotage missions, gathered intelligence, and launched guerrilla attacks, significantly disrupting German operations and contributing to the eventual Allied victory. The integration of conventional military force with irregular tactics and psychological operations during World War II highlights the multifaceted nature of hybrid warfare²⁴.

1.6 The Cold War

The Cold War (1947-1991) epitomized the era of hybrid warfare, characterized by the extensive use of proxy wars, espionage, economic pressure, and propaganda. Both the United States and the Soviet Union engaged in a prolonged struggle for global influence without direct military confrontation, utilizing a variety of unconventional methods to achieve their strategic goals.

The United States countered with its own hybrid strategies, including covert operations by the CIA, psychological operations, and economic warfare. The CIA's involvement in the 1953 Iranian coup and the Bay of Pigs invasion in 1961 are examples of U.S. hybrid tactics. Additionally, the U.S. used information warfare to promote its ideology and counter Soviet propaganda. The American approach to hybrid warfare during the Cold War highlights the versatility and adaptability required to counter complex threats²⁵.

The U.S. response to Soviet hybrid warfare included a combination of covert actions, economic measures, and information campaigns. The CIA orchestrated coups and supported anti-communist insurgencies, while economic sanctions and aid were used to influence political outcomes in various countries. Information warfare played a critical role, with initiatives like Radio Free Europe broadcasting Western viewpoints behind the Iron Curtain, aiming to undermine Soviet control and inspire resistance among Eastern Bloc populations²⁶.

Both superpowers invested heavily in cultural diplomacy and propaganda to win the hearts and minds of populations around the world. The United States, for example, launched the Voice of America and other media initiatives to broadcast American ideals of freedom and

²⁴ Ibid.

²⁵ John Lewis Gaddis, *The Cold War: A New History* (New York: Penguin Books, 2005)

²⁶ Ibid.

democracy to audiences in communist countries. These psychological operations were designed not only to counter Soviet propaganda but also to create a positive image of the United States as a champion of liberty and human rights. The impact of these efforts was significant in shaping public opinion and influencing political developments in various parts of the world, further demonstrating the importance of psychological tactics in hybrid warfare²⁷.

1.7 Vietnam War

The Vietnam War (1955-1975) further highlighted the complexities of hybrid warfare. The North Vietnamese and the Viet Cong employed a mix of conventional and guerrilla tactics, supported by a robust propaganda campaign. The use of tunnels, ambushes, and hit-and-run attacks against superior U.S. army forces exemplified effective irregular warfare. Concurrently, the Tet Offensive in 1968 combined conventional assaults with psychological operations to influence public opinion and undermine U.S. resolve. The Vietnam War serves as a case study in the successful application of hybrid warfare by a less technologically advanced opponent²⁸.

The Vietnam War showcased the effective use of hybrid tactics by the North Vietnamese and the Viet Cong. They constructed an extensive network of tunnels to hide troops, weapons, and supplies, enabling them to launch surprise attacks and then disappear. These guerrilla tactics were supported by a comprehensive propaganda effort aimed at winning the "hearts and minds" of the South Vietnamese population and international audiences. The Tet Offensive, a coordinated series of attacks on more than 100 cities and outposts, was a psychological victory for the North, despite heavy casualties, as it dramatically shifted U.S. public opinion against the war. The strategic integration of guerrilla tactics and propaganda during the Vietnam War underscores the enduring relevance of hybrid warfare principles²⁹.

The assistance provided by the Soviet Union and China, in the form of weapons, supplies, and financial aid, significantly bolstered the capabilities of the North Vietnamese forces. This external support not only provided the material means necessary to sustain prolonged guerrilla operations but also served as a political and ideological endorsement of their cause. The strategic use of foreign aid in the Vietnam War illustrates the broader

²⁷ Odd Arne Westad, *The Global Cold War: Third World Interventions and the Making of Our Times* (Cambridge: Cambridge University Press, 2007), 311.

²⁸ Stanley Karnow, *Vietnam: A History* (New York: Penguin Books, 1997).

²⁹ Ibid.

application of hybrid warfare, where non-military elements such as international alliances and economic support play a crucial role in achieving military objectives³⁰.

1.8 Post-Cold War Era and the 21st Century

In the post-Cold War era, hybrid warfare evolved with advancements in technology and the rise of non-state actors. Conflicts in the Middle East, such as the Iraq War, showcased the use of improvised explosive devices (IEDs), cyber attacks, and media manipulation alongside traditional military operations. The 21st century has further seen the integration of cyber warfare and information operations as central components of hybrid warfare³¹.

1.8.1 The Gulf Wars

The Gulf Wars (1990-1991, 2003-2011) showcased the evolving nature of hybrid warfare in the post-Cold War era. During the 1991 Gulf War, Iraq employed a mix of conventional military defenses, information warfare, and environmental sabotage by setting Kuwaiti oil fields on fire. The 2003 invasion of Iraq by the United States and its allies saw the initial use of conventional military force, followed by a prolonged insurgency that utilized guerrilla tactics, IEDs, and cyber attacks against coalition forces. The Gulf Wars highlight the dynamic and adaptive nature of hybrid warfare in modern conflict³².

The 1991 Gulf War highlighted Iraq's use of hybrid tactics to counter the overwhelming military superiority of the U.S.-led coalition. Iraqi forces employed scorched earth tactics, setting oil fields ablaze to create environmental and economic damage. In the 2003 invasion, the initial phase saw the rapid defeat of the Iraqi military, but the subsequent occupation faced a fierce insurgency. Iraqi insurgents used IEDs, suicide bombings, and guerrilla tactics to inflict casualties and create instability, while cyber attacks targeted coalition communication networks and infrastructure. The multifaceted tactics used by Iraq during the Gulf Wars illustrate the complexity and adaptability of hybrid warfare³³.

³⁰ Mark Atwood Lawrence, *The Vietnam War: A Concise International History* (Oxford: Oxford University Press, 2008), 201.

³¹ Heap, *Hybrid Threats: A Strategic Communication Perspective*.

³² Anthony H. Cordesman, *The Iraq War: Strategy, Tactics, and Military Lessons* (Washington, DC: Center for Strategic and International Studies, 2003).

³³ Ibid.

Furthermore, during the 2003 invasion, the U.S. employed extensive psychological operations (PSYOP) to weaken Iraqi resolve and encourage defections among Iraqi forces. Leaflets were dropped, and radio broadcasts were made to convince Iraqi soldiers to surrender, emphasizing the futility of resistance and the inevitability of defeat. These psychological tactics, combined with overwhelming military force, aimed to reduce the need for prolonged conflict by undermining the enemy's will to fight. The successful use of PSYOP in the Gulf Wars highlights the importance of psychological elements in complementing kinetic military operations³⁴.

1.8.2 The War on Terror

The War on Terror, particularly in Afghanistan and Iraq, exemplifies modern hybrid warfare. Non-state actors like Al-Qaeda and the Taliban have effectively used guerrilla tactics, terrorism, and propaganda to counter superior conventional military forces. The Taliban's use of IEDs, suicide bombings, and hit-and-run attacks, combined with their ability to blend into local populations, highlights the challenges of combating hybrid threats. Additionally, the use of social media for propaganda and recruitment by groups like ISIS represents a significant evolution in information warfare. The War on Terror underscores the persistent and evolving nature of hybrid warfare in contemporary conflicts³⁵.

In Afghanistan, the Taliban's insurgency utilized asymmetric tactics to exploit the vulnerabilities of U.S. and NATO forces. Their strategic use of IEDs caused significant casualties and logistical challenges. Meanwhile, Al-Qaeda's global reach and ability to inspire lone-wolf attacks through sophisticated propaganda underscored the transnational nature of hybrid threats. ISIS further advanced these tactics, using social media to recruit fighters worldwide and spread their extremist ideology, demonstrating the power of digital platforms in modern hybrid warfare. The adaptive strategies of non-state actors during the War on Terror highlight the need for a comprehensive approach to counter hybrid threats³⁶.

³⁴ Cheryl A. Walley and Michael R. Mullins, *Psychological Operations in Operation Iraqi Freedom* (Washington, D.C.: U.S. Army Special Operations Command, 2005), 36.

³⁵ Kilcullen, David. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2009).

³⁶ Ibid.

1.8.3 The Russian Hybrid Warfare Doctrine

Russia's annexation of Crimea in 2014 is one of the most illustrative examples of contemporary hybrid warfare. The operation combined conventional military force with Russian soldiers who were masked and wore unmarked uniforms upon the outbreak of the Russo-Ukrainian War ("little green men"), cyber attacks, and an extensive disinformation campaign. Russia used social media and state-controlled media to shape narratives, create confusion, and justify their actions. This multifaceted approach successfully avoided a full-scale conventional conflict while achieving strategic objectives. The annexation of Crimea highlights the sophisticated and integrated nature of modern hybrid warfare³⁷.

The annexation of Crimea showcased Russia's ability to blend various elements of hybrid warfare effectively. The deployment of unmarked troops allowed Russia to deny direct involvement and avoid immediate international backlash. Simultaneously, cyber attacks targeted Ukrainian government and military communications, while a coordinated disinformation campaign on social media platforms sought to legitimize the annexation and sow discord within Ukraine and among Western allies. This operation highlighted the seamless integration of military, cyber, and informational tactics to achieve strategic goals without engaging in open warfare³⁸.

Also by leveraging its control over energy supplies, particularly natural gas, Russia exerted significant economic pressure on Ukraine and other European nations. The threat of cutting off energy supplies during the winter months created a potent lever to influence political decisions and reduce resistance to Russian actions. This use of economic coercion, combined with military and informational tactics, underscores the comprehensive nature of Russia's hybrid warfare approach, which effectively combines multiple instruments of power to achieve its strategic objectives³⁹.

³⁷ Mark Galeotti, "Hybrid War or Gibrinaya Voyna? Getting Russia's Non-Linear Military Challenge Right," *Prism* 6, no. 2 (2016): 2-15.

³⁸ *Ibid.*

³⁹ Mark Galeotti, *Hybrid War or Gibrinaya Voyna? Getting Russia's Non-Linear Military Challenge Right* (Prague: Mayak Intelligence, 2016), 54.

CHAPTER 2

Components of Hybrid Warfare

2.1 Introduction

Hybrid warfare is a complex and multifaceted approach that integrates various methods of conflict to achieve strategic objectives. Understanding the components of hybrid warfare is crucial for developing effective countermeasures. This chapter examines the primary components of hybrid warfare: conventional tactics, unconventional tactics, cyber warfare, information warfare, economic and political pressure, and the integration of these elements to form a cohesive strategy. These components, when integrated effectively, create a comprehensive approach to conflict that is difficult to counter with traditional military strategies alone.

2.2 Conventional Tactics

Conventional military tactics remain a core component of hybrid warfare. These tactics involve structured, organized operations with clearly defined command and control structures, utilizing advanced weaponry and technology. Conventional forces can establish dominance in physical domains and provide a credible threat or deterrent. For instance, during the annexation of Crimea, Russian conventional military forces played a pivotal role in providing a robust and credible threat that supported irregular operations and political maneuvers⁴⁰.

The effectiveness of conventional tactics in hybrid warfare lies in their ability to achieve rapid and decisive victories on the ground, thereby creating favorable conditions for the employment of other hybrid tactics. The initial use of overwhelming force can demoralize the enemy and disrupt their ability to coordinate an effective response. This approach was evident in the Gulf Wars, where the U.S. military's conventional superiority allowed it to achieve swift victories, setting the stage for subsequent hybrid tactics by insurgent groups⁴¹.

⁴⁰ Heap, *Hybrid Threats: A Strategic Communication Perspective*, 14.

⁴¹ Anthony H. Cordesman, *The Iraq War: Strategy, Tactics, and Military Lessons* (Washington, DC: Center for Strategic and International Studies, 2003).

However, conventional tactics alone are often insufficient in hybrid warfare. They need to be complemented by other strategies to address the multifaceted nature of modern conflicts. For example, while conventional military power was essential in the initial phases of the Iraq War, it was the subsequent unconventional and asymmetric tactics employed by insurgents that prolonged the conflict and challenged the coalition forces' dominance⁴².

Conventional military power provides a strategic framework that supports the deployment and success of other hybrid tactics. For instance, conventional forces can create the necessary security environment that allows for the execution of cyber and information warfare operations. The NATO analysis on hybrid threats, highlights that the credible presence of conventional forces can dissuade potential adversaries from overt military actions, thereby forcing them to rely on less direct, hybrid approaches such as cyberattacks or disinformation campaigns. This dynamic was particularly evident in the context of the Baltic states, where the presence of NATO forces served as a deterrent, compelling adversaries to shift towards non-conventional methods of exerting influence⁴³.

Modern conventional forces increasingly rely on precision-guided munitions, unmanned aerial vehicles (drones), and advanced surveillance systems to conduct operations with greater accuracy and efficiency. These technologies enable conventional forces to strike key targets with minimal collateral damage, thereby reducing the risk of civilian casualties and maintaining the legitimacy of military operations. Moreover, the use of technology in intelligence gathering and battlefield awareness allows for more informed decision-making, ensuring that conventional forces can adapt quickly to the evolving dynamics of hybrid warfare. The incorporation of such advanced technologies not only strengthens conventional military capabilities but also complements other hybrid warfare tactics, making them more integrated and effective in achieving strategic objectives⁴⁴.

2.3 Unconventional Tactics

Unconventional tactics, including guerrilla warfare, insurgency, and sabotage, are designed to exploit the vulnerabilities of superior conventional forces. These tactics rely on

⁴² Ibid.

⁴³ NATO, *Hybrid Threats: A Strategic Challenge* (Brussels: NATO, 2024), 31.

⁴⁴ Erik Gartzke and Jon R. Lindsay, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019), 204.

mobility, surprise, and intimate knowledge of the terrain. They aim to wear down the enemy through attrition and psychological impact rather than decisive engagements. The Viet Cong's use of guerrilla tactics during the Vietnam War is a classic example of effective unconventional warfare⁴⁵.

Guerrilla warfare and insurgency tactics are particularly effective in environments where conventional forces are constrained by rules of engagement and the need to minimize civilian casualties. By blending into local populations and utilizing the element of surprise, irregular forces can conduct hit-and-run attacks, ambushes, and sabotage operations that inflict disproportionate damage and erode the enemy's resolve. These tactics were extensively used by the Taliban in Afghanistan, causing significant casualties and logistical challenges for U.S. and NATO forces⁴⁶.

Unconventional tactics also include acts of sabotage and subversion aimed at disrupting the enemy's operations and infrastructure. For example, during World War II, resistance movements across occupied Europe conducted sabotage missions against German supply lines, communication networks, and industrial facilities. These actions not only disrupted German military operations but also had a significant psychological impact on both German forces and the occupied populations⁴⁷.

The evolution of unconventional tactics has also been significantly shaped by historical lessons, where hybrid forces effectively used non-traditional methods to counteract stronger adversaries. The use of unconventional warfare by smaller or technologically inferior forces has consistently proven to be a critical factor in their ability to survive and impose costs on larger military powers. This adaptability is particularly evident in the tactics employed by Hezbollah during the 2006 Lebanon War, where they utilized a combination of guerrilla tactics, information warfare, and urban combat to effectively challenge the Israeli Defense Forces⁴⁸.

⁴⁵ Stanley Karnow, *Vietnam: A History* (New York: Penguin Books, 1997).

⁴⁶ David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2009).

⁴⁷ Peter Calvocoressi, Guy Wint, and John Pritchard, *Total War: Causes and Courses of the Second World War* (New York: Penguin Books, 1989).

⁴⁸ Williamson Murray and Peter R. Mansoor, eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Cambridge: Cambridge University Press, 2012), 298.

Additionally, the effectiveness of unconventional tactics in hybrid warfare is amplified when they are used in conjunction with political and social manipulation. For instance, insurgent groups in the Middle East and North Africa have leveraged local grievances and sectarian divides to recruit fighters and gain popular support, thus creating a more resilient and motivated force. This method of intertwining unconventional military tactics with socio-political strategies complicates counterinsurgency efforts and prolongs conflicts, making them more difficult to resolve through conventional military means alone⁴⁹.

2.4 Cyber Warfare

Cyber warfare has become an essential element of hybrid conflict. Cyber operations can disrupt, damage, or gain unauthorized access to critical systems, often conducted covertly to complicate attribution. Cyber attacks can paralyze military operations, disrupt communications, and create widespread confusion. Notable examples include the Stuxnet worm that targeted Iran's nuclear facilities and the 2016 cyber attacks on the Ukrainian power grid⁵⁰.

The use of cyber operations in hybrid warfare allows state and non-state actors to achieve strategic objectives without engaging in physical combat. These attacks can target critical infrastructure, financial systems, and communication networks, creating significant disruption and chaos. The covert nature of these operations complicates attribution, making it difficult for the targeted state to respond effectively. Additionally, cyber espionage provides valuable intelligence that can be used to enhance other hybrid tactics⁵¹.

Cyber warfare also includes psychological operations conducted through digital platforms. For instance, during the 2016 U.S. presidential election, Russian cyber operatives used social media to spread disinformation and sow discord among the American public. This cyber campaign aimed to influence the political process and undermine public trust in democratic institutions. The strategic use of cyber operations in hybrid warfare underscores the importance of cybersecurity and digital resilience in modern conflict⁵².

⁴⁹ NATO, *Hybrid Threats: A Strategic Challenge* (Brussels: NATO, 2024), 31.

⁵⁰ Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012).

⁵¹ Ibid.

⁵² Galeotti, *Hybrid War or Gibrinaya Voina?*.

The growing sophistication of cyber warfare tactics in hybrid conflicts is evident in the increasing use of artificial intelligence (AI) and machine learning to automate and enhance cyber attacks. These technologies enable attackers to conduct more precise and adaptive operations, such as targeting specific vulnerabilities in critical infrastructure or using AI to generate deepfake videos for disinformation campaigns. The integration of AI into cyber warfare not only increases the effectiveness of these attacks but also complicates detection and response efforts, making them a formidable tool in the hybrid warfare arsenal⁵³.

Moreover, cyber warfare in hybrid conflicts often involves the strategic targeting of civilian infrastructure, such as power grids, communication networks, and financial systems, to create widespread disruption and panic. These attacks can have cascading effects, leading to economic instability, social unrest, and a loss of public confidence in the government. The ability to disrupt civilian life through cyber means without direct military engagement highlights the asymmetric nature of cyber warfare and its potential to achieve strategic objectives in hybrid conflicts⁵⁴.

The integration of cyber tactics allows adversaries to conduct operations that can cripple critical infrastructure, disrupt communication networks, and undermine the strategic stability of a nation without engaging in conventional military confrontations. As cyber capabilities continue to evolve, they have become increasingly central to the strategic calculations of states, enabling them to project power and influence across borders with minimal physical presence. The United States, recognizing the transformative impact of cyber warfare, has placed significant emphasis on developing its cyber capabilities as part of its broader hybrid warfare strategy, aiming to both defend against and deter cyber-enabled threats⁵⁵.

2.5 Information Warfare

Information warfare involves the use of propaganda, misinformation, psychological operations, and media manipulation to influence public perception and decision-making

⁵³ Erik Gartzke and Jon R. Lindsay, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019), 204.

⁵⁴ Frank Hoffman, Colonel Matt Neumeier, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 5.

⁵⁵ Christopher Whyte and Brian M. Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy*, 2nd ed. (Routledge, 2023), 87.

processes. This component aims to undermine the morale and cohesion of adversaries, shape narratives, and create favorable conditions for other hybrid tactics. The strategic use of social media for disinformation campaigns by state and non-state actors exemplifies modern information warfare⁵⁶.

This kind of warfare is a critical aspect of hybrid conflict, as it can shape the strategic environment and influence the actions of both adversaries and allies. By controlling the narrative and spreading disinformation, actors can create confusion, erode trust in institutions, and polarize societies. The use of social media platforms allows for the rapid dissemination of propaganda and fake news, reaching a global audience and amplifying the impact of other hybrid tactics. Effective information warfare can weaken an adversary's resolve and create opportunities for strategic gains⁵⁷.

The Russian annexation of Crimea is a prime example of effective information warfare. Russian state media and social media platforms were used to disseminate narratives that justified the annexation, portrayed Ukrainian authorities as illegitimate, and depicted Russian intervention as a protective measure for ethnic Russians in Crimea. This information campaign significantly influenced public perception both within Russia and internationally, complicating the response from Ukraine and its allies. The strategic manipulation of information highlights the importance of media literacy and strategic communication in countering hybrid threats⁵⁸.

In addition to traditional media, the use of advanced data analytics and micro-targeting in information warfare has revolutionized the way disinformation campaigns are conducted. By analyzing vast amounts of data from social media and other online sources, actors can identify specific demographics to target with tailored messages, increasing the effectiveness of their propaganda efforts. This approach was notably employed during the Brexit referendum and the 2016 U.S. presidential election, where targeted disinformation campaigns were used to influence voter behavior and sow discord within the population⁵⁹.

⁵⁶ Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia* (New York: PublicAffairs, 2015).

⁵⁷ Ibid.

⁵⁸ Galeotti, *Hybrid War or Gibrinaya Voina?*.

⁵⁹ NATO, *Hybrid Threats: A Strategic Challenge* (Brussels: NATO, 2024).

Furthermore deepfake technology enables the creation of hyper-realistic videos and audio that can depict individuals saying or doing things they never actually did, potentially leading to false perceptions and misguided actions based on fabricated evidence. This technology has the potential to undermine trust in media and public figures, making it a powerful tool in the hands of those seeking to manipulate public opinion and disrupt social cohesion. As deepfakes become more sophisticated, the challenge for governments and societies to detect and counteract such misinformation will only grow, emphasizing the need for advanced tools and strategies to maintain the integrity of information in the digital age⁶⁰.

Information warfare, particularly when enabled by cyber operations, plays a pivotal role in shaping the strategic environment of hybrid conflicts. By leveraging the global reach of digital platforms, adversaries can conduct disinformation campaigns, psychological operations, and propaganda efforts that sow discord, erode trust in institutions, and influence public opinion. The effectiveness of information warfare in hybrid conflicts lies in its ability to operate below the threshold of armed conflict, making it difficult for targets to respond without escalating the situation. The United States has increasingly focused on countering information warfare by enhancing its cyber defenses, promoting media literacy, and developing strategies to disrupt adversarial information operations before they can achieve their intended effects⁶¹.

2.6 Economic and Political Pressure

Economic and political pressure are critical components of hybrid warfare, employed to weaken an adversary without direct military confrontation. These methods include economic sanctions, trade restrictions, diplomatic isolation, and the use of economic leverage to influence political outcomes. The strategic use of economic and political tools can complement military and non-military tactics to achieve broader strategic objectives⁶².

Economic sanctions are a common tool used to exert pressure on adversaries. For example, the U.S. has imposed sanctions on countries like Iran and North Korea to curb their nuclear programs and influence their political behavior. These sanctions target key sectors of the economy, aiming to create internal dissent and force policy changes. The effectiveness of

⁶⁰ Galeotti, *Hybrid War or Gibrinaya Voina?*, 78.

⁶¹ Christopher Whyte and Brian M. Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy*, 2nd ed. (Routledge, 2023), 135.

⁶² Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

economic sanctions lies in their ability to inflict significant economic pain without resorting to direct military action⁶³.

Political pressure can also be exerted through diplomatic means, such as forming alliances, supporting opposition movements, and leveraging international organizations to isolate an adversary. During the Cold War, both the U.S. and the Soviet Union used political pressure to influence global events and shape the international order. The strategic use of political leverage is evident in the support provided to various insurgent movements and the diplomatic efforts to build coalitions against adversaries⁶⁴.

In hybrid warfare, economic and political pressure is often used in conjunction with other tactics to create a comprehensive strategy. For instance, Russia's hybrid warfare approach includes the use of energy resources as a tool of economic coercion. By manipulating gas supplies to Europe, Russia can exert political pressure on European countries, influencing their policies and actions. This multifaceted approach demonstrates the integration of economic and political tools in hybrid warfare strategies⁶⁵.

Moreover, the use of economic and political pressure in hybrid warfare can be strategically timed to coincide with other forms of aggression, such as cyber or military actions. For example, economic sanctions imposed on Russia following its annexation of Crimea were complemented by ongoing cyber operations and information campaigns, creating a comprehensive strategy that complicated the West's ability to respond effectively. This combination of economic, political, and military tactics illustrates the complexity and effectiveness of hybrid warfare in modern conflicts.

2.7 Integration of Components

The effectiveness of hybrid warfare lies in the seamless integration of its various components into a cohesive strategy. The combination of conventional and unconventional tactics, cyber warfare, information warfare, and economic and political pressure creates a complex and adaptive approach to conflict. This integration allows actors to exploit the

⁶³ Cordesman, *The Iraq War*.

⁶⁴ John Lewis Gaddis, *The Cold War: A New History* (New York: Penguin Books, 2005).

⁶⁵ Galeotti, *Hybrid War or Gibridnaya Voyna?*.

vulnerabilities of their adversaries and achieve strategic objectives with minimal direct confrontation⁶⁶.

The integration of these components requires careful planning and coordination. During the annexation of Crimea, Russia combined military operations with cyber attacks and an extensive information campaign. The use of unmarked troops created ambiguity and delayed the international response, while cyber attacks targeted Ukrainian communications and infrastructure. Concurrently, the information campaign shaped public perception and justified the intervention. This coordinated approach allowed Russia to achieve its objectives with limited direct confrontation⁶⁷.

The successful integration of hybrid warfare components also involves exploiting the synergies between different tactics. For instance, cyber operations can support information warfare by hacking into communication networks to obtain and leak sensitive information, thereby influencing public opinion. Similarly, economic sanctions can create internal dissent, which can be further amplified by propaganda and misinformation campaigns. The ability to combine and adapt these tactics to the specific context of the conflict is a hallmark of effective hybrid warfare⁶⁸.

Another example of the integration of hybrid warfare components is the strategy employed by ISIS. The group used a combination of conventional military tactics to seize territory, guerrilla tactics to defend it, and an extensive online propaganda campaign to recruit fighters and spread their ideology. They also leveraged economic resources from captured territories to fund their operations and used cyber warfare to coordinate attacks and communicate securely. This integrated approach allowed ISIS to establish and maintain control over significant regions despite facing superior conventional forces⁶⁹.

Flexible and decentralized leadership models enable rapid decision-making and adjustment to evolving battlefield conditions, allowing for coordinated and timely deployment of diverse tactics. Non-state actors like Hezbollah have demonstrated sophisticated integration of military, political, and social strategies through adaptive command structures, effectively

⁶⁶ Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*.

⁶⁷ Galeotti, *Hybrid War or Gibrinaya Voina?*.

⁶⁸ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

⁶⁹ Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*.

coordinating guerrilla tactics with information and psychological operations to challenge more conventional military forces. Such organizational adaptability enhances resilience and effectiveness, making hybrid warfare strategies more robust against traditional countermeasures⁷⁰.

The integration of hybrid warfare components poses significant challenges for those attempting to counter it. Traditional military responses are often insufficient to address the multifaceted nature of hybrid threats. Effective counter-strategies require a comprehensive approach that combines military, cyber, informational, economic, and diplomatic tools. This necessitates close coordination between different government agencies and international partners, as well as the development of new capabilities and doctrines to address the unique challenges posed by hybrid warfare⁷¹.

Additionally, hybrid warfare's effectiveness lies in its ability to create a multi-layered threat environment where the lines between different types of conflict are blurred. For example, in the ongoing conflict in Eastern Ukraine, Russia's integration of conventional military support, cyber operations, and a well-orchestrated information campaign has created a persistent low-intensity conflict that is challenging for Ukraine and its allies to address effectively⁷².

⁷⁰ Andrew Mumford, *Proxy Warfare* (Cambridge: Polity Press, 2013), 47.

⁷¹ Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*.

⁷² U.S. Government Publishing Office, *The Evolution of Hybrid Warfare and Key Challenges* (Washington, DC: U.S. Government Publishing Office, 2017), 6.

CHAPTER 3

American Strategy and Response to Hybrid Warfare

3.1 Introduction

As the nature of warfare evolves, the United States has had to adapt its strategies and responses to effectively counter the multifaceted threats posed by hybrid warfare. Hybrid warfare poses significant challenges to national security, demanding a comprehensive and adaptive strategy. The United States has recognized the complexity of hybrid threats and has developed multifaceted strategies to counter these challenges.

As hybrid warfare continues to blur the lines between traditional and non-traditional forms of conflict, the U.S. has increasingly focused on the need for an integrated approach that leverages both military and non-military means. This involves not only enhancing the capabilities of the armed forces but also ensuring that diplomatic, economic, and informational tools are effectively employed in a coordinated manner. The complexity of hybrid warfare requires that these various elements of national power work together seamlessly, enabling the U.S. to respond more flexibly and effectively to the diverse range of challenges posed by adversaries⁷³.

Furthermore, the evolving nature of hybrid threats has necessitated a shift in how the U.S. conceptualizes security and defense. The traditional focus on military superiority is increasingly complemented by efforts to strengthen societal resilience, enhance cybersecurity, and counter disinformation. These efforts are essential in ensuring that the U.S. is not only prepared to confront hybrid threats on the battlefield but also in the broader societal and economic domains where these conflicts often play out⁷⁴.

3.2 Current U.S. Defense Strategy

The U.S. defense strategy for countering hybrid warfare is articulated in the 2022 National Defense Strategy (NDS) and the National Security Strategy (NSS). These documents

⁷³ The White House, *National Security Strategy* (Washington, DC: The White House, 2022), 16.

⁷⁴ Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 12.

emphasize integrated deterrence, advanced technological capabilities, and strengthened alliances and partnerships to address hybrid threats. The NDS highlights the importance of maintaining a competitive edge in cyber operations, electronic warfare, and space capabilities, stressing the need for adaptability and resilience in the face of rapidly evolving threats. The NSS complements this by outlining broader national security objectives, emphasizing the importance of whole-of-government approaches to counter hybrid threats. It underscores the need for cooperation with international partners and the importance of enhancing national resilience to withstand and recover from hybrid attacks⁷⁵.

3.2.1 National Defense Strategy

A key component of the NDS is the focus on integrated deterrence, which combines conventional military power with unconventional and non-military tools to deter adversaries. This approach recognizes that hybrid warfare blurs the lines between peace and conflict, requiring a more flexible and adaptive response. The strategy also highlights the need for improved intelligence capabilities to detect and counter hybrid threats early. The U.S. aims to build a more agile and resilient force capable of responding to the diverse challenges of hybrid warfare⁷⁶.

The U.S. places a significant emphasis on cyber capabilities, recognizing that cyber warfare is a critical component of hybrid conflicts. The Department of Defense Cyber Strategy outlines initiatives to defend critical infrastructure, enhance cyber defenses, and develop offensive cyber capabilities to deter and respond to cyber threats. The integration of cyber capabilities into the broader defense strategy reflects the evolving nature of modern warfare⁷⁷.

The 2022 National Defense Strategy also emphasizes the role of forward-deployed forces and prepositioned equipment in deterring and responding to hybrid threats. By maintaining a strong presence in key regions, the U.S. can quickly respond to emerging threats and support its allies in countering hybrid warfare tactics. This approach is particularly

⁷⁵ U.S. Department of Defense, *National Defense Strategy of the United States of America: 2022*, (Washington, DC: Department of Defense, 2022), 10.

⁷⁶ Ibid.

⁷⁷ Ibid.

important in regions like Eastern Europe and the Indo-Pacific, where the presence of U.S. forces serves as a deterrent against adversaries employing hybrid tactics⁷⁸.

Furthermore, the emphasis on alliances and partnerships in the NDS is critical for countering hybrid warfare effectively. By strengthening ties with NATO and other international allies, the U.S. enhances its collective defense posture, ensuring that it can respond to hybrid threats across different regions. This approach also includes efforts to improve the interoperability of allied forces and to conduct joint exercises that simulate hybrid warfare scenarios, thereby preparing for the complex nature of these threats⁷⁹.

The NDS also stresses the importance of technological innovation and adaptation in maintaining a strategic advantage in hybrid warfare. The U.S. military is increasingly investing in emerging technologies such as artificial intelligence, autonomous systems, and quantum computing to enhance its capabilities in areas like cybersecurity, electronic warfare, and intelligence gathering. These investments are designed to ensure that the U.S. remains at the forefront of technological advancements, which are crucial in the dynamic environment of hybrid warfare⁸⁰.

3.2.2 National Security Strategy

In addition, the National Security Strategy highlights the importance of defending the U.S. homeland against hybrid threats, particularly in the cyber and information domains. The strategy outlines measures to protect critical infrastructure from cyber attacks, enhance the resilience of democratic institutions against disinformation, and improve the ability of U.S. society to withstand and recover from hybrid warfare tactics. This comprehensive approach reflects the recognition that hybrid warfare targets not only military assets but also civilian and governmental structures, requiring a whole-of-society response⁸¹.

Hybrid threats pose significant challenges to American infrastructure, targeting critical systems that are essential for national security, economic stability, and public safety. These threats often combine cyberattacks, disinformation, and physical sabotage to exploit

⁷⁸ Ibid, 23.

⁷⁹ Ibid, 50.

⁸⁰ Ibid.

⁸¹ The White House, *National Security Strategy* (Washington, DC: The White House, 2022), 45.

vulnerabilities in sectors such as energy, transportation, financial services, and communications. The increasing interconnectivity of these infrastructures, driven by advancements in digital technology, has created new opportunities for adversaries to disrupt essential services and sow confusion.

The energy sector, particularly the power grid, is one of the most vulnerable to hybrid threats. A successful cyberattack on the electrical grid could result in widespread power outages, crippling other critical infrastructures that depend on electricity, such as water treatment plants, hospitals, and communication networks. The U.S. power grid's aging infrastructure and its dependence on digital control systems make it a prime target for cyber operations that could be part of a broader hybrid strategy aimed at destabilizing the country.

Similarly, the financial services sector is highly susceptible to hybrid threats, particularly cyberattacks. These threats can disrupt financial markets, compromise sensitive data, and erode public trust in the financial system. The financial sector's reliance on complex and interconnected networks makes it vulnerable to coordinated attacks that combine cyber operations with misinformation campaigns designed to induce panic and instability.

Transportation systems, including air traffic control and rail networks, also face significant risks from hybrid threats. The potential for cyberattacks to disrupt these systems could have cascading effects on the economy and public safety. Adversaries can exploit these vulnerabilities through a mix of cyber operations and physical sabotage, creating widespread disruption and fear.

In summary, hybrid threats to American infrastructure are diverse and multifaceted, targeting the very systems that underpin the nation's security and economic well-being. Addressing these vulnerabilities requires a comprehensive approach that integrates cybersecurity, infrastructure resilience, and coordinated responses across multiple sectors.

3.3 Doctrine and Policies

The U.S. military has developed several doctrines and policies to address the complexities of hybrid warfare. The Joint Publication 3-0 (JP 3-0), Joint Operations, provides a framework for integrating conventional and unconventional operations to achieve strategic

objectives. This doctrine emphasizes the need for joint operations across different domains, including land, sea, air, space, and cyberspace, to effectively counter hybrid threats⁸².

The U.S. Army's Field Manual 3-24 (FM 3-24), Counterinsurgency, is another critical document that outlines strategies for dealing with irregular warfare and insurgencies, which are key components of hybrid warfare. This manual highlights the importance of understanding the operational environment, building relationships with local populations, and integrating military and civilian efforts to achieve long-term stability⁸³. The principles outlined in FM 3-24 are essential for addressing the unconventional aspects of hybrid warfare.

Additionally, the Department of Defense has developed the Defense Cyber Strategy, which outlines the steps needed to secure U.S. cyber infrastructure and respond to cyber threats. This strategy emphasizes the need for a proactive defense posture, including the development of offensive cyber capabilities and the integration of cyber operations into broader military campaigns. The Defense Cyber Strategy reflects the increasing importance of cyberspace in contemporary hybrid conflicts⁸⁴.

The 2014 Quadrennial Defense Review also highlights the importance of adapting U.S. military doctrines to address the challenges of hybrid warfare. The QDR emphasizes the need for joint force adaptability and innovation in countering hybrid threats, which often involve a combination of conventional, irregular, and asymmetric tactics. The review calls for the development of new operational concepts and the integration of emerging technologies to enhance the U.S. military's ability to respond to hybrid warfare⁸⁵.

Another significant policy development in addressing hybrid threats is the emphasis on resilience and adaptability within military doctrines. This includes enhancing the ability of U.S. forces to operate in contested environments where adversaries may employ a mix of conventional, unconventional, and cyber tactics. The development of new doctrines that

⁸² Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations* (Washington, DC: Joint Chiefs of Staff, 2017).

⁸³ Department of the Army, *Field Manual 3-24: Counterinsurgency* (Washington, DC: Department of the Army, 2014).

⁸⁴ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018).

⁸⁵ U.S. Department of Defense, *Quadrennial Defense Review 2014* (Washington, DC: U.S. Department of Defense, 2014), 37.

emphasize adaptability, such as the Multi-Domain Operations concept, is crucial in preparing U.S. forces to respond to the complex and rapidly changing nature of hybrid warfare⁸⁶.

3.4 Case Studies

3.4.1 Ukraine and Russian Hybrid Warfare

The U.S. response to Russian hybrid warfare in Ukraine provides a significant case study. Following Russia's annexation of Crimea in 2014 and its support for separatist movements in Eastern Ukraine, the U.S. implemented a range of measures to counter Russian aggression. These measures included economic sanctions, diplomatic efforts to isolate Russia, and military assistance to Ukraine⁸⁷.

The U.S. provided Ukraine with non-lethal military aid, such as communications equipment, body armor, and medical supplies. In 2017, the U.S. expanded its support to include lethal aid, such as Javelin anti-tank missiles. This assistance aimed to enhance Ukraine's defensive capabilities and deter further Russian aggression. Additionally, the U.S. conducted joint military exercises with NATO allies in Eastern Europe to demonstrate its commitment to regional security⁸⁸. These actions reflect the U.S. strategy of combining military support with economic and diplomatic measures to counter hybrid threats.

In the cyber domain, the U.S. has worked to improve Ukraine's cyber defenses and resilience against Russian cyber attacks. This includes providing technical assistance, sharing intelligence on cyber threats, and supporting efforts to secure critical infrastructure. The U.S. has also imposed sanctions on Russian individuals and entities involved in cyber operations, signaling a strong stance against cyber aggression. The comprehensive U.S. response to Russian hybrid warfare in Ukraine demonstrates the importance of a multifaceted approach⁸⁹.

There were significant efforts to strengthen Ukraine's information environment. The U.S. provided support for Ukrainian media outlets and civil society organizations to

⁸⁶ U.S. Department of Defense, *National Defense Strategy of the United States of America: 2022*, (Washington, DC: Department of Defense, 2022), 74.

⁸⁷ Galeotti, *Hybrid War or Gibrinaya Voyna?*.

⁸⁸ *Ibid.*

⁸⁹ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

counter Russian disinformation campaigns. This included training journalists, supporting fact-checking initiatives, and promoting media literacy among the Ukrainian population. These efforts were aimed at building resilience against Russian information operations and ensuring that the Ukrainian public had access to accurate and reliable information⁹⁰.

Additionally, the U.S. has focused on enhancing the interoperability of Ukrainian forces with NATO through joint exercises and training programs. By improving the capabilities of the Ukrainian military and aligning their operations with NATO standards, the U.S. has sought to bolster Ukraine's ability to defend itself against Russian aggression. This approach reflects the U.S. strategy of not only providing direct military aid but also building long-term capacity and resilience in partner nations facing hybrid threats⁹¹.

The U.S. has also taken steps to counter Russia's hybrid warfare by increasing its presence in Eastern Europe. This includes the deployment of additional troops and the establishment of forward operating bases to deter further Russian aggression. The U.S. has also expanded its intelligence-sharing arrangements with European allies to better detect and respond to Russian hybrid tactics. These measures are intended to reassure NATO allies and demonstrate U.S. commitment to collective security in the face of hybrid threats⁹².

3.4.2 Middle East: ISIS and Hybrid Warfare

The U.S. response to the hybrid warfare tactics of ISIS in the Middle East represents another critical case study. ISIS employed a blend of conventional military tactics, guerrilla warfare, and sophisticated information operations to seize and control territory in Iraq and Syria. The group's use of social media for propaganda and recruitment was particularly effective, drawing foreign fighters to its cause and spreading its ideology globally⁹³.

To counter ISIS, the U.S. adopted a strategy that combined military action with efforts to undermine the group's ideological appeal. Operation Inherent Resolve, the U.S.-led coalition campaign against ISIS, involved airstrikes, special operations, and support for local

⁹⁰ Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 19.

⁹¹ Ibid.

⁹² U.S. Department of Defense, *National Defense Strategy of the United States of America: 2022*, (Washington, DC: Department of Defense, 2022), 84.

⁹³ Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*.

ground forces, including the Iraqi Security Forces and the Syrian Democratic Forces. This military effort aimed to degrade ISIS's capabilities, reclaim territory, and disrupt its operations⁹⁴.

In addition to military action, the U.S. focused on countering ISIS's information operations. This included efforts to counteract ISIS propaganda on social media, disrupt the group's online recruitment networks, and promote counter-narratives to undermine its ideological appeal. The U.S. also worked with international partners to cut off ISIS's financial resources, including targeting oil revenue and other sources of funding. The U.S. strategy against ISIS highlights the importance of addressing both the physical and informational dimensions of hybrid warfare⁹⁵.

The U.S. also included efforts to rebuild and stabilize regions liberated from ISIS control. This involved not only military operations but also the provision of humanitarian aid, reconstruction efforts, and support for local governance structures. By addressing the underlying conditions that allowed ISIS to thrive, the U.S. aimed to prevent the resurgence of the group and promote long-term stability in the region⁹⁶.

Furthermore, the U.S. strategy against ISIS emphasized the importance of international cooperation. The Global Coalition to Defeat ISIS, which includes more than 80 countries, played a crucial role in coordinating military, diplomatic, and financial efforts against the group. This coalition-based approach allowed the U.S. to leverage the strengths and resources of its partners, enhancing the overall effectiveness of the campaign against ISIS and demonstrating the importance of alliances in countering hybrid threats⁹⁷.

The U.S. has also prioritized efforts to counter the financing of terrorism as part of its strategy against ISIS. This involved targeting the group's revenue streams, such as oil smuggling, extortion, and kidnapping for ransom. The U.S. worked closely with international partners to disrupt these financial networks and to ensure that ISIS could no longer generate the

⁹⁴ Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (1st quarter 2009): 37.

⁹⁵ Kathleen J. McInnis, *Coalition Contributions to Countering the Islamic State* (Washington, DC: Congressional Research Service, 2016).

⁹⁶ The White House, *National Security Strategy* (Washington, DC: The White House, 2022), 56.

⁹⁷ Frank Hoffman, Colonel Matt Neumeier, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 25.

resources needed to sustain its operations. This financial warfare aspect of the U.S. strategy was crucial in weakening ISIS's ability to wage hybrid warfare⁹⁸.

In addition, the U.S. has focused on countering the ideological appeal of ISIS through strategic communications. This involved working with local and international partners to promote narratives that countered the extremist ideology of ISIS and to highlight the negative consequences of joining the group. By undermining ISIS's recruitment efforts and reducing its influence online, the U.S. aimed to diminish the group's ability to attract new followers and sustain its operations⁹⁹.

3.5 Strengths and Weaknesses

3.5.1 Strengths

One of the primary strengths of the U.S. strategy in countering hybrid warfare is its comprehensive and integrated approach. By combining military, economic, diplomatic, and informational tools, the U.S. can address the multifaceted nature of hybrid threats. This holistic approach allows for greater flexibility and adaptability in responding to different aspects of hybrid warfare¹⁰⁰.

The emphasis on alliances and partnerships is another significant strength of the U.S. strategy. By working closely with NATO and other international partners, the U.S. can leverage a broader range of capabilities and resources. Joint military exercises, intelligence sharing, and coordinated diplomatic efforts enhance the collective ability to counter hybrid threats and deter adversaries¹⁰¹.

The U.S. also benefits from its advanced technological capabilities, particularly in the cyber domain. The development of sophisticated cyber defenses and offensive cyber capabilities allows the U.S. to protect its critical infrastructure, respond to cyber attacks, and

⁹⁸ U.S. Government Publishing Office, *The Evolution of Hybrid Warfare and Key Challenges* (Washington, DC: U.S. Government Publishing Office, 2017), 42.

⁹⁹ U.S. Department of Defense, *National Defense Strategy of the United States of America: 2022*, (Washington, DC: Department of Defense, 2022), 102.

¹⁰⁰ Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*.

¹⁰¹ Gaddis, *The Cold War: A New History*.

disrupt adversaries' operations. The integration of cyber operations into broader military campaigns is a key strength in addressing the cyber component of hybrid warfare¹⁰².

Another strength of the U.S. strategy is its focus on adaptability and innovation. The U.S. military has invested heavily in research and development to ensure that it can respond to emerging threats and leverage new technologies effectively. This commitment to innovation is critical in the context of hybrid warfare, where adversaries constantly develop new tactics and tools. The U.S. military's investment in cutting-edge technologies, such as artificial intelligence, autonomous systems, and cyber capabilities, ensures that it remains at the forefront of innovation in warfare. The ability to quickly adapt to these changes and incorporate new capabilities into military operations gives the U.S. a significant advantage¹⁰³.

The U.S. strategy also emphasizes the importance of resilience, both in terms of military capabilities and societal resilience. The recognition that hybrid warfare targets not just military assets but also civilian infrastructure and public morale has led to efforts to enhance the resilience of U.S. society. This includes improving the security of critical infrastructure, promoting media literacy to counter disinformation, and fostering public awareness of hybrid threats. By building resilience across multiple domains, the U.S. strengthens its overall defense against hybrid warfare¹⁰⁴.

Furthermore, the U.S. strategy benefits from its ability to project power globally, allowing it to respond to hybrid threats wherever they may arise. This global reach is supported by a network of alliances, forward-deployed forces, and prepositioned equipment, enabling the U.S. to quickly mobilize and respond to emerging threats. This capacity for rapid response is a key advantage in countering the often unpredictable and dynamic nature of hybrid warfare¹⁰⁵.

3.5.2 Weaknesses

Despite these strengths, there are several weaknesses and challenges in the U.S. strategy for countering hybrid warfare. One significant weakness is the difficulty in identifying

¹⁰² Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹⁰³ U.S. Department of Defense, *National Defense Strategy of the United States of America: 2022*, (Washington, DC: Department of Defense, 2022), 68.

¹⁰⁴ The White House, *National Security Strategy* (Washington, DC: The White House, 2022), 72.

¹⁰⁵ U.S. Department of Defense, *National Defense Strategy of the United States of America: 2022*, (Washington, DC: Department of Defense, 2022), 86.

and attributing hybrid warfare attacks. The covert and ambiguous nature of hybrid tactics makes it challenging to determine the responsible actors and develop an appropriate response. This ambiguity can delay decision-making and complicate efforts to build international consensus for action¹⁰⁶.

Another challenge is the need for better interagency coordination. Hybrid warfare requires a coordinated response from multiple government agencies, including the Department of Defense, the State Department, intelligence agencies, and others. Ensuring effective communication and collaboration between these agencies can be difficult, leading to potential gaps and inefficiencies in the response¹⁰⁷.

The rapid pace of technological advancements also poses a challenge. Adversaries continuously develop new tactics and tools, particularly in the cyber and information domains. The U.S. must remain agile and adaptive to keep pace with these developments and ensure that its defenses and strategies are effective. This requires ongoing investment in research and development, as well as continuous updates to military doctrines and training programs¹⁰⁸.

There is a need for greater resilience against hybrid threats. This includes not only military and cyber resilience but also societal resilience. Building public awareness of hybrid threats, enhancing media literacy, and promoting social cohesion are essential for countering the psychological and informational components of hybrid warfare. Ensuring that society can withstand and recover from hybrid attacks is crucial for maintaining national security¹⁰⁹.

Moreover, the complexity of hybrid warfare makes it difficult to develop a one-size-fits-all strategy. Each hybrid threat is unique, with different actors, tactics, and objectives. This requires the U.S. to tailor its responses to each specific threat, which can be resource-

¹⁰⁶ Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*.

¹⁰⁷ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

¹⁰⁸ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹⁰⁹ Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*.

intensive and time-consuming. The need for tailored responses can also strain the U.S. military and intelligence agencies, which must constantly adapt to new challenges and environments¹¹⁰.

Another weakness in the U.S. strategy is the challenge of coordinating with international partners in countering hybrid threats. While alliances and partnerships are a strength, they also present challenges in terms of aligning strategies, sharing intelligence, and conducting joint operations. Differences in capabilities, legal frameworks, and political will among allies can complicate efforts to mount a unified response to hybrid threats, potentially undermining the overall effectiveness of the strategy¹¹¹.

The U.S. strategy also faces challenges related to the balance between offensive and defensive operations in the cyber domain. While the U.S. has developed significant offensive cyber capabilities, there is ongoing debate about how and when to use these tools in the context of hybrid warfare. The challenge lies in deterring adversaries without escalating conflicts, as well as in ensuring that offensive operations do not inadvertently expose vulnerabilities in U.S. cyber defenses¹¹².

Finally, the U.S. strategy faces challenges in sustaining long-term commitment and focus on hybrid threats. Hybrid warfare often involves protracted conflicts that require sustained attention and resources. However, shifting political priorities and budget constraints can lead to fluctuations in U.S. engagement and support for counter-hybrid warfare efforts. Ensuring consistent and sustained efforts to counter hybrid threats is essential for maintaining the effectiveness of U.S. strategy¹¹³.

¹¹⁰ U.S. Government Publishing Office, *The Evolution of Hybrid Warfare and Key Challenges* (Washington, DC: U.S. Government Publishing Office, 2017), 46.

¹¹¹ U.S. Department of Defense, *National Defense Strategy of the United States of America: 2022*, (Washington, DC: Department of Defense, 2022), 98.

¹¹² Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 43.

¹¹³ U.S. Department of Defense, *Quadrennial Defense Review 2014* (Washington, DC: U.S. Department of Defense, 2014), 88.

CHAPTER 4

Challenges in Countering Hybrid Warfare

4.1 Introduction

Hybrid warfare presents a complex and evolving challenge that blurs the lines between conventional and unconventional conflict, cyber operations, information warfare, and economic coercion. The United States and its allies face significant hurdles in effectively countering these threats. This chapter examines key challenges in countering hybrid warfare, including identification and attribution, interagency coordination, technological and intelligence gaps, legal and ethical considerations, strategic adaptations and innovations, international cooperation and legal frameworks, and societal resilience and public awareness.

Hybrid warfare's complexity is exacerbated by the rapid technological advancements that allow adversaries to employ increasingly sophisticated tactics. The convergence of cyber capabilities, artificial intelligence, and automated systems has given rise to new forms of attack that are difficult to detect and counter. As these technologies continue to evolve, the U.S. must continually adapt its strategies to mitigate the risks posed by hybrid threats. This requires not only an understanding of the current landscape but also foresight into future developments that could further complicate the security environment¹¹⁴.

Moreover, the decentralized nature of hybrid warfare means that attacks can be launched from multiple fronts, often simultaneously. This multi-vector approach complicates defense strategies, as it requires a coordinated response across various domains, including military, cyber, economic, and informational. The U.S. must develop an integrated approach that can address the full spectrum of hybrid threats, ensuring that responses are not only reactive but also proactive in anticipating and mitigating potential risks¹¹⁵.

¹¹⁴ Andrew Mumford, *Proxy Warfare* (Cambridge: Polity Press, 2013), 47.

¹¹⁵ The White House, *National Security Strategy* (Washington, DC: The White House, 2022), 16.

4.2 Identification and Attribution

One of the most significant challenges in countering hybrid warfare is the difficulty in identifying and attributing attacks to specific actors. Hybrid warfare tactics often involve covert operations, cyber attacks, and disinformation campaigns designed to create ambiguity and confusion. This deliberate obfuscation makes it challenging for states to determine the responsible parties and develop appropriate responses¹¹⁶.

Attributing hybrid warfare attacks to specific actors involves gathering and analyzing diverse types of evidence, including intelligence reports, digital forensics, and human sources. The covert nature of hybrid operations often means that the available evidence is fragmented and circumstantial. This can lead to delays in attribution and challenges in building a clear and convincing case against the perpetrators. The distinction between state and non-state actors in hybrid warfare further complicates attribution. Hybrid operations frequently involve proxies, such as militia groups or cyber mercenaries, who act on behalf of a state but maintain a degree of operational independence. This allows the sponsoring state to distance itself from the actions of these proxies and deny direct involvement¹¹⁷.

For instance, cyber attacks, a key component of hybrid warfare, can be launched from anywhere in the world, often using sophisticated techniques to mask the origin of the attack. The use of proxy servers, botnets, and other anonymizing tools complicates the process of tracing the source of the attack. This was evident in the cyber attacks on Estonia in 2007, where the attribution to Russian actors took considerable time and effort, delaying the international response. The challenge of attribution in cyber warfare highlights the need for improved cyber forensics and international cooperation. Effective attribution is crucial for developing a coordinated response and deterring future hybrid attacks. However, the covert and decentralized nature of hybrid warfare tactics requires advanced technological capabilities and robust intelligence networks. Enhancing these capabilities is essential for improving the identification and attribution of hybrid threats¹¹⁸.

¹¹⁶ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹¹⁷ Pavel Felgenhauer, "A New Version of the 'Gerasimov Doctrine'?" *Eurasia Daily Monitor* 16, no.32 (2019):15.

¹¹⁸ Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

Furthermore, the role of AI in enhancing attribution capabilities is gaining attention. AI can analyze large datasets and detect patterns that might be missed by human analysts, thereby improving the speed and accuracy of attribution. However, there are also concerns about the potential misuse of AI in this context, such as the possibility of false attribution or escalation due to automated decision-making processes. As such, the integration of AI into attribution efforts must be carefully managed to avoid unintended consequences¹¹⁹.

The annexation of Crimea and the subsequent conflict in Eastern Ukraine are prime examples of the challenges in identification and attribution in hybrid warfare. The use of unmarked soldiers and local proxies allowed Russia to maintain plausible deniability, complicating efforts to attribute the actions to the Russian state conclusively. International responses were delayed as evidence was gathered and analyzed to build a convincing case against Russia¹²⁰.

Another example of these challenges, is the Russian interference in the 2016 U.S. presidential election. The use of cyber-attacks and social media manipulation to influence the election outcome demonstrated how hybrid tactics could be employed to destabilize democratic processes without triggering a traditional military response. The subsequent investigations revealed the complexity of attributing such actions directly to the Russian state, highlighting the challenges the U.S. faces in deterring similar future threats¹²¹.

4.3 Interagency Coordination

Another significant challenge in countering hybrid warfare is the need for effective interagency coordination. Hybrid warfare requires a coordinated response from multiple government agencies, including the Department of Defense, the State Department, intelligence agencies, and others. Ensuring effective communication and collaboration between these agencies can be difficult, leading to potential gaps and inefficiencies in the response¹²².

¹¹⁹ Galeotti, Hybrid War or Gibridnaya Voina?, 78.

¹²⁰ Johann Schmid, "Hybrid Warfare on the Ukrainian Battlefield: Developing Theory Based on Empirical Evidence," *Journal on Baltic Security* 5, no. 1 (2019): 5.

¹²¹ Hoffman, Frank G. "Hybrid Warfare and Challenges." *Military Review* 89, no. 3 (2009): 44-45.

¹²² U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

The complexity of hybrid warfare necessitates a whole-of-government approach, where military, diplomatic, economic, and informational tools are integrated into a cohesive strategy. This requires not only interagency cooperation but also collaboration with international allies and partners. The U.S. response to Russian hybrid warfare in Ukraine, for example, involved coordination between the Department of State, the Department of Defense, intelligence agencies, and NATO allies. Despite these efforts, challenges in communication and coordination sometimes hampered the effectiveness of the response¹²³.

Effective interagency coordination also involves overcoming bureaucratic silos and fostering a culture of collaboration. This requires clear lines of communication, shared goals, and joint training exercises to build trust and understanding between different agencies. The establishment of interagency task forces and liaison offices can facilitate better coordination and improve the overall response to hybrid threats¹²⁴.

The need for improved interagency coordination extends to the private sector as well. Many critical infrastructure systems, such as energy, finance, and communications, are owned and operated by private companies. Coordinating with these entities to enhance cybersecurity, share intelligence, and develop joint response plans is essential for addressing the multifaceted nature of hybrid warfare¹²⁵.

4.4 Technological and Intelligence Gaps

Addressing technological and intelligence gaps is crucial for countering hybrid warfare effectively. Adversaries continuously develop new tactics and tools, particularly in the cyber and information domains. The U.S. must remain agile and adaptive to keep pace with these developments and ensure that its defenses and strategies are effective. This requires ongoing investment in research and development, as well as continuous updates to military doctrines and training programs¹²⁶.

The rapid pace of technological advancements presents both opportunities and challenges. While new technologies can enhance defensive capabilities, they also provide

¹²³ Galeotti, *Hybrid War or Gibridnaya Voina?*.

¹²⁴ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

¹²⁵ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹²⁶ *Ibid.*

adversaries with novel ways to conduct hybrid warfare. For example, the proliferation of AI and machine learning can be leveraged for cyber attacks, deepfake videos, and automated disinformation campaigns. Keeping up with these technological advancements requires a robust innovation ecosystem and collaboration with the private sector¹²⁷.

Intelligence gaps pose another significant challenge. Effective counter-hybrid warfare strategies depend on timely and accurate intelligence to detect, attribute, and respond to threats. However, gathering intelligence on hybrid warfare activities, especially those conducted by non-state actors or through covert means, is inherently difficult. Enhancing intelligence capabilities involves improving Human Intelligence, Signals Intelligence, and Cyber Intelligence to provide a comprehensive understanding of hybrid threats¹²⁸.

This challenge is not new. During the Cold War, the United States faced significant intelligence gaps in understanding and countering Soviet espionage and influence operations. The Soviet Union employed a wide range of hybrid tactics, including the use of disinformation (dezinformatsiya), which the U.S. struggled to counter effectively. Today, similar gaps are evident in the U.S.'s ability to counter cyber intrusions and disinformation campaigns by state and non-state actors. The decentralized nature of hybrid threats, which can involve state actors, criminal networks, and private entities, complicates the intelligence-gathering process. The U.S. intelligence community has struggled to keep pace with these evolving threats, as evidenced by the gaps in detecting and responding to foreign cyber interference in domestic affairs¹²⁹.

The integration of big data analytics and AI into intelligence operations can help address some of these gaps. Advanced data analytics can process vast amounts of information to identify patterns and anomalies indicative of hybrid warfare activities. AI can assist in predictive analysis, helping to anticipate potential threats and inform proactive measures. However, the use of these technologies must be balanced with ethical considerations and the protection of civil liberties¹³⁰.

¹²⁷ Rid, *Cyber War Will Not Take Place*.

¹²⁸ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

¹²⁹ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats – a European Union Response*, JOIN(2016) 18 final (Brussels, April 6, 2016), 1-18.

¹³⁰ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

4.5 Legal and Ethical Considerations

Navigating legal and ethical considerations is a critical aspect of countering hybrid warfare. The unconventional and covert nature of hybrid tactics often blurs the lines between peacetime and wartime activities, complicating the legal frameworks governing state responses. Ensuring that responses to hybrid threats comply with domestic and international laws is essential to maintain legitimacy and avoid unintended consequences¹³¹.

Traditional legal frameworks, like those under international humanitarian law, are primarily designed for conventional warfare, leaving a gap when it comes to actions that fall in the gray zones of conflict, such as cyber operations and misinformation campaigns. For instance, current U.S. laws struggle to directly address issues related to social media, intellectual property, and privacy in the context of hybrid warfare. As hybrid threats often involve non-state actors and activities that blur the lines between civilian and military targets, the legal framework must evolve to adequately protect both national security and civil liberties¹³².

One of the primary legal challenges is the application of international law to cyber warfare. The Tallinn Manual on the International Law Applicable to Cyber Warfare provides a comprehensive analysis of how existing international laws apply to cyber operations. However, the manual acknowledges that there are still many unresolved issues and gray areas. For instance, determining whether a cyber attack constitutes an "armed attack" under the United Nations Charter Article 51, which would justify a self-defense response, remains contentious¹³³.

The use of offensive cyber operations also raises ethical concerns. While offensive capabilities can deter adversaries and disrupt their operations, they can also escalate conflicts and cause unintended collateral damage. Ensuring that such operations adhere to the principles of necessity, proportionality, and distinction is crucial to minimize harm to civilians and maintain ethical standards in warfare¹³⁴.

¹³¹ Rid, *Cyber War Will Not Take Place*.

¹³² NC State University Libraries, "Legal and Ethical Implications," *Social Media Archives Toolkit*, 2023, <https://www.lib.ncsu.edu/social-media-archives-toolkit/legal>.

¹³³ Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

¹³⁴ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

Information warfare poses additional ethical dilemmas. Disinformation campaigns, while effective in undermining adversaries, can erode trust in public institutions and contribute to societal polarization. Countering disinformation without infringing on freedom of speech and press is a delicate balance. Developing ethical guidelines for information operations and promoting transparency and accountability in government communications are essential steps in addressing these challenges¹³⁵.

Moreover, the use of AI and autonomous systems in military operations raises significant concerns. These systems, which can make decisions without human intervention, raise questions about accountability and the potential for unintended consequences. As these technologies become more advanced, the ethical implications of their use in warfare become more pressing. Issues such as the moral agency of AI systems, the potential for unintended harm, and the transparency of decision-making processes are at the forefront of the debate. The U.S. must consider whether AI systems can be held accountable for their actions and how to ensure that their deployment in warfare aligns with ethical standards that protect human rights and maintain public trust¹³⁶.

United States faces substantial legal and ethical challenges in the realm of hybrid warfare, particularly as technological advancements outpace the development of corresponding legal and ethical frameworks. Addressing these challenges will require a concerted effort to update laws, establish clear ethical guidelines, and ensure that new technologies are used responsibly in a way that safeguards both national security and fundamental rights.

4.6 Strategic Adaptations and Innovations

To overcome the challenges posed by hybrid warfare, the U.S. must continuously adapt and innovate its strategies. This involves not only improving current capabilities but also anticipating future threats and developing proactive measures. Enhancing resilience across military, cyber, informational, economic, and societal domains is critical for countering the multifaceted nature of hybrid threats¹³⁷.

¹³⁵ Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*.

¹³⁶ Jakob Mökander, "Auditing of AI: Legal, Ethical and Technical Approaches," *Digital Society 2* (2023): 49, <https://doi.org/10.1007/s44206-023-00074-y>.

¹³⁷ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

Investing in research and development is essential to keep pace with technological advancements. Public-private partnerships can foster innovation and accelerate the development of new defense technologies. For example, the Defense Advanced Research Projects Agency (DARPA) has been instrumental in pioneering cutting-edge technologies that have significant applications in hybrid warfare. Collaborating with tech companies and academic institutions can enhance the U.S. military's technological edge¹³⁸.

Training and education are also vital components of strategic adaptation. Preparing military personnel and civilian leaders to understand and respond to hybrid threats requires comprehensive training programs that cover the full spectrum of hybrid warfare tactics. Joint training exercises with international allies can enhance interoperability and build collective resilience. Incorporating hybrid warfare scenarios into military exercises helps to identify weaknesses and improve response strategies¹³⁹.

Developing a strategic communications framework is crucial for countering information warfare. This involves not only defending against disinformation but also proactively shaping narratives to support national security objectives. Building public awareness of hybrid threats and promoting media literacy can help mitigate the impact of disinformation campaigns. Engaging with the media and leveraging social media platforms to communicate transparently and effectively with the public are essential elements of a robust strategic communications strategy¹⁴⁰.

4.7 International Cooperation and Legal Frameworks

Given the transnational nature of hybrid threats, international cooperation is vital for effective countermeasures. No single nation can counter hybrid warfare effectively on its own, particularly when adversaries operate across borders and utilize global networks to achieve their objectives. International cooperation is a cornerstone of effective responses to hybrid warfare. Given the transnational nature of hybrid threats, collaborative efforts with allies and partners are essential to enhance collective security. NATO's adoption of the "Comprehensive Approach" to hybrid threats underscores the importance of integrating military and non-military

¹³⁸ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹³⁹ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

¹⁴⁰ Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*.

tools in response strategies. NATO has established centers of excellence, such as the Cooperative Cyber Defence Centre of Excellence, to enhance capabilities and share best practices among member states¹⁴¹.

Establishing clear legal frameworks and norms for hybrid warfare is also critical. While existing international laws provide some guidance, there is a need for updated frameworks that address the unique challenges of hybrid conflicts. Efforts such as the Tallinn Manual on the International Law Applicable to Cyber Warfare and the development of international agreements on cyber norms are steps in the right direction. Promoting international consensus on these issues can help to establish clearer rules and reduce the risk of escalation¹⁴².

Engaging with international organizations, such as the United Nations and the European Union, can also enhance efforts to counter hybrid warfare. These organizations can facilitate coordination, provide platforms for dialogue, and support capacity-building initiatives. For example, the EU's creation of the Hybrid Fusion Cell within its intelligence analysis center aims to improve the detection and response to hybrid threats by enhancing information sharing and analysis among member states¹⁴³.

4.8 Societal Resilience and Public Awareness

Building societal resilience is a critical component of countering hybrid warfare. This involves enhancing the capacity of communities and institutions to withstand and recover from hybrid attacks. Promoting public awareness of hybrid threats and fostering a culture of resilience can help mitigate the impact of disinformation campaigns and other hybrid tactics. Public awareness campaigns should focus on educating citizens about the nature of hybrid warfare and the tactics used by adversaries. This includes promoting media literacy, encouraging critical thinking, and providing tools to identify and counter disinformation. Schools, community organizations, and media outlets can play a vital role in these efforts by incorporating media literacy programs and facilitating discussions on hybrid threats¹⁴⁴.

¹⁴¹ NATO, *Hybrid Threats: A Strategic Challenge* (Brussels: NATO, 2024).

¹⁴² Schmitt, ed., *Tallinn Manual 2.0 on the International Law*.

¹⁴³ European Commission, *Joint Framework on Countering Hybrid Threats*.

¹⁴⁴ Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*.

Strengthening the resilience of critical infrastructure is also essential. Ensuring that essential services, such as energy, water, transportation, and communications, can continue to operate during hybrid attacks is crucial for maintaining societal stability. This requires robust cybersecurity measures, redundant systems, and contingency planning to mitigate the impact of disruptions. Engaging the private sector in resilience-building efforts is vital, given that many critical infrastructure systems are privately owned and operated. Public-private partnerships can enhance information sharing, improve cybersecurity practices, and develop joint response plans. Establishing frameworks for collaboration and incentivizing private sector investments in resilience can help build a more robust defense against hybrid threats¹⁴⁵.

During the Cold War, the U.S. government launched public awareness campaigns to educate citizens about the threat of communism and promote resilience against Soviet propaganda. This historical effort mirrors contemporary initiatives aimed at building resilience against hybrid threats. The U.S. government has launched several initiatives aimed at building public resilience, such as promoting media literacy and improving the public's ability to recognize and resist disinformation. However, these efforts face significant challenges, including political polarization and widespread mistrust in the media. Building societal resilience against hybrid threats in the U.S. is a long-term process that requires sustained investment and coordination across multiple sectors, including government, civil society, and the private sector¹⁴⁶.

¹⁴⁵ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹⁴⁶ U.S. Government Publishing Office, *The Evolution of Hybrid Warfare and Key Challenges* (Washington, DC: U.S. Government Publishing Office, 2017).

CHAPTER 5

U.S. Strategic Adaptations and Recommendations

5.1 Introduction

The United States faces a multifaceted and evolving threat landscape characterized by the integration of conventional and unconventional tactics, cyber warfare, information warfare, and economic manipulation, collectively known as hybrid warfare. To effectively counter these threats, the U.S. must adapt its strategic framework, incorporating technological advancements, robust training programs, and enhanced resilience mechanisms.

In this context, the role of hybrid warfare as a tool of statecraft has become increasingly prominent. Adversaries like Russia have successfully employed hybrid strategies to undermine and destabilize regions without triggering a full-scale military response. The 2014 annexation of Crimea and ongoing conflicts in Eastern Europe exemplify the effectiveness of hybrid tactics in achieving political objectives while avoiding direct military confrontation¹⁴⁷.

Therefore, the U.S. must recalibrate its strategic framework to address these evolving challenges, recognizing that hybrid warfare will likely remain a central component of global conflicts in the foreseeable future. This chapter outlines specific policy changes, technological advancements, training and education initiatives, international cooperation strategies, public-private sector collaboration, and measures to increase resilience against hybrid attacks.

5.2 Policy Recommendations

Effective policy changes are fundamental to addressing the challenges posed by hybrid warfare. One critical policy recommendation is the establishment of a centralized coordinating body within the U.S. government dedicated to hybrid warfare. This body would facilitate interagency coordination, streamline responses, and ensure that all relevant departments and

¹⁴⁷ Robert Person, Isak Kulalic, and John Mayle, "Back to the Future: The Persistent Problems of Hybrid War," *International Affairs* 100, no. 4 (2024): 1751.

agencies are aligned in their efforts. Such an entity could enhance the effectiveness of responses by providing a unified command structure and clear lines of communication¹⁴⁸.

Additionally, updating existing military doctrines to reflect the realities of hybrid warfare is crucial. This includes incorporating lessons learned from recent conflicts and integrating cyber, information, and economic warfare into traditional military strategies. The U.S. Army's Field Manual 3-24 on Counterinsurgency is a step in the right direction, but further updates are needed to address the full spectrum of hybrid threats. Doctrines should emphasize the importance of joint operations, interoperability with allies, and the integration of non-military tools in achieving strategic objectives¹⁴⁹.

Another important policy recommendation is enhancing the legal framework for cyber operations. The U.S. should work with international partners to establish clearer norms and rules for cyber warfare, building on efforts such as the Tallinn Manual. These norms should address issues of attribution, proportionality, and the distinction between military and civilian targets. Clearer legal guidelines would help to reduce ambiguity and provide a basis for collective action against cyber aggressors¹⁵⁰.

The nature of hybrid threats requires doctrines that are not only reactive but also proactive, incorporating anticipatory strategies that preempt hybrid tactics before they fully materialize. This means integrating cyber warfare, economic coercion, and information warfare into traditional military planning and operations. The U.S. military must adopt a mindset that views hybrid warfare as a continuous spectrum of conflict rather than a distinct form of warfare. By doing so, it can develop more flexible and adaptive strategies that can respond to the fluid and dynamic nature of hybrid threats¹⁵¹.

5.3 Technological Advancements

Technological advancements are at the forefront of the United States' efforts to strengthen its cybersecurity defenses against a rapidly evolving landscape of threats. Investing

¹⁴⁸ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

¹⁴⁹ Department of the Army, *Field Manual 3-24*.

¹⁵⁰ Schmitt, ed., *Tallinn Manual 2.0 on the International Law*.

¹⁵¹ Robert Person, Isak Kulalic, and John Mayle, "Back to the Future: The Persistent Problems of Hybrid War," *International Affairs* 100, no. 4 (2024): 1758.

in cutting-edge technologies such as AI, machine learning, quantum computing and blockchain technology can significantly enhance the U.S.'s ability to detect, attribute, and respond to hybrid threats.

The U.S. must continue to invest in cybersecurity infrastructure, including the development of advanced intrusion detection systems, automated response mechanisms, and robust encryption protocols. Public-private partnerships can play a vital role in this effort by fostering collaboration and information sharing between government agencies and private companies. The Cybersecurity and Infrastructure Security Agency (CISA) is an example of an agency that can facilitate such partnerships and drive improvements in national cybersecurity¹⁵².

5.3.1 Artificial Intelligence

One of the most significant technological advancements impacting U.S. cybersecurity strategy is Artificial Intelligence. AI and machine learning are transforming the way cybersecurity threats are detected and mitigated. AI-driven systems can process vast amounts of data at speeds far beyond human capabilities, enabling them to identify patterns indicative of cyber threats in real-time¹⁵³.

For example, AI is used to enhance intrusion detection systems (IDS) and intrusion prevention systems (IPS). Traditional cybersecurity measures often rely on predefined rules and signatures to detect threats, making them less effective against new, unknown threats. AI, on the other hand, can learn from vast datasets, identifying anomalies that suggest malicious activity without relying solely on known signatures. This capability is crucial for defending against zero-day exploits, which are vulnerabilities that are unknown to the software vendor and can be exploited by attackers before a fix is available¹⁵⁴.

A practical application of AI in cybersecurity is its use in predictive analytics. For instance, U.S. defense contractors have developed AI systems capable of predicting where and when cyber-attacks are most likely to occur by analyzing historical data and identifying

¹⁵² Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹⁵³ Christopher Whyte and Brian M. Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy*, 2nd ed. (Routledge, 2023), 166-172.

¹⁵⁴ Ibid.

trends. These systems provide defense agencies with early warnings, allowing them to bolster defenses in anticipation of attacks¹⁵⁵.

5.3.2 Quantum Computing

Quantum computing, while still in its developmental stages, holds the potential to revolutionize cybersecurity by providing new methods for encryption and decryption. The U.S. should prioritize research and development in quantum technologies to stay ahead of adversaries who are also investing heavily in this area. Collaborating with the private sector and academic institutions can accelerate advancements and ensure that the U.S. remains at the forefront of technological innovation¹⁵⁶.

For example, quantum computers could theoretically break traditional encryption methods, such as RSA and ECC (Elliptic Curve Cryptography), which currently secure most online communications and transactions. This poses a significant risk to national security, as adversaries with access to quantum computing could decrypt sensitive information, compromising everything from military communications to financial transactions¹⁵⁷.

In response to this potential threat, the U.S. is investing in the development of quantum-resistant algorithms. These algorithms are designed to be secure against quantum attacks, ensuring that data remains protected even in a post-quantum world. The National Institute of Standards and Technology (NIST) has been leading the charge in standardizing quantum-resistant cryptography, working with researchers and industry experts to develop new cryptographic methods that can withstand the power of quantum computers¹⁵⁸.

5.3.3 Blockchain Technology

Blockchain technology, best known for its role in cryptocurrencies, offers promising applications in cybersecurity due to its decentralized and tamper-resistant nature. Blockchain's distributed ledger system ensures that data is not stored in a single location but

¹⁵⁵ Ibid.

¹⁵⁶ Rid, *Cyber War Will Not Take Place*.

¹⁵⁷ Christopher Whyte and Brian M. Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy*, 2nd ed. (Routledge, 2023), 172-175.

¹⁵⁸ Ibid.

rather across a network of nodes, making it extremely difficult for attackers to alter data without detection¹⁵⁹.

In the context of U.S. cybersecurity, blockchain technology can be applied to enhance the security of critical infrastructure. For instance, blockchain can be used to secure supply chains by providing a transparent and immutable record of transactions. This capability is particularly valuable for the defense industry, where ensuring the integrity of the supply chain is critical to maintaining national security¹⁶⁰.

Moreover, blockchain technology can improve identity management systems. By using blockchain for digital identity verification, the U.S. can reduce the risk of identity theft and fraud, which are often precursors to more significant cyber-attacks. Blockchain-based identity management systems are already being piloted in various government and private sector initiatives, demonstrating the technology's potential to transform how identity and access are managed. An example of blockchain application in cybersecurity is its use in securing voting systems. During elections, blockchain can provide a secure and transparent way to record votes, ensuring that the process is free from tampering or fraud. The use of blockchain in voting has been explored in pilot projects across several U.S. states, reflecting a growing interest in leveraging this technology to protect democratic processes¹⁶¹.

5.3.4 The role of Public Sector

Public-private partnerships are vital for enhancing cybersecurity. The CISA plays a crucial role in facilitating collaboration between government agencies and private companies. CISA's initiatives, such as the Information Sharing and Analysis Centers (ISACs), help to disseminate timely and actionable intelligence, enabling faster and more effective responses to cyber threats¹⁶².

Encouraging the private sector to invest in cybersecurity is essential. Financial incentives, such as tax breaks and grants, can motivate companies to enhance their defenses.

¹⁵⁹ Christopher Whyte and Brian M. Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy*, 2nd ed. (Routledge, 2023), 175-179.

¹⁶⁰ Ibid.

¹⁶¹ Ibid.

¹⁶² Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2013).

Additionally, establishing clear guidelines for incident response and collaboration can streamline coordination and improve the overall effectiveness of public-private partnerships. These measures can help to build a more resilient national cybersecurity posture¹⁶³. Public-private partnerships can facilitate the transfer of knowledge and technology, accelerating the development of new defense capabilities. The U.S. should also explore opportunities for international collaboration in research and development, leveraging the expertise and resources of its allies and partners¹⁶⁴.

5.4 Training and Education

Comprehensive training and education programs are essential for preparing military personnel and civilian leaders to effectively counter hybrid threats. These programs should cover the full spectrum of hybrid warfare tactics, including cyber operations, information warfare, and unconventional tactics. Training should emphasize the importance of joint operations and interoperability with allies, ensuring that personnel are equipped to operate in a coordinated and cohesive manner¹⁶⁵.

Joint training exercises with international partners are particularly valuable for building interoperability and enhancing collective defense capabilities. These exercises can simulate hybrid warfare scenarios, allowing participants to practice responding to complex and multifaceted threats. For example, NATO's annual Cyber Coalition exercise provides a platform for member states to collaborate on cybersecurity challenges and develop joint response strategies¹⁶⁶.

In addition to military training, civilian education programs are necessary to build public awareness and resilience against hybrid threats. These programs should focus on media literacy, critical thinking, and the identification of disinformation. Schools, universities, and community organizations can play a key role in delivering these programs, helping to create a more informed and resilient society¹⁶⁷.

¹⁶³ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹⁶⁴ U.S. Department of Defense, *Summary of the 2018 National Defense Strategy*.

¹⁶⁵ Ibid.

¹⁶⁶ NATO, *Hybrid Threats: A Strategic Challenge* (Brussels: NATO, 2024).

¹⁶⁷ Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*.

Furthermore, to combat the evolving nature of hybrid warfare, military and civilian personnel must be equipped with the necessary skills to recognize and respond to these threats. Training programs should not only focus on the technical aspects of cyber operations and information warfare but also on understanding the broader strategic context in which these tactics are employed. This includes developing a deep understanding of adversaries' motivations, methods, and objectives, which can inform more effective counter-strategies. By incorporating real-world scenarios and simulations into training exercises, personnel can gain practical experience in managing the complexities of hybrid conflicts¹⁶⁸.

In response to this need, U.S. academic institutions and military training programs have begun incorporating interdisciplinary curricula that blend computer science with international relations, law, and ethics. For example, the U.S. Naval Academy and the U.S. Air Force Academy offer specialized programs that teach cadets about the legal frameworks governing cyber warfare, the ethical considerations of offensive cyber operations, and the strategic importance of cybersecurity in national defense¹⁶⁹.

These interdisciplinary programs are designed to produce well-rounded cybersecurity professionals who can navigate the complexities of the cyber domain. For instance, understanding the nuances of international law is crucial for cyber operators who may engage in activities that cross national borders. Similarly, knowledge of ethics helps ensure that cyber operations are conducted in a manner consistent with U.S. values and international norms¹⁷⁰.

5.5 Resilience and Defense Mechanisms

Building resilience against hybrid threats is crucial for maintaining national security. This involves enhancing the capacity of communities and institutions to withstand and recover from hybrid attacks. Ensuring the resilience of critical infrastructure is a key priority, requiring robust cybersecurity measures, redundant systems, and contingency planning¹⁷¹.

¹⁶⁸ Juan Jose Terrados, "Hybrid Warfare", *The Three Swords Magazine*, 35/2019, 10-12.

¹⁶⁹ Christopher Whyte and Brian M. Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy*, 2nd ed. (Routledge, 2023), 179-182.

¹⁷⁰ Ibid.

¹⁷¹ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

Developing a comprehensive resilience strategy involves multiple stakeholders, including government agencies, private sector companies, and civil society organizations. The National Infrastructure Protection Plan (NIPP) outlines a framework for enhancing the resilience of critical infrastructure sectors through public-private collaboration and risk management approaches. Implementing the NIPP's guidelines can help to improve the resilience of essential services and reduce the impact of hybrid attacks¹⁷².

Promoting societal resilience is also essential for countering the psychological and informational components of hybrid warfare. Public awareness campaigns can educate citizens about the nature of hybrid threats and the tactics used by adversaries. These campaigns should focus on media literacy, encouraging critical thinking, and providing tools to identify and counter disinformation. Schools, community organizations, and media outlets can play a vital role in these efforts by incorporating media literacy programs and facilitating discussions on hybrid threats¹⁷³.

Building community resilience involves fostering social cohesion and trust in public institutions. Engaging with local communities, promoting inclusive policies, and addressing social inequalities can help to create a more resilient society. This is particularly important in countering the divisive tactics used in information warfare, which often aim to polarize societies and undermine trust in democratic processes¹⁷⁴.

5.6 Developing a Long-Term Strategy

To maintain a competitive edge against hybrid threats, the U.S. must develop a long-term strategy that is flexible and adaptable to evolving challenges. This strategy should prioritize innovation, resilience, and international cooperation, ensuring that the U.S. can effectively counter the multifaceted nature of hybrid warfare.

Innovation is a key pillar of a long-term strategy. Investing in research and development to stay ahead of technological advancements is crucial. Public-private partnerships and collaboration with academic institutions can drive innovation and accelerate the development

¹⁷² Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2013).

¹⁷³ Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*.

¹⁷⁴ *Ibid.*

of new defense technologies. The U.S. should also explore emerging technologies such as quantum computing, AI, and machine learning, which have the potential to transform cybersecurity and hybrid warfare tactics¹⁷⁵.

Resilience should be another cornerstone of the long-term strategy. Enhancing the resilience of critical infrastructure, communities, and institutions is essential for withstanding and recovering from hybrid attacks. This involves robust cybersecurity measures, redundant systems, and comprehensive contingency planning. Promoting societal resilience through public awareness and media literacy programs can help to mitigate the impact of disinformation and other hybrid tactics¹⁷⁶.

International cooperation is also critical for addressing the global nature of hybrid threats. Strengthening alliances, building international norms, and engaging with international organizations can enhance collective security and facilitate coordinated responses. The U.S. should continue to lead diplomatic efforts to establish clear rules for hybrid warfare and promote a unified front against hybrid aggressors. International cooperation is a cornerstone of effective responses to hybrid warfare. Given the transnational nature of hybrid threats, collaborative efforts with allies and partners are essential to enhance collective security. The U.S. should continue to strengthen its alliances, particularly with NATO and other like-minded nations, to build a unified front against hybrid aggressors¹⁷⁷.

Bilateral and multilateral agreements on cybersecurity and hybrid warfare can facilitate information sharing, joint exercises, and coordinated responses. The establishment of international norms and rules for hybrid warfare, including cyber operations, is critical for reducing ambiguity and ensuring a collective response to violations. The U.S. should actively engage in diplomatic efforts to promote these norms and build international consensus¹⁷⁸.

Engaging with international organizations such as the United Nations and the European Union can also enhance efforts to counter hybrid warfare. These organizations provide platforms for dialogue, coordination, and capacity-building initiatives. For example, the EU's Hybrid Fusion Cell within its intelligence analysis center aims to improve the detection and

¹⁷⁵ Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.

¹⁷⁶ Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*.

¹⁷⁷ NATO, *Hybrid Threats: A Strategic Challenge* (Brussels: NATO, 2024).

¹⁷⁸ Schmitt, ed., *Tallinn Manual 2.0 on the International Law*.

response to hybrid threats by enhancing information sharing and analysis among member states¹⁷⁹.

5.7 Developing Resilience in Critical Infrastructure

Critical infrastructure is the backbone of any nation, supporting essential services such as energy, water, transportation, and communications. In the United States, the resilience of these systems against cyber threats is of paramount importance. The interconnected nature of modern infrastructure means that a successful cyber-attack on one sector can have cascading effects across others, potentially leading to widespread disruption and economic damage.

This involves implementing robust cybersecurity measures, creating redundant systems, and developing comprehensive contingency plans. Public-private partnerships can play a vital role in enhancing the resilience of critical infrastructure sectors, such as energy, finance, and communications. The NIPP provides a framework for enhancing the resilience of critical infrastructure through public-private collaboration and risk management approaches. Implementing the NIPP's guidelines can help to improve the resilience of essential services and reduce the impact of hybrid attacks. Regular risk assessments, joint exercises, and continuous improvement initiatives are essential for maintaining and enhancing infrastructure resilience¹⁸⁰.

One notable example of vulnerability assessments in action is the energy sector's GridEx exercise, a biennial event that simulates cyber-attacks on the U.S. power grid. This exercise, organized by the North American Electric Reliability Corporation (NERC), brings together government and private sector participants to test the resilience of the grid and develop strategies for mitigating the impact of potential cyber incidents. The lessons learned from GridEx have been instrumental in enhancing the security and resilience of the nation's energy infrastructure¹⁸¹.

Promoting resilience also involves engaging with local communities and fostering social cohesion. Inclusive policies, addressing social inequalities, and building trust in public

¹⁷⁹ European Commission, *Joint Framework on Countering Hybrid Threats*.

¹⁸⁰ Department of Homeland Security, *National Infrastructure Protection Plan*.

¹⁸¹ Kate Ledesma, "GridEx: How exercising response and recovery supports grid reliability", *Security* (2021), <https://www.securitymagazine.com/articles/96260-gridex-how-exercising-response-and-recovery-supports-grid-reliability>.

institutions can help to create a more resilient society. This is particularly important in countering the divisive tactics used in information warfare, which often aim to polarize societies and undermine trust in democratic processes¹⁸².

In addition to national-level plans, individual infrastructure operators are encouraged to develop their own incident response plans tailored to the specific needs and vulnerabilities of their systems. These plans should include provisions for maintaining critical operations during an incident, such as using backup systems or rerouting services, and for communicating effectively with stakeholders and the public.

A practical example of incident response planning in action is the healthcare sector's response to cyber-attacks during the COVID-19 pandemic. With hospitals and healthcare facilities under increased strain, the need for resilient systems became more apparent than ever. The healthcare sector's incident response plans were tested as cyber-attacks targeted vital systems, from patient records to medical devices. The ability to quickly isolate affected systems and restore functionality was crucial in maintaining patient care during these challenging times¹⁸³.

5.8 Strengthening International Legal Frameworks

As cyber threats transcend national borders, there is an urgent need for robust international legal frameworks to govern state and non-state activities in cyberspace. The United States plays a crucial role in shaping these frameworks, which are essential for establishing norms of behavior, promoting cooperation, and holding accountable those who engage in malicious cyber activities. Strengthening international legal frameworks is critical for addressing the unique challenges of hybrid warfare. While existing international laws provide some guidance, there is a need for updated frameworks that address the complexities of hybrid conflicts. Efforts such as the Tallinn Manual on the International Law Applicable to

¹⁸² Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*.

¹⁸³ Anna Ribeiro, "Biden Administration Boosts Healthcare Cybersecurity Following a 128% Rise in Cyberattacks; Ropes in Microsoft, Google," *Industrial Cyber*, June 12, 2024, <https://industriacyber.co/medical/biden-administration-boosts-healthcare-cybersecurity-following-a-128-rise-in-cyberattacks-ropes-in-microsoft-google/>.

Cyber Warfare and the development of international agreements on cyber norms are steps in the right direction¹⁸⁴.

The U.S. should actively engage in diplomatic efforts to promote international norms and rules for hybrid warfare. Establishing clearer legal guidelines for cyber operations, information warfare, and the use of autonomous systems can help to reduce ambiguity and provide a basis for collective action against violations. Building international consensus on these issues is essential for ensuring a unified and effective response to hybrid threats¹⁸⁵.

Engaging with international organizations such as the United Nations and the European Union can enhance efforts to develop and enforce these legal frameworks. These organizations provide platforms for dialogue, coordination, and capacity-building initiatives. For example, the EU's Hybrid Fusion Cell within its intelligence analysis center aims to improve the detection and response to hybrid threats by enhancing information sharing and analysis among member states¹⁸⁶.

¹⁸⁴ Schmitt, ed., *Tallinn Manual 2.0 on the International Law*.

¹⁸⁵ *Ibid.*

¹⁸⁶ European Commission, *Joint Framework on Countering Hybrid Threats*.

CHAPTER 6

Conclusions

6.1 The Evolution and Relevance of Hybrid Warfare

From ancient times to the modern era, hybrid tactics have consistently been used to exploit the weaknesses of conventionally superior adversaries. Modern conflicts increasingly involve a combination of military, cyber, economic, and informational tactics, requiring a multidimensional approach to defense and security. Understanding this historical context is crucial for developing effective strategies to counter contemporary hybrid threats.

The historical context and evolution of hybrid warfare reveal its enduring principles and adaptability across different eras and geopolitical landscapes. From ancient empires to modern state and non-state actors, the use of a blend of conventional and unconventional tactics has proven to be an effective strategy in achieving strategic objectives. The examination of hybrid warfare's evolution underscores its relevance in contemporary conflicts and the need for comprehensive strategies to counter its multifaceted threats. As global power dynamics continue to shift, understanding the historical and evolving nature of hybrid warfare will be crucial for developing effective defense and security strategies¹⁸⁷.

In the 20th and 21st centuries, hybrid warfare has evolved in response to technological advancements and the changing geopolitical landscape. The World Wars introduced the institutionalization of propaganda and psychological operations, while the Cold War epitomized the extensive use of proxy wars, espionage, economic pressure, and disinformation. The Vietnam War showcased the effectiveness of guerrilla tactics and psychological operations in weakening a technologically superior opponent. In the post-Cold War era, the rise of non-state actors and the integration of cyber warfare and information operations have become central components of hybrid warfare, as seen in the conflicts in the Middle East and Eastern Europe.

¹⁸⁷ Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).

6.2 The U.S. Response to Hybrid Warfare

The U.S. strategy for countering hybrid warfare is characterized by its comprehensive and integrated approach, leveraging military, economic, diplomatic, and informational tools. The emphasis on alliances, technological capabilities, and flexible response strategies provides a strong foundation for addressing the multifaceted nature of hybrid threats. However, challenges such as identification and attribution, interagency coordination, technological advancements, and societal resilience must be addressed to enhance the effectiveness of U.S. responses.

Case studies of U.S. responses to hybrid warfare in Ukraine and against ISIS demonstrate the importance of a multifaceted approach that combines military action with efforts to undermine adversaries' capabilities and influence. These examples highlight the need for continuous adaptation and innovation in U.S. strategy to effectively counter the evolving nature of hybrid warfare. As global power dynamics continue to shift, the U.S. must remain vigilant and proactive in addressing the complex challenges posed by hybrid threats.

Countering hybrid warfare presents numerous challenges, from identifying and attributing attacks to ensuring effective interagency coordination, addressing technological and intelligence gaps, and navigating legal and ethical considerations. To overcome these challenges, the U.S. must continuously adapt and innovate its strategies, invest in research and development, and enhance training and education programs. International cooperation and the development of clear legal frameworks are essential for addressing the transnational nature of hybrid threats. Building societal resilience and public awareness is also crucial for mitigating the impact of hybrid warfare tactics.

By taking a comprehensive and integrated approach, the U.S. can enhance its ability to counter the multifaceted nature of hybrid warfare and protect national security. As global power dynamics continue to evolve, maintaining vigilance and proactive measures will be critical for addressing the complex challenges posed by hybrid threats.

Addressing the challenges posed by hybrid warfare requires a comprehensive and integrated approach that combines policy changes, technological advancements, training and education, international cooperation, public-private sector collaboration, and resilience-

building efforts. By continuously adapting and innovating its strategies, the U.S. can enhance its ability to counter the multifaceted nature of hybrid threats and protect national security.

Policy recommendations such as establishing a centralized coordinating body, updating military doctrines, and enhancing the legal framework for cyber operations are essential for improving the U.S.'s response to hybrid warfare. Investing in cutting-edge technologies, building public awareness, and promoting media literacy can help to address the technological and informational components of hybrid threats.

International cooperation, public-private sector collaboration, and developing resilience in critical infrastructure are also crucial for countering hybrid warfare. By strengthening alliances, building international norms, and fostering a culture of resilience, the U.S. can create a robust defense against hybrid threats.

6.3 Hybrid Warfare as the Continuation of War with Other Weapons

Carl von Clausewitz, the influential military theorist, famously asserted that "*War is a mere continuation of policy by other means*". This assertion encapsulates the idea that war is not an isolated act of violence but a strategic tool used by states to achieve political objectives when diplomacy and other means have failed. In Clausewitz's view, war is inherently connected to the political goals of a nation, with military force being one of many instruments at its disposal¹⁸⁸.

In the 21st century, the emergence of hybrid warfare has extended Clausewitz's theory into new domains. Hybrid warfare represents the evolution of conflict where the lines between war and peace, military and civilian, and combatants and non-combatants are increasingly blurred. It is a strategic blend of conventional and unconventional methods, combining cyber attacks, disinformation, economic coercion, and the use of proxy forces to achieve political objectives without the need for full-scale military confrontation¹⁸⁹.

¹⁸⁸ 1. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 87.

¹⁸⁹ Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 8-12.

Hybrid warfare, therefore, can be seen as a continuation of war with other weapons—those of the modern, interconnected world. In this framework, the traditional battlefield has expanded to include cyberspace, the media, and global financial systems, where adversaries engage in a form of conflict that does not necessarily involve traditional armed forces. This type of warfare allows states to pursue their political goals while maintaining plausible deniability and avoiding the costly and destructive consequences of conventional war¹⁹⁰.

Clausewitz's notion that war is a continuation of policy by other means is directly applicable to hybrid warfare. In hybrid conflicts, the objectives remain fundamentally political, but the means of achieving these objectives have diversified. The use of cyber operations, for example, allows states to disrupt an adversary's critical infrastructure or steal sensitive information, thereby weakening their position without a single shot being fired. Similarly, disinformation campaigns can erode trust in public institutions and influence elections, effectively altering the political landscape in favor of the aggressor.

The United States, recognizing the evolving nature of conflict, has adapted its strategy to address these challenges. The U.S. has embraced the concept of integrated deterrence, which combines military strength with cyber, economic, and informational tools to deter and counter hybrid threats. This strategy reflects an understanding that in the modern world, war is not just fought on the battlefield but also in the digital, economic, and informational realms. The U.S. strategy acknowledges that hybrid warfare is a continuation of war with new weapons and has accordingly enhanced its cyber defenses, developed offensive cyber capabilities, and integrated these into broader military strategies¹⁹¹.

The U.S. has also prioritized building resilience across its society and infrastructure, recognizing that hybrid warfare targets civilian sectors as much as military ones. This includes protecting critical infrastructure from cyber attacks, countering disinformation campaigns, and enhancing public awareness of hybrid threats. The U.S. strategy emphasizes the need for a whole-of-government approach, integrating efforts across different sectors and agencies to build a comprehensive defense against hybrid warfare.

¹⁹⁰ Ilmari Käihkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," *Parameters* 51, no. 3 (2021): 22-27. <https://press.armywarcollege.edu/parameters/vol51/iss3/11>.

¹⁹¹ *Ibid.*

International collaboration is another cornerstone of the U.S. strategy. By strengthening alliances, particularly with NATO, the U.S. enhances its ability to respond to hybrid threats that often transcend national borders. Joint exercises, intelligence sharing, and coordinated responses are essential components of this strategy, reflecting the understanding that hybrid warfare is a global challenge that requires a unified international response¹⁹².

In essence, hybrid warfare is the embodiment of Clausewitz's theory in the contemporary era, where the means of warfare have expanded beyond the battlefield to include a wide array of non-military strategies. It reflects the reality that war, as a tool of policy, is evolving in response to technological advancements and the changing nature of global power dynamics. The U.S. strategy, with its focus on integrated deterrence, resilience, and international collaboration, is designed to address these challenges, ensuring that the United States can continue to protect its national interests and uphold global stability in an era where hybrid warfare is likely to remain a central feature of international relations.

In conclusion, just as Clausewitz viewed war as an extension of politics, hybrid warfare should be understood as an extension of war into new realms, where the weapons are not just guns and tanks, but also bits and bytes, narratives, and economic leverage. The U.S. strategy reflects this understanding, adapting to the complexities of modern conflict to ensure that it remains capable of achieving its political objectives in a world where the nature of war is continuously evolving.

6.4 The Necessity of Adapting

As hybrid warfare evolves into a dominant form of conflict in the 21st century, the United States has recognized the necessity of adapting its national defense strategy to meet these challenges head-on. Hybrid warfare, characterized by the integration of conventional and unconventional tactics—such as cyber attacks, disinformation, economic coercion, and proxy warfare—presents a complex and multifaceted threat to national security. The U.S. strategy in hybrid warfare, therefore, must evolve to not only counter these threats effectively but also anticipate future developments in this ever-changing landscape.

¹⁹² Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 55-57.

To strengthen its position against hybrid threats, the United States has begun prioritizing investments in several critical sectors that are essential to maintaining a strategic advantage. These sectors include cybersecurity, artificial intelligence, advanced military technology, information warfare capabilities, and international collaboration. Each of these areas represents a crucial component of a comprehensive strategy to counter hybrid threats, ensuring that the U.S. remains resilient and capable of protecting its interests in an increasingly complex global environment.

6.4.1 Cybersecurity: The Frontline of Hybrid Warfare

Cybersecurity is at the forefront of the U.S. strategy in hybrid warfare. As hybrid threats often involve cyber attacks aimed at critical infrastructure, financial systems, and government networks, the need for robust cybersecurity measures has never been more urgent. The U.S. has already recognized the centrality of cyberspace in modern warfare, as evidenced by the establishment of U.S. Cyber Command, which operates as both a defensive and offensive entity in the realm of cyber operations¹⁹³.

Investments in cybersecurity must be prioritized to address the increasing sophistication of cyber threats. This includes enhancing the security of critical infrastructure, such as energy grids, water supply systems, and communication networks, which are often targeted by adversaries in hybrid conflicts. The protection of these systems is vital to ensuring the continuity of essential services during a hybrid attack and to maintaining public confidence in the government's ability to protect the nation¹⁹⁴.

Moreover, there is a pressing need for investment in the development of advanced cyber defense technologies. This includes artificial intelligence and machine learning algorithms that can detect and respond to cyber threats in real-time, thereby reducing the window of vulnerability. The use of AI in cybersecurity can automate threat detection and response, enabling quicker and more effective countermeasures against cyber attacks. By

¹⁹³ Ilmari Käihkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," *Parameters* 51, no. 3 (2021): 29-33.

¹⁹⁴ Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 45-48.

prioritizing investments in these technologies, the U.S. can stay ahead of adversaries who are increasingly leveraging AI in their cyber warfare strategies.

6.4.2 AI and Autonomous Systems: Shaping the Future Battlefield

Artificial Intelligence and autonomous systems represent the next frontier in hybrid warfare. The U.S. has already begun to explore the potential of AI to enhance its military capabilities, particularly in areas such as surveillance, reconnaissance, and decision-making. However, to fully harness the power of AI in hybrid warfare, significant investments are required in research, development, and deployment of AI technologies¹⁹⁵.

AI can be a game-changer in hybrid warfare by providing the U.S. military with the ability to process vast amounts of data and make decisions at a speed that far exceeds human capabilities. This is particularly important in the context of cyber operations, where the ability to quickly identify and neutralize threats can mean the difference between success and failure. Furthermore, AI-driven systems can be used to enhance situational awareness on the battlefield, providing real-time intelligence that can be used to inform strategic and tactical decisions¹⁹⁶.

Investing in autonomous systems is another critical priority. These systems, which include unmanned aerial vehicles (drones), autonomous ground vehicles, and robotic platforms, can be deployed in environments that are too dangerous or inaccessible for human soldiers. Autonomous systems can conduct reconnaissance, deliver supplies, and even engage in combat, reducing the risk to human life and increasing operational efficiency.

However, the development and deployment of AI and autonomous systems also raise significant ethical and legal challenges, particularly concerning the use of lethal autonomous weapons. The U.S. must invest not only in the technology itself but also in the establishment of robust ethical guidelines and legal frameworks that govern the use of AI in warfare. Ensuring that AI and autonomous systems are deployed in a manner consistent with international law and ethical standards is crucial to maintaining the legitimacy of U.S. military operations in the eyes of the global community.

¹⁹⁵ Ilmari Käihkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," *Parameters* 51, no. 3 (2021): 38-42.

¹⁹⁶ Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 55-59.

6.4.3 Advanced Military Technology: Enhancing Conventional Capabilities in a Hybrid World

While hybrid warfare often emphasizes unconventional tactics, maintaining and enhancing conventional military capabilities remains a cornerstone of U.S. defense strategy. In a hybrid conflict, conventional forces play a critical role in deterring adversaries, responding to crises, and providing the backbone for other forms of hybrid operations, such as cyber and information warfare¹⁹⁷.

Investments in advanced military technology are essential to ensuring that the U.S. military can operate effectively in a hybrid warfare environment. This includes the development of next-generation weapons systems, such as hypersonic missiles, directed energy weapons, and advanced missile defense systems. These technologies provide the U.S. with the capability to project power and defend against high-tech threats that are increasingly becoming a feature of hybrid warfare¹⁹⁸.

Moreover, the modernization of existing military platforms is a priority. Upgrading the U.S. military's fleet of aircraft, ships, and armored vehicles with the latest technology ensures that these platforms remain effective in the face of evolving threats. This includes integrating advanced sensors, communication systems, and electronic warfare capabilities into conventional forces, enabling them to operate seamlessly in a hybrid warfare environment.

Another area of investment is in the development of multi-domain operational capabilities. Hybrid warfare often spans multiple domains—land, sea, air, space, and cyberspace—requiring a coordinated response across all these areas. The U.S. military must prioritize investments in technologies and strategies that enable seamless integration and coordination across these domains. This includes the development of joint command and control systems that allow for real-time communication and decision-making across different branches of the military and with allied forces.

¹⁹⁷ Ilmari Käihkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," *Parameters* 51, no. 3 (2021): 42-47.

¹⁹⁸ Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 65-69.

6.4.4 Information Warfare: Winning the Battle of Narratives

Information warfare is a critical component of hybrid warfare, where the control of information and the manipulation of public perception can have strategic consequences. The U.S. strategy in hybrid warfare must prioritize investments in capabilities that allow it to dominate the information space, both defensively and offensively¹⁹⁹.

Defensively, the U.S. must invest in technologies and strategies that protect against disinformation and influence operations conducted by adversaries. This includes enhancing the resilience of democratic institutions, improving media literacy among the population, and developing tools to detect and counter false narratives. Investments in artificial intelligence can play a crucial role in these efforts by enabling the rapid identification and response to disinformation campaigns²⁰⁰.

Offensively, the U.S. must prioritize the development of capabilities that allow it to conduct effective information operations against adversaries. This includes the ability to shape narratives, influence public opinion, and undermine the morale of opposing forces. Investments in psychological operations, strategic communications, and social media platforms are essential to achieving these objectives. The ability to control the narrative and project a positive image of U.S. actions is crucial to winning the battle of hearts and minds in hybrid conflicts.

6.4.5 International Collaboration: Strengthening Alliances in a Hybrid World

Hybrid warfare often transcends national borders, making international collaboration a critical element of U.S. strategy. The U.S. must prioritize investments in strengthening alliances and partnerships to ensure a coordinated and effective response to hybrid threats²⁰¹.

¹⁹⁹ Ilmari Käihkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," *Parameters* 51, no. 3 (2021): 50-55.

²⁰⁰ Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 74-79.

²⁰¹ Ilmari Käihkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," *Parameters* 51, no. 3 (2021): 60-65.

NATO, for example, has been a central pillar of U.S. strategy in countering hybrid warfare in Europe. The alliance has developed several initiatives aimed at enhancing the collective defense against hybrid threats, including the establishment of the Hybrid Warfare Centre of Excellence and the adoption of the Comprehensive Approach to hybrid threats. The U.S. must continue to invest in these initiatives, ensuring that NATO remains capable of responding to the complex and evolving nature of hybrid warfare²⁰².

Beyond NATO, the U.S. must also prioritize partnerships with other countries and international organizations. This includes strengthening ties with allies in the Indo-Pacific region, where hybrid threats from state and non-state actors are increasingly prevalent. Collaborating with countries like Japan, South Korea, and Australia in areas such as cybersecurity, intelligence sharing, and joint military exercises is essential to countering hybrid threats in this strategically important region.

Finally, international collaboration must extend to the development of global norms and legal frameworks that address the challenges of hybrid warfare. The U.S. should prioritize investments in diplomatic efforts to establish international agreements on issues such as cyber warfare, disinformation, and the use of autonomous systems in conflict. Establishing clear norms and rules for hybrid warfare can help to reduce the risk of escalation and ensure that all nations play by the same rules in the increasingly complex world of modern conflict²⁰³.

²⁰² Frank Hoffman, Colonel Matt Neumeyer, and Benjamin Jensen, *The Future of Hybrid Warfare* (Washington, DC: Center for Strategic and International Studies, 2024), 80-85.

²⁰³ Ilmari Käihkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," *Parameters* 51, no. 3 (2021): 70-75.

REFERENCES

Barfield, Thomas J. *The Perilous Frontier: Nomadic Empires and China*. Oxford: Basil Blackwell, 1989.

Caliskan, Murat. "Hybrid warfare through the lens of strategic theory", *Defence & Security Analysis* (2019). doi: 10.1080/14751798.2019.1565364.

Calvocoressi, Peter, Guy Wint, and John Pritchard. *Total War: Causes and Courses of the Second World War*. London: Penguin Books, 1989.

Chandler, David G. *The Campaigns of Napoleon*. New York: Scribner, 2009.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2012.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Coakley, Robert W., and Stetson Conn. *The War of the American Revolution*. Washington, D.C.: Center of Military History, United States Army, 2010.

Cordesman, Anthony H. *The Iraq War: Strategy, Tactics, and Military Lessons*. Washington, DC: Center for Strategic and International Studies, 2003.

Department of the Army. *Field Manual 3-24: Counterinsurgency*. Washington, DC: Department of the Army, 2014.

Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security, 2013.

Esdaile, Charles. *Napoleon's Wars: An International History, 1803-1815*. London: Penguin Books, 2008.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication to the European Parliament and the Council: Joint Framework*

on *Countering Hybrid Threats – a European Union Response*. JOIN (2016) 18 final. Brussels, April 6, 2016.

Felgenhauer, Pavel. "A New Version of the 'Gerasimov Doctrine'?" *Eurasia Daily Monitor* 16, no. 32 (2019): 15. Accessed [05 Jul 2024]. <https://jamestown.org/program/a-new-version-of-the-gerasimov-doctrine/>

Ferling, John. *Whirlwind: The American Revolution and the War That Won It*. New York: Bloomsbury Press, 2015.

Gaddis, John Lewis. *The Cold War: A New History*. New York: Penguin Books, 2005.

Galeotti, Mark. *Hybrid War or Gibrinaya Voina? Getting Russia's Non-Linear Military Challenge Right*. Prague: Mayak Intelligence, 2016.

Gartzke, Erik, and Jon R. Lindsay. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford: Oxford University Press, 2019.

Haldon, John. *Warfare, State and Society in the Byzantine World, 565-1204*. London: Routledge, 1999.

Heap, Bean. *Hybrid Threats: A Strategic Communication Perspective*, .NATO StartCom COE, 2019.

Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007.

Hoffman, Frank G. "Hybrid Warfare and Challenges." *Joint Force Quarterly* 52 (1st quarter 2009): 34-39.

Hoffman, Frank, Colonel Matt Neumeier, and Benjamin Jensen. *The Future of Hybrid Warfare*. Washington, DC: Center for Strategic and International Studies, 2024.

Joint Chiefs of Staff. *Joint Publication 3-0: Joint Operations*. Washington, DC: Joint Chiefs of Staff, 2017.

Käihkö, Ilmari. "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession." *Parameters* 51, no. 3 (2021): 22-27. <https://press.armywarcollege.edu/parameters/vol51/iss3/11>.

Karnow, Stanley. *Vietnam: A History*. New York: Penguin Books, 1997.

Kilcullen, David. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. Oxford: Oxford University Press, 2009.

Lawrence, Mark Atwood. *The Vietnam War: A Concise International History*. Oxford: Oxford University Press, 2008.

Ledesma, Kate. "GridEx: How exercising response and recovery supports grid reliability", *Security* (2021), <https://www.securitymagazine.com/articles/96260-gridex-how-exercising-response-and-recovery-supports-grid-reliability>.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. London: Routledge, 2004.

Luttwak, Edward N. *The Grand Strategy of the Byzantine Empire*. Cambridge, MA: Belknap Press of Harvard University Press, 2009.

Mattis, James N. and Frank Hoffman. "Future Warfare: The Rise of Hybrid Wars", USNI, no.11 (2005): 1-2.

May, Timothy. *The Mongol Art of War: Chinggis Khan and the Mongol Military System*. Yardley, PA: Westholme Publishing, 2007.

McInnis, Kathleen J. *Coalition Contributions to Countering the Islamic State*. R44135. Washington, D.C.: Congressional Research Service, August 24, 2016.

Messinger, Garry S. *British Propaganda and the State in the First World War*. Manchester: Manchester University Press, 1992.

Mökander, Jakob. "Auditing of AI: Legal, Ethical and Technical Approaches." *Digital Society* 2 (2023): 49. Accessed [05 Jul 2024]. <https://doi.org/10.1007/s44206-023-00074-y>.

Mumford, Andrew. *Proxy Warfare*. Cambridge: Polity Press, 2013.

Murray, Williamson, and Peter R. Mansoor, eds. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge: Cambridge University Press, 2012.

NATO. *Hybrid Threats: A Strategic Challenge*. Brussels: NATO, 2024.

NC State University Libraries. "Legal and Ethical Implications." *Social Media Archives Toolkit*, 2023. Accessed [14 Jul 2024]. <https://www.lib.ncsu.edu/social-media-archives-toolkit/legal>.

Person, Robert, Isak Kulalic, and John Mayle. "Back to the Future: The Persistent Problems of Hybrid War." *International Affairs* 100, no. 4 (2024): 1749-1761.

Pomerantsev, Peter. *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*. New York: Public Affairs, 2014.

Ribeiro, Anna. "Biden Administration Boosts Healthcare Cybersecurity Following a 128% Rise in Cyberattacks; Ropes in Microsoft, Google." *Industrial Cyber*. June 12, 2024. <https://industrialcyber.co/medical/biden-administration-boosts-healthcare-cybersecurity-following-a-128-rise-in-cyberattacks-ropes-in-microsoft-google/>.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013.

Schmid, Johann. "Hybrid Warfare on the Ukrainian Battlefield: Developing Theory Based on Empirical Evidence." *Journal on Baltic Security* 5, no. 1 (2019): 5-15.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

The White House. *National Security Strategy*. Washington, DC: The White House, 2022.

Terrados, Juan Jose. "Hybrid Warfare". *The Three Swords Magazine*, 35/2019.

U.S. Department of Defense, Quadrennial Defense Review Report, Washington DC, 2010.

U.S. Department of Defense. *Quadrennial Defense Review 2014*. Washington, DC: U.S. Department of Defense, 2014.

U.S. Department of Defense. *National Defense Strategy of the United States of America: 2022*. Washington, DC: Department of Defense, 2022.

U.S. Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*. Washington, DC: Department of Defense, 2018.

U.S. Government Publishing Office. *The Evolution of Hybrid Warfare and Key Challenges*. Washington, DC: U.S. Government Publishing Office, 2017.
<https://www.govinfo.gov/content/pkg/CHRG-115hrg25088/pdf/CHRG-115hrg25088.pdf>.

Walley, Cheryl A., and Michael R. Mullins. *Psychological Operations in Operation Iraqi Freedom*. Washington, D.C.: U.S. Army Special Operations Command, 2005.

Westad, Odd Arne. *The Global Cold War: Third World Interventions and the Making of Our Times*. Cambridge: Cambridge University Press, 2007.

Whyte, Christopher, and Brian M. Mazanec. *Understanding Cyber-Warfare: Politics, Policy and Strategy*. 2nd ed. Routledge, 2023.