



## COUNTERING GRAY-ZONE HYBRID THREATS

An Analysis of Russia's 'New Generation Warfare'  
and Implications for the US Army

By John Chambers  
October 18, 2016







Captain John Chambers is an instructor of American politics in the Department of Social Sciences at the US Military Academy at West Point. He is an Engineer officer with ten years of service including a combat deployment to Baghdad, Iraq, during the 2007 “surge” and a no-notice deployment to Haiti as part of the Global Response Force following the 2010 earthquake. He served as the Task Force Engineer for 2-325 AIR, a Sapper Platoon Leader and Executive Officer in 2 BCT, 82<sup>nd</sup> Airborne, and commanded the US Army’s Sapper Leader Course and the 509<sup>th</sup> Clearance Company at Fort Leonard Wood, MO. He holds a BS in Civil Engineering from the US Military Academy, an MS in Engineering Management from the Missouri University of Science and Technology, and a Masters in Public Policy from Harvard’s Kennedy School of Government. He is also a certified Project Management Professional. The views in this report reflect those of the author and do not represent the views of the Department of Defense or the US Army.

# Countering Gray-Zone Hybrid Threats

## Contents

Abstract .....	4
I. Executive Summary .....	4
II. Describing Hybrid Threats and the Gray Zone .....	8
Contemporary View of Hybrid Threats .....	9
The Spectrum of Conflict: Hybrid Threats vs. the Gray Zone .....	12
Characteristics of Contemporary Hybrid Threats .....	15
Gray-Zone Hybrid Threats .....	16
Open-Warfare Hybrid Threats .....	22
Findings and Recommendations .....	22
III. Identifying and Adapting to Challenges Posed by Gray-Zone Hybrid Threats Due to Laws, Norms, and Processes .....	23
Challenges Posed by Gray-Zone Hybrid Threats .....	23
Russia’s “New Generation Warfare” vs. US Doctrine .....	25
Findings and Recommendations .....	30
IV: Improving US Army Capacity to Counter Gray-Zone Hybrid Threats .....	31
Identifying and Understanding the Threat .....	31
Reducing Risk .....	35
V: Summary: The Future of Hybrid Threats .....	41
Appendix A: Select Definitions.....	44
Appendix B: US Operational Phases from Joint Publication 5-0, Operational Art and Design .....	46
Appendix C: Ukraine Crisis Maps .....	47

# Countering Gray-Zone Hybrid Threats

Appendix D: Ethnic Russian Populations in Eastern Europe .....	48
Appendix E: Methodology & Acknowledgements .....	49
Bibliography.....	50

## List of Figures:

Figure 1: Spectrum of Conflict	5
Figure 2: US vs. Russian Operational Phases	26

## Abstract

*The gray zone is an operating environment in which aggressors use ambiguity and leverage non-attribution to achieve strategic objectives while limiting counter-actions by other nation states. Inside the gray zone, aggressors use hybrid tactics to achieve their strategic objectives. While hybrid threats have historically been associated with irregular and conventional warfare, their use in the gray zone leads to a dichotomy between two types of hybrid threats that can mainly be attributed to the need for ambiguity and non-attribution in the gray zone. The two types of hybrid threats are “open-warfare hybrid threats” and “gray-zone hybrid threats.” A case in point is Russia’s military actions in eastern Ukraine, part of what the Kremlin calls its “New Generation Warfare.” In this MWI report, Captain John Chambers draws on this case study to recommend ways the US Army can improve its capacity to counter ongoing as well as future gray-zone hybrid threats.*

## I. Executive Summary

The gray zone is the “space” between peace and war on the spectrum of conflict. It is an operational environment “churning with political, economic, and security competitions that require constant attention.”<sup>1</sup> On the heels of Russia’s military actions in eastern Ukraine and China’s expansion in the South China Sea, the military and academic communities have attempted to describe conflict in the gray zone to create shared understanding and spur discussion on conflict and competition in this space.

Toward the mid-to-late 2000s, a similar effort was underway to describe the integration and fusion of irregular and conventional tactics on a single battlefield. This became known as

hybrid warfare and was best described by retired Lt. Col. Frank Hoffman as when “an adversary simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives.”<sup>2</sup>

Describing the current state of warfare is not just important to academic and military strategists, it is also essential to helping policymakers and civilian leaders understand the changing nature of warfare. Ultimately, being able to describe the challenges faced by the military helps the Army organize and equip itself with the capabilities necessary to achieve

---

<sup>1</sup> Nadia Schadlow, “Peace and War: The Space Between,” August 18, 2014, *War on the Rocks*.

<sup>2</sup> Frank Hoffman, “The Contemporary Spectrum of Conflict: Protracted, Gray zone, Ambiguous, and Hybrid Modes of War.” 2016 Index of US Military Strength. The Heritage Foundation (October 2015).

## Countering Gray-Zone Hybrid Threats

its strategic objectives. Without describing threats and defining the current state in the evolution of warfare, it is difficult to achieve shared understanding among the military, the public, and policymakers.

To that end, this report pursues three lines of effort: (1) describing hybrid threats and the gray zone, (2) identifying challenges that gray-zone hybrid threats pose for the US Army due to laws, norms, and processes, and (3) recommending ways that the US Army can improve capacity to counter gray-zone hybrid threats. To develop these solutions, I use a mix of research, interviews, and working-group participation. The interviews were conducted with experts from across the United States and focused on unconventional warfare, hybrid warfare, military strategy, non-violent civil resistance, and Russian affairs. Finally, the

working groups, hosted by the Strategic Studies Institute at the Army War College (AWC), focused on hybrid warfare and the gray zone. Participants included AWC professors and students, scholars, and strategists.

The Army must adequately define hybrid threats and the gray zone in order to achieve shared understanding amongst strategists, leaders, and policymakers. When doing this, the Army should consider that the gray zone is not a specific type of conflict but an operational environment as defined in Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms. Finally, the Army must recognize that there is a distinct difference between hybrid threats in the gray zone and open-warfare hybrid threats (See Figure 1):

Hybrid Threats			
Gray-Zone Hybrid Threats		Open-Warfare Hybrid Threats	
Gray Zone Conflict	Irregular Warfare	Limited Conventional	Theater Conventional

Figure 1: Spectrum of Conflict

This report posits that hybrid threats in the gray zone are dependent on ambiguity and non-attribution. This creates a dichotomy and breaks hybrid threats into two types: gray-zone hybrid threats and open-warfare hybrid threats.

This report will address the characteristics of gray-zone hybrid threats in depth. These characteristics include: (1) Ambiguity, (2) Exploitation of Adversary Weaknesses through DIME, (3) Attacks in Five Domains, (4) Use of

## Countering Gray-Zone Hybrid Threats

Criminal Organizations and Networks, and (5) Using Laws and Cultural Norms as a Weapons System. Open-warfare hybrid threats are what are commonly thought of today as hybrid tactics/warfare. Consequently, this report will not address them in-depth, as there is a large amount of literature already written on the subject.

*Hybrid threats and the gray zone are issues that have existed in warfare for centuries. However, their recent emergence in the discussion of conflict amongst strategists, scholars, and policymakers highlights their renewed importance.*

Gray-zone hybrid threats take advantage of the US government's bureaucracy by exploiting the fact that the Department of Defense is often not the lead agency operating in the gray zone as they would be during large-scale, conventional conflict. Specifically, "New Generation Warfare" conducted by the Russians is focused on taking action and achieving strategic objectives within Phase 0 of US military operations. Phase 0, the "Shape" phase, of US military operations, is defined as "Joint and multinational operations—inclusive of normal routine military activities—and various interagency activities . . . performed to dissuade or deter potential adversaries and to assure or

solidify relationships with friends and allies,"<sup>3</sup> and is ultimately where US doctrine addresses gray-zone conflict. The Russians target this area because it is where US bureaucracy is greatest and, consequently, the reaction time is slowest.

To counter adversary actions within Phase 0 of US Army operations, the US Army must recognize and adapt to the challenges that gray-zone hybrid threats pose due to existing laws, norms, and processes. This entails conducting an analysis of gray-zone doctrine from the most likely gray-zone adversaries (Russia, China, and Iran) and then evaluating the US phasing construct and options for action within Phase 0 to decide if they are appropriate to counter gray-zone hybrid threats. Secondly, the US Army needs to look at systems and processes used to fuse intelligence and create shared understanding across multiple agencies. If the systems and processes are inadequate to quickly and efficiently share information, then these systems and processes must be changed to increase speed and efficiency.

The US Army must improve its capacity to counter gray-zone hybrid threats. To do this, the Army must take actions to better identify and understand the threat as well as reduce risk. To identify and understand the threat, the

---

<sup>3</sup> The Joint Staff, "Joint Publication 5-0, *Joint Operational Planning*," August 2011.

## Countering Gray-Zone Hybrid Threats

US Army must rebuild unconventional warfare capacity within the special operations forces (SOF). This capacity has atrophied over the past 15 years as SOF, in particular the US Army special forces, have focused more on counter-terrorism, direct action, and foreign internal defense operations. While the special operations community has recently taken steps to rebuild this capacity, it will take time to reconstitute institutional knowledge and this must remain a priority. Secondly, the US Army should increase broadening opportunities for education among special operations junior officers and non-commissioned officers. These opportunities will improve the critical thinking skills of personnel operating in the gray zone, allowing them to put individual actions of an adversary into the context of a broader strategy and US foreign policy. This will, in turn, help our soldiers on the ground better identify and understand the threat and communicate that threat upwards and across the multiple agencies involved in gray-zone operations.

Finally, to reduce risk, the US Army can take three concrete actions. First, the Army must move to pre-position forces in at-risk countries and develop unconventional warfare campaign plans. Pre-positioned forces not only bolster the militaries of countries they are working with, but act as a deterrent and change the calculus of gray-zone aggressors.

Additionally, pre-positioning forces reduces the risk that moving US soldiers into a region involved in a gray-zone conflict will inflame the situation. Developing unconventional warfare campaign plans staffed and approved through all relevant agencies and organizations decreases the negative effects that slow-moving US bureaucratic processes have on quickly reacting to new threats in a fast-moving, fluid environment such as the gray zone. Secondly, the US Army should work with the Department of State and host nations to better integrate at-risk ethnic populations into the host country. These populations are at risk for subversion and coercion by gray-zone aggressors. By better integrating them with the host country, the US Army can limit this risk and their usefulness to gray-zone aggressors. Thirdly, the US Army should work with the Department of State and host nations to introduce and expand non-violent civil resistance programs in at-risk countries. By building non-violent civil resistance networks, the United States creates a mechanism for resisting aggressors in the gray zone. Furthermore, in the event that an aggressor takes territory, these networks can be activated, which buys time for policymakers and international institutions to determine an appropriate response to the aggressor. Finally, if necessary, these networks can be used to

identify potential allies for an unconventional warfare campaign.

Since 1918, less than 20 percent of all conflicts have been state-on-state conventional conflicts and there is nothing hinting that this will change in the future.<sup>4</sup> Therefore, we can posit that gray-zone hybrid tactics will continue to play a prominent role in future conflict. Consequently, the US Army must ensure that it is appropriately postured to counter gray-zone hybrid threats. To do this, the US Army must (1) accurately describe hybrid threats and the gray zone, (2) identify ways that it can align doctrine to counter gray-zone hybrid threats, and (3) improve capacity to do so. Doing these things will give strategists, scholars, and policymakers a shared understanding of the complexities of gray-zone conflict. Additionally, it will ensure that the Army is ready to achieve its strategic objectives wherever called upon to do so.

## II. Describing Hybrid Threats and the Gray Zone

Warfare is “the mechanism, method, or modality of armed conflict against the enemy.”<sup>5</sup>

<sup>4</sup> David Maxwell, “Congress Has Embraced Unconventional Warfare: Will the US Military and The Rest of the US Government?,” *Small Wars Journal*, December 29, 2015.

<sup>5</sup> The Joint Staff, “Joint Publication 1, *Doctrine for the Armed Forces of the United States*,” March 25, 2013.

While war hasn’t changed for thousands of years, warfare, specifically, the technology used to conduct war, is constantly changing. It evolved from soldiers with broadswords and bows, to soldiers on horseback with repeating rifles, to soldiers with machine guns, driving tanks, and calling in airstrikes from drones. Due to this continuously evolving nature, one must understand the most current tactics, techniques, procedures, and technology of warfare in order to develop and employ the appropriate capabilities needed to achieve tactical, operational, and strategic objectives.

According to Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, there are two forms of warfare, traditional and irregular, and “each serves a fundamentally different strategic purpose that drives different approaches to its conduct; this said, one should not lose sight of the fact that the conduct of actual warfare is seldom divided neatly into these subjective categories.” Hybrid threats bridge the gap and combine aspects of these two types of warfare in a single space and time.

Hybrid threats are when “an adversary simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle

space to obtain their political objectives.”<sup>6</sup> The objective of hybrid threats is to attack the seams in policy, organization, and doctrine to create leverage and exploit vulnerabilities. Consequently, it is important for the US Army to understand what hybrid threats are and how they may be employed to attack our weaknesses. Defense planners tend to try to place modes of conflict into boxes or bins that define the type of conflict and help identify the correct resources and capabilities to defeat the threat. However, hybrid threats asymmetrically attack the seams between these boxes and look to exploit the vulnerability and inadequacy of incorrectly applied capabilities.

Though hybrid threats are not new in the history of warfare (arguably, American colonists used hybrid tactics against the British in the Revolutionary War), their recent use by the Russians in Ukraine in 2014, Hezbollah in their war with Israel in 2006, and Russia’s release of the “Gerasimov Doctrine”<sup>7</sup> has

brought them to the forefront of discussion within the military and academia. Consequently, it is important that military scholars and strategists re-examine hybrid threats to determine how they will evolve, what characteristics they possess, and how the US Army can counter their employment.

Describing the current evolutions in warfare is not just important to academia and military strategists, it is also essential in helping policymakers and civilian leaders understand its changing nature. Ultimately, being able to describe the challenges faced by the military helps the Army organize and equip itself with the capabilities necessary to achieve national strategic objectives. Without describing threats and defining the current state in the evolution of warfare, it is difficult to achieve shared understanding amongst the military, the public, and policymakers. Consequently, describing and understanding hybrid and gray-zone threats employed against the United States, our friends, and our allies is vital to US national security.

<sup>6</sup> Frank Hoffman, “Hybrid vs Compound War,” *Armed Forces Journal*, October 1, 2009.

<sup>7</sup> The “Gerasimov Doctrine” refers to a vision for the future of warfare outlined by the Chief of the Russian General Staff, Gen. Valery Gerasimov, in a FEB 2013 issue of a Russian Military Journal (*Voyenno-Promyshlenny Kurier*). Many of the concepts outlined in the paper were seen during Russian actions in eastern Ukraine. However, there is some debate as to whether or not the Gerasimov Doctrine is actually Russian doctrine and the way the Russians plan to fight in the future or just Gen Gerasimov’s view of the evolution of warfare.

### *Contemporary View of Hybrid Threats*

Currently, there is little consensus among the military, scholars, and strategists as to what constitutes a hybrid threat or how to define them. While retired Lt. Col. Frank Hoffman views hybrid threats as “simultaneously and

adaptively employ(ing) a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior,”<sup>8</sup> retired Col. David Maxwell argues in his 2012 testimony before the House Armed Services Committee that “hybrid warfare” is really just a new name for irregular warfare and, in particular, its subset of unconventional warfare. The Joint Staff, in JP 1-02, defines irregular warfare as “a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations,” and unconventional warfare as “activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerilla force in a denied area.”<sup>9</sup>

However, JP 1-02 fails to define hybrid warfare or hybrid threats. Additionally, Army Doctrine Publication (ADP) 3-0, Unified Land Operations, defines hybrid threats as “the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually

benefitting effects.”<sup>10</sup> Finally, Michael Kofman and Matthew Rojansky argue that the term “hybrid” “denotes a combination of previously defined types of warfare, whether conventional, irregular, political or information” and its “analytical utility is limited.”<sup>11</sup>

Disagreements over what hybrid threats are or aren’t or whether they are a new phenomenon or something as old as war itself aside, it is important that this emerging trend is identified and discussed. Ultimately, hybrid threats attack the seams of conventional views of warfare and the strong capabilities developed by the United States to fight conventional and irregular warfare. For example, the United States began Operation Iraqi Freedom (OIF) with a strong set of conventional warfare capabilities that provided strategic overmatch against the Iraqi Army. When the Iraqi Army collapsed and the country became gripped by an insurgency, the US military had a difficult time adjusting its strategy and bringing the appropriate assets to the battlefield in order to fight a growing insurgency. Ultimately, the United States applied a counter-insurgency strategy during “the Surge” under retired Gen.

---

<sup>8</sup> Frank Hoffman, “Hybrid vs Compound War,” *Armed Forces Journal*, October 1, 2009.

<sup>9</sup> The Joint Staff, “Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms,” November 15, 2015.

<sup>10</sup> Headquarters, Department of the Army, “ADP 3-0: Unified Land Operations” (HQDA, October 2011).

<sup>11</sup> Michael Kofman and Matthew Rojansky, “A Closer Look at Russia’s ‘Hybrid War,’” Kennan Cable (Kennan Institute at the Woodrow Wilson Center, April 2015).

## Countering Gray-Zone Hybrid Threats

David Petraeus and was able to beat back the insurgency and dramatically reduce violence in order to buy time for the Iraqi government to establish security before the United States ended its combat mission in 2010.

Looking at OIF, the US Army participated in both traditional and irregular warfare and the characterization of the conflict fell into different “bins” as the conflict progressed, rarely at the same time. It started out as a traditional conflict with offensive operations to take down the regime of Saddam Hussein and stability operations to re-constitute the Iraqi government. It then moved into the realm of irregular warfare with the counter-insurgency campaigns against Al-Qaeda in Iraq and Iranian-backed Shiite militias. However, these different types of warfare involved different adversaries (i.e. different state and non-state actors) and, for the most part, did not occupy the same time period.

When faced with these different phases of warfare in the conflict, US military leaders and strategists were able to tailor their forces, capabilities, and strategies to fight and defeat the enemy (though not without significant difficulties). What led to the prolonged nature of OIF was the military’s difficulty in transitioning from offensive combat operations to stability operations and then to counter-

insurgency operations while trying to find the correct strategy to achieve the objectives in each phase. Where hybrid threats draw their utility and, ultimately, their effectiveness is their ability to exploit the seams between these “bins” by fusing different tactics from different subsets of warfare (e.g. high-intensity, guerrilla, cyber, information, etc.) together in a single space and time.

When taking Mosul, the Islamic State in Iraq and Syria (ISIS) isolated enemy combat units, disrupted effective command and control and sustainment, and simultaneously attacked multiple forces both inside and outside of the city.<sup>12</sup> This type of strategy is conventional in nature. However, ISIS executed it using weaponry typical to irregular warfare (e.g. suicide vehicle-borne improvised explosive devices), conventional weapons such as RPGs, mortars, and armored vehicles, as well as tactics more akin to terrorism such as kidnapping and operating in small teams or cells.<sup>13</sup> This fusion of the conventional, unconventional, and the criminal highlights how hybrid threats occur across multiple “bins” of warfare. When a conventional force, such as

---

<sup>12</sup> TRADOC G-2 Intelligence Support Activity – Complex Operational Environment and Threat Integration Directorate, “Threat Tactics Report: Islamic State of Iraq and the Levant,” NOV 2014: 3.

<sup>13</sup> Ibid.

## Countering Gray-Zone Hybrid Threats

the US Army, faces these type of threats, it has difficulty transitioning between different types of operations and calibrating its force levels and tactics to effectively counter these operations and achieve its objectives in each phase.

Because hybrid threats occur across multiple domains, they pose a distinct threat for US Army strategist who must understand the threat and then ensure the proper campaign plan, resources, and capabilities are in place to counter the threat. This mix is difficult to get correct because strategists must strike the right balance between forces dedicated to fighting each threat. For example, artillery is essential in a high-intensity conflict. However, artillery is largely ineffective in stability or counter-insurgency operations. Conversely, special operations forces such as civil affairs and military information support operations are more effective in stability operations than they are in high-intensity conflict. In a hybrid-threat environment, where both high-intensity combat and stability operations may exist simultaneously, planners must get the force/capability mix right within the limits imposed by civilian political leaders in order to effectively counter the threat.

Further enhancing the effectiveness of hybrid threats is the ability of nation states to use them across the peace-war continuum.

Hybrid threats can use one or more of a nation's instruments of power (diplomatic, information, military, and economic) to influence an adversary and achieve strategic objectives, often below the threshold of war in the gray zone. In essence, hybrid threats in the gray zone are often implemented to achieve objectives without violating international norms and/or crossing arbitrarily established thresholds (e.g. President Obama's "red line" on Syrian chemical weapons use) that would lead to the intervention of an adversary. For example, Russia used hybrid tactics to achieve its strategic objectives in destabilizing Ukraine and annexing Crimea without crossing a threshold that would draw other global powers into the conflict against the Russians. It is important to note that it is difficult to define these thresholds as they are often arbitrarily established and are highly dependent upon situational context, the international standing of the countries involved, and domestic politics (e.g. the United States did not initially intervene during the Rwandan genocide in 1994 nor did the United States intervene in Syria when the Assad regime used chemical weapons against civilians in 2013).

### *The Spectrum of Conflict: Hybrid Threats vs. the Gray Zone*

Recently, the concept of gray-zone conflict emerged amongst scholars, strategists, and,

particularly, members of the United States special operations community. In their recent article in *Joint Forces Quarterly* Gen. Joseph Votel, commander of US Special Operations Command, retired Lt. Gen. Charles Cleveland, former commander of US Army Special Operations Command (USASOC), Col. Charles Connell, director of the Commander's Initiatives Group at USASOC, and Will Irwin, a resident senior fellow at the Joint Special Operations University, defined gray-zone conflicts as a segment of the conflict continuum "characterized by intense political, economic, information, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war."<sup>14</sup> Essentially, gray-zone conflict encompasses the space between peace and war. Or, as defense analyst Nadia Schadlow described it, "the space between peace and war is not an empty one—but a landscape churning with political, economic, and security competitions that require constant attention."<sup>15</sup>

Contrary to what many academics and strategists have posited, the gray zone is actually an operational environment (OE), albeit

not a physical one. Additionally, gray-zone conflicts are those in which nation states and non-state actors use hybrid threats/tactics, such as fusing political and information warfare with non-violent civil resistance, to achieve strategic objectives without violating international norms or crossing established thresholds and leading to open war. Joint doctrine defines an operational environment as "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."<sup>16</sup> As the gray zone encompasses the space between peace and war in which aggressors use hybrid threats to shape the battlefield and achieve strategic objectives short of all-out, declared conflict, it is, by description, a set of conditions, circumstances, and influences that affect the ability of the US Army to employ capabilities and US Army commanders to make decisions. Consequently, the gray zone is an OE and not a type of conflict, in the same way that urban or desert warfare refers to the OE in which the conflict takes place and is not a distinct form of conflict. Though the tactics, techniques, procedures, and strategy used in each OE may differ, these areas are not a type of warfare in the same vein as irregular or conventional warfare. Irregular and conventional warfare can

---

<sup>14</sup> General Joseph Votel et al., "Unconventional Warfare in the Gary Zone," *Joint Forces Quarterly* 80, no. 1st Quarter (January 17, 2016): 101–9.

<sup>15</sup> Nadia Schadlow, "Peace and War: The Space Between," August 18, 2014, *War on the Rocks*.

---

<sup>16</sup> The Joint Staff, "Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*," November 15, 2015.

## Countering Gray-Zone Hybrid Threats

occur in any type of operational environment and are characterized by distinctly different employment of capabilities, whereas the gray zone describes conflict in an ambiguous operating environment in the “space” between peace and war.

Further, hybrid threats take place across the spectrum and in each of the “bins” of conflict as opposed to being an independent type of conflict on the spectrum. As such, on the spectrum of irregular conflict, hybrid threats are present throughout the spectrum but are broken into two types: gray-zone hybrid threats and open-warfare hybrid threats. While each type encompasses the principles outlined by Frank Hoffman, each is distinctly different in its characteristics. For example, ambiguity is much more important in gray-zone hybrid threats than open-warfare hybrid threats. More on the individual characteristics of gray-zone hybrid threats and the dichotomy between the two types will be discussed in the next section.

Some people argue that the difference between gray-zone conflict and hybrid conflict is that gray-zone conflict does not involve kinetic activity. Others argue that gray-zone conflicts can only be executed by states, while states, non-state actors, and proxies can execute hybrid threats. While these ideas may hold water at first glance, they are, ultimately,

incorrect. First, hybrid warfare does not exist in the vein that it is a separate form of warfare on par with irregular and conventional warfare. Hybrid threats exist and are best described as tactics used throughout the modes of warfare to achieve gains through the use of “simultaneously and adaptively employ(ing) a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior”<sup>17</sup> in a single space and time. Secondly, non-state actors are involved in the gray zone. Importantly, states often use proxies or work in combination with proxies while operating in the gray zone in order to maintain ambiguity that contributes to the confusion of actions in the gray zone. For example, in Crimea, Russia used criminal networks to help set the conditions for annexation,<sup>18</sup> and in the South China Sea, the Chinese use fishermen to lay claim to disputed waters and disrupt US naval activities.<sup>19</sup> Consequently, hybrid tactics and grey-zone conflict are not independent of each other; they are inextricably linked and aggressors use hybrid tactics across the spectrum of conflict to achieve their desired ends.

---

<sup>17</sup> Frank Hoffman, “Hybrid vs Compound War,” *Armed Forces Journal*, October 1, 2009.

<sup>18</sup> Dmitry Gorenberg, (January 15, 2016).

<sup>19</sup> Harry J. Kazianis, “China’s 50,000 Secret Weapons in the South China Sea,” Text, *The National Interest*, accessed February 7, 2016.

### *Characteristics of Contemporary Hybrid Threats*

First, it is important to note that no two conflicts and no two adversaries are alike. For example, if Russia were to use hybrid tactics against a Baltic state, they would be different than those used in eastern Ukraine and much different than those used by China in the South China Sea or by Hezbollah against Israel in their 2006 conflict. Tactics and strategy used in each situation are based on an analysis of the situation on the ground (or sea) and available capabilities. Consequently, the contemporary characteristics of hybrid threats are a generalization and should be applied to individual situations differently in order to help understand the situation on the ground and develop an appropriate response. Furthermore, when preparing to counter hybrid threats, it is important to “not fight the last war.” To paraphrase retired Lt. Gen. James Dubik, “We need to fight the war we’ve got, not the one we want.”<sup>20</sup>

Hybrid threats break down into two distinct categories: gray-zone hybrid threats and open-warfare hybrid threats. Gray-zone hybrid threats take place to the left of limited conventional conflict on the spectrum of

<sup>20</sup> James Dubik, “Winning the War We’ve Got, Not the One We Want,” *ARMY Magazine*, January 12, 2016.

conflict (Figure 1). They comprise political warfare, unconventional warfare, and irregular warfare. Open-warfare hybrid threats happen to the right of irregular warfare on the spectrum. The major differences between the two types are the overt use of conventional weapons/formations/tactics and a lack of ambiguity in open-warfare hybrid threats. Gray-zone hybrid threats are characterized by the use of special operations forces, irregular forces, and criminal networks employing a mix of conventional weapons and irregular tactics in a single space and time while striving for ambiguity and non-attribution.

A recent example of this dichotomy is Russian actions in Ukraine. In eastern Ukraine, the Russians used gray-zone hybrid threats to take terrain and destabilize a pro-Western government. They used Russian troops in green uniforms without insignia, took over government buildings and turned them over to unarmed civilians, and used “humanitarian” convoys to move supplies into the country.<sup>21</sup> However, in Crimea, Russia used much more overt hybrid threats to annex the region and secure the “protection” of ethnic Russians. Russia openly moved troops from its base in

<sup>21</sup> Maciej Bartkowski, “Nonviolent Civilian Defense to Counter Russian Hybrid Warfare” (The Johns Hopkins University Center for Advanced Governmental Studies, March 2015).

Sevastopol into Crimea to “protect fleet positions,” facilitated a vote in the regional government to secede from Ukraine, and publicly discussed their actions to “answer the call of its compatriots who ‘feared for their safety.’”<sup>22</sup> While not entirely considered a limited conventional war, Russia’s actions to secure Crimea were overt enough to differentiate them from gray-zone hybrid threats, as Russia did not seek to hide its actions or to avoid violating international norms, such as annexing a part of another sovereign country, that would entangle them in a broader conflict with Ukraine and upset the international community.

### *Gray-Zone Hybrid Threats*

Hybrid threats in the gray zone are unique in that they stay below the threshold of conventional conflict between states. While there may be some shooting between states, state proxies and/or non-state actors, hybrid threats in the gray zone will stay below the threshold of open, conventional conflict. The main reason for this is that aggressors in the gray zone seek to take advantage of non-attribution to shape the battlefield to achieve their strategic objectives with minimal cost in

terms of responses by other nations. This was most recently seen in Russia’s initial foray into eastern Ukraine and is also observed in Chinese actions in the South China Sea. Though not addressed as a separate characteristic in this report, operations in the human domain (defined in US Army Special Operations Command’s ARSOF Operating Concept 2022 as “the totality of the physical, cultural, and social environments that influence human behavior to the extent that success of any military operation or campaign depends on the application of unique capabilities that are designed to fight and win the population-centric conflicts”)<sup>23</sup> are a key component of gray-zone hybrid threats and are interwoven throughout the following characteristics of gray-zone hybrid threats:

*Ambiguity:* In the gray zone, ambiguity is essential to keeping conflict in the space between peace and war. Therefore, when a nation takes action in the gray zone the goal is often to achieve strategic objectives without overtly violating international norms or crossing thresholds established by political leaders which would lead to open warfare. Aggressors try to maintain ambiguity through the use of

---

<sup>22</sup> Center for Strategic and International Studies, “The Ukraine Crisis Timeline,” n.d..

<sup>23</sup> United States Army Special Operations Command, “ARSOF Operating Concept 2022,” 26 September 2014, p. 52.

proxies such as criminal networks or militias, special operations forces, intelligence operatives, or through the use of civilians to achieve objectives through non-violent means. The goal of ambiguity is to maintain plausible deniability and, thus, limit the responses of international actors and institutions such as the United States or the United Nations. This allows the aggressor state to achieve its objectives while minimizing diplomatic, military, and/or economic consequences. It is important for aggressors to maintain ambiguity throughout operations in the gray zone. Once ambiguity is lost, the aggressor is open to conflict escalation, often towards a larger, more conventional conflict, and/or sanctions and other negative diplomatic and economic actions from the international community writ large.

A recent example of an aggressor using ambiguity in the gray zone is Russia using “unidentified troops” in eastern Ukraine to secure key government buildings. Once secure, these “unidentified troops” brought in unarmed civilians to set up barricades

and stage demonstrations.<sup>24</sup> While it is very likely that these “unidentified troops” were Russian soldiers not wearing uniforms, it was ambiguous enough as to whom they were that the Ukrainians, and the rest of the world, could not say for sure who was occupying the buildings prior to the arrival of civilians. Thus, ambiguity played a key role in the Russians achieving their objectives in eastern Ukraine without drawing significant negative actions from the international community, and it plays a key role in gray-zone hybrid threats.

*Exploit Weaknesses of the Adversary Through DIME:* When using hybrid tactics in the gray zone, aggressors use a whole-of-government approach to exploit their adversary’s weaknesses through the use of diplomatic, information, military, and economic instruments of power. Often, this is more effective in autocratic regimes in which the leadership focuses the government on a single objective. Russia’s organization is especially

---

<sup>24</sup> Maciej Bartkowski, “Nonviolent Civilian Defense to Counter Russian Hybrid Warfare” (The Johns Hopkins University Center for Advanced Governmental Studies, March 2015).

effective in this regard.<sup>25</sup> Using all of a nation's instruments of power is an especially effective tactic against large, democratic bureaucracies such as the United States, because of the bureaucracy's inability to synchronize efforts and information flow across multiple branches and departments. Because of the inherent inflexibility, lack of information sharing, and time-consuming interagency processes, autocratic governments who execute a synchronized approach using all instruments of power are able to shape the battlefield and achieve their objectives within the decision cycles of the larger, more unwieldy bureaucracy. This penchant for speed and the ability to fuse different instruments of power in a single time and space provides a huge advantage to the aggressor. It often allows the aggressor to achieve its objectives while the adversary or its allies are trying to make sense of the situation, formulate a policy response, and allocate appropriate resources to react to the aggression.

In the case of the United States, our government is built on a system of

checks and balances and separation of powers which prevents a single branch of government from becoming too powerful. With respect to defense, this system is most apparent in the relationship between the president and Congress: while the President can wage war and is the commander in chief, only Congress can declare war and appropriate funds to finance military operations. This system is designed to take time and involve multiple agencies in order to prevent rash decisions. While this system is useful in large-scale conflict where there is little ambiguity and a more easily recognized threat, it is hugely disadvantageous in the gray zone where the true nature of the conflict is murky, the situation is changing rapidly, and it is difficult to develop a true common operating picture in order to achieve shared understanding across multiple agencies.

In April–May 2014 in eastern Ukraine, the Russians used their “unidentified troops” to seize government buildings in Donetsk, Luhansk, and Kharkiv, had their separatist allies in eastern Ukraine declare independence as “people’s republics,” and gathered uniformed

---

<sup>25</sup> Dmitry Gorenberg, January 15, 2016.

troops on the border of eastern Ukraine in a threat to annex the separatist-controlled territory (See Appendix C).<sup>26</sup> This fusion of the instruments of national power allowed the Russians to destabilize eastern Ukraine and ultimately led to a ceasefire and the retention of territory by Russian separatists backed up by Russian forces. (Of note is that at this point in the conflict Russia's use of hybrid tactics in the gray zone began to transition to open-warfare hybrid tactics as the Russians began to openly back the separatists with artillery and some conventional ground forces. An example of this is the use of Russian military artillery to target the strategic Ukrainian town of Debaltseve in support of separatist forces leading up to the February 2015 ceasefire.)<sup>27</sup> During this time period, the United States and its allies were unsure (at least publicly) as to the true nature of the conflict in eastern Ukraine. There was little understanding of who was operating in eastern Ukraine other than "civilians"

who were revolting against the government and Russian troops massing on the border. There was widespread suspicion that the Russians were operating in Ukraine but no tangible proof until pictures of suspected Spetnaz soldiers and Russian military equipment were crowd-sourced and identified at multiple locations throughout eastern Ukraine. Furthermore, the main concern of the US Congress at this point was the massing of Russian troops on the border, not the actions taken by Russians inside of eastern Ukraine.<sup>28</sup> This is a great example of gray-zone actions moving faster than the bureaucracy can react and the difficulty in achieving shared understanding of the true nature of the conflict amongst all parties involved.

*Attack in Five Domains: Land, Sea, Air, Cyber, Information/Propaganda:* In the gray zone, aggressors will use hybrid threats in five domains (land, sea, air, cyber, and information) to achieve their objectives. Given the uniqueness of

---

<sup>26</sup> "Ukraine Crisis in Maps," *BBC News*, accessed February 7, 2016.

<sup>27</sup> Naftali Bendavid, "Images Appear to Show Russian Artillery Targeting Ukrainian Town," *Wall Street Journal*, February 14, 2015, sec. World.

---

<sup>28</sup> Bill Gertz, "Russian Troop Movements Near Eastern Ukraine Trigger Fears of Imminent Invasion," *The Washington Free Beacon* (accessed September 11, 2016).

each situation, aggressors will conduct an exhaustive analysis of each operational environment and determine where they can achieve the most leverage in the gray zone. This analysis will lead to the aggressor determining the best domain(s) in which to use his hybrid threats. Examples of operations in each of these domains include using proxies and criminal networks on land, using swarms of attack boats or fisherman at sea, using reconnaissance drones or civilian aircraft in the air, shutting down electrical grids or conducting denial of service attacks over networks, and, finally, using information warfare and propaganda to influence the population. The goal of using all available domains is to fuse multiple tactics and techniques together in a single space and time to strain the opponent's resources and take advantage of where he is weak.

*Use of Criminal Organizations and Networks:* In the gray zone, aggressors will use criminal networks to create ambiguity, shape public perception, and move supplies around the battlefield. Criminal organizations, especially those focused on smuggling and the distribution of narcotics, have ready-

built distribution networks inside their areas of operation. These resources are susceptible to use by gray-zone aggressors because of their efficiency, built-in operational security, and ease of activation. For a price, gray-zone aggressors can use these organizations and networks to supply proxies, disrupt adversary operations, distract adversary police forces, and intimidate or coerce target populations.

While the notion of using criminal networks and organizations is uncomfortable for the American public, it isn't for many of our adversaries. For example, Russia used criminal networks during its annexation of Crimea and the current prime minister of Crimea, who is supported by Russian President Vladimir Putin, has extensive ties to organized crime.<sup>29</sup> Consequently, we must recognize that criminal networks pose unique advantages to adversaries operating in the gray zone and we must work with our partners to mitigate their effects and understand whom they are working for.

---

<sup>29</sup> Simon Shuster, "Putin's Man in Crimea Is Ukraine's Worst Nightmare," *Time*, March 10, 2014.

*Laws and Cultural Norms as a Weapons System:* When operating in the gray zone, aggressors try to use the law and international and cultural norms to their advantage. Understanding where the “red lines” are and taking actions within those boundaries to achieve strategic objectives epitomizes gray-zone conflict. Multi-national organizations such as the UN and NATO are institutions based on laws and common understanding. Furthermore, societies have their own cultures and beliefs that affect how they act. For example, the sanctity of human life is much different in eastern Europe than it is in ISIS-controlled territory in the Middle East. While these laws and norms have tremendous value and are the bedrock of our society, these same laws and norms can be used against organizations and cultures to prevent them from taking action. Furthermore, as large bodies comprised of many actors, the reaction speed of many of these institutions is inherently slow. Consequently, gray-zone actors conducting operations with speed and autonomy are able to exploit the bureaucratic processes inherent in these institutions and achieve

objectives before the institutions are able to decide upon and take appropriate action.

For example, during Russia’s actions in eastern Ukraine, Vladimir Putin openly talked about using Ukrainian citizens to shield Russian troops.<sup>30</sup> Then, they used the unwillingness to fire on unarmed citizens to stage occupations and demonstrations, as well as to seize Ukrainian army garrisons.<sup>31</sup> Furthermore, once Russian involvement in Ukraine became more overt (and Russian actions began to shift to open-warfare hybrid tactics), the Russians used legal systems and frameworks (e.g. parliamentary approval of Crimea’s annexation) to justify their actions.<sup>32</sup> Consequently, gray-zone actions are highly influenced and shaped by culture, laws, and beliefs.

---

<sup>30</sup> Maciej Bartkowski, “Nonviolent Civilian Defense to Counter Russian Hybrid Warfare” (The Johns Hopkins University Center for Advanced Governmental Studies, March 2015).

<sup>31</sup> Ibid.

<sup>32</sup> Janis Berzins, “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy” (National Defence Academy of Latvia Center for Security and Strategic Research, April 2014).

### *Open-Warfare Hybrid Threats*

Open-warfare hybrid threats are unique from gray-zone hybrid threats because they bring the full spectrum of conventional and unconventional operations to bear on a conflict. Open-warfare hybrid threats consist of all instruments of national power, proxies, terrorism, conventional tactics, unconventional warfare, and criminal elements employed and fused in a single space and time. While not all elements need to be fused together in a single space and time to qualify as hybrid tactics, multiple elements must be fused for the tactics to qualify as hybrid. Open-warfare hybrid threats are considered “traditional” hybrid warfare. They occur when countries are involved in open conflict and, while there may be some instances where ambiguity is helpful, for the most part aggressors are not trying to hide their involvement in conflict. Recent examples of open-warfare hybrid threats include the 2006 war between Hezbollah and Israel as well as Russian actions during the annexation of Crimea. In this report, I will not go into the characteristics of open-warfare hybrid threats, as there is a large amount of literature already written on them. Chief among those is Frank Hoffman’s 2009 article in Armed Forces Journal titled “Hybrid vs. Compound War.”<sup>33</sup>

---

<sup>33</sup> Frank Hoffman, “Hybrid vs Compound War,” *Armed Forces Journal*, October 1, 2009.

### *Findings and Recommendations*

Hybrid threats and the gray zone are important concepts to define as they allow strategists, leaders, and policymakers to achieve shared understanding regarding the complexity of modern conflict and the capabilities needed to fight and win in a complex world. While previously well documented, hybrid threats have not been applied to gray-zone conflict and their description thus needs to be updated.

The gray zone is the space between peace and war. It is an operating environment in which aggressors use ambiguity and leverage non-attribution to achieve strategic objectives while limiting counter-actions by other nation states. Inside the gray zone, aggressors use hybrid tactics to achieve their strategic objectives. While hybrid threats have historically been associated with irregular and conventional warfare, their use in the gray zone leads to a dichotomy between two types of hybrid threats that can mainly be attributed to the need for ambiguity and non-attribution in the gray zone. The two types of hybrid threats are “open-warfare hybrid threats” and “gray-zone hybrid threats.”

The characteristics of gray-zone hybrid threats include: (1) ambiguity (2) exploitation of adversary weaknesses using all elements of

national power (3) attacks from land, sea, air, information, and cyber (4) use of criminal organizations and networks, and (5) the use of laws and cultural norms as a weapons system. While some of these can be found throughout the spectrum of conflict, ambiguity, the use of criminal organizations and networks, and the use of laws and cultural norms against an adversary differentiate gray-zone hybrid threats from tactics used in limited or conventional war. Furthermore, ambiguity distinguishes gray-zone hybrid threats from open-warfare hybrid threats as it allows the aggressor to maintain plausible deniability and achieve its goal of accomplishing strategic objectives without causing the United States to intervene.

Moving forward, the Army needs to evaluate if its definition of hybrid threats in ADP 3-0, “the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects,” is sufficient to address the complexity of hybrid threats both in and out of the gray zone. It must also decide if this definition is too broad and does not allow leaders, strategists, and policy makers to achieve shared understanding with respect to the nature of hybrid threats and the capabilities needed to defeat them. Finally, the Army needs to decide if the gray-zone concept is worth

defining in our doctrine and, if so, how it fits into the overall scheme of Army operations.

### **III. Identifying and Adapting to Challenges Posed by Gray-Zone Hybrid Threats Due to Laws, Norms, and Processes**

#### *Challenges Posed by Gray-Zone Hybrid Threats*

Hybrid threats pose a myriad of challenges to the US Army, as they are specifically designed by the aggressor to exploit the weaknesses of the adversary. In the case of the United States, our biggest weakness in the gray zone is our bureaucracy and our inability to understand and react quickly to adversary actions in the gray zone. While bureaucracy can be an advantage in getting a large organization to accomplish its mission, it is generally unwieldy, slow, and inflexible. As a result, adversaries are realigning their organizations and developing doctrine and capabilities targeted at exploiting our slow reaction time in the gray zone. This slow reaction time ultimately stems from our bureaucratic processes and, in particular, the difficulties in getting large organizations to work together to identify actions and trends and then come to a common understanding about what is happening and developing and executing an appropriate response. This problem is compounded when multiple large organizations, for example the Department of Defense,

## Countering Gray-Zone Hybrid Threats

Department of State, and the Central Intelligence Agency, are involved in understanding and solving a problem. In essence, the new capabilities and tactics developed by our adversaries are designed to operate within our decision cycle, exploit our inability to react, and allow them to reach strategic objectives before we can counter their actions.

The solution to this problem is outlined in ARSOF 2022, the US Army Special Operations Command's strategic blueprint for the future: "Dealing with transnational and hybrid organizations requires a high level of ongoing, real-time cooperation with JIIM (Joint, Interagency, intergovernmental and multinational) organizations reliant on established responsibilities understood by all participants. Hybrid teams consisting of military, law enforcement, and composite authorities will become the new norm to counter transnational and hybrid threats. SOF operational design will be optimized in the human domain and in operations not led by the Department of Defense (DOD)."<sup>34</sup>

An example of an adversary creating doctrine to exploit weaknesses of large

bureaucracies is Russia's hybrid threat doctrine, known as "New Generation Warfare" or the "Gerasimov Doctrine." This doctrine was designed to take place in the gray zone and within adversaries' decision cycles. This strategy was designed around the weaknesses of Russian adversaries to include the United States.<sup>35</sup> In an article for the Russian military, Russian Chief of the General Staff Valery Gerasimov the doctrine based on his views on the future of warfare:

*Wars are no longer declared and, having begun, proceed according to an unfamiliar template... [A] perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a morass of chaos, humanitarian catastrophe, and civil war.... The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness... The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures — applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. The open use of forces — often under the guise of peacekeeping and crisis regulation — is resorted to only at a*

---

<sup>34</sup> United States Army Special Operations Command, "ARSOF Operating Concept 2022," 26 September 2014, p. 8.

<sup>35</sup> David Maxwell, January 8, 2016

*certain stage, primarily for the achievement of final success in the conflict.<sup>36</sup>*

In Gerasimov's description of the future of warfare, hybrid threats in the gray zone will play a big role. Gerasimov sees the non-military elements of national power as an important part of achieving Russian strategic objectives. Further, he highlights the fact that non-military means will be supplemented by the use of military force either covertly through the use of special operations forces or overtly "under the guise of peacekeeping and crisis regulation."

### *Russia's "New Generation Warfare" vs. US Doctrine*

Russia's "New Generation Warfare" can be organized and broken down into an eight-phase planning construct. US planning processes, by comparison, generally use a six-phase construct. The alignment of these two doctrines against each other (Figure 2) is problematic because the Russian operational process allows for multiple actions within a single phase of the US operational process. Essentially, Russia can act within the decision cycle of the US military, resulting in greater Russian agility and reduced US ability to react to Russian aggression.

The six-phase vs. the eight-phase construct is not problematic on the surface. However, the first four phases of New Generation Warfare fall within a single phase of US operational planning: Phase 0. This is an issue because there are more stringent authorities and coordination required with other government agencies when the US military seeks to operate within Phase 0. To put it bluntly, the Russian construct codifies their ability to operate and be agile in an area in which the US military is constrained in its ability to operate due to the bureaucracy of the interagency process and its lack of authority to operate freely and independently. While this does not mean that the US military cannot request and receive these authorities, it does mean that the US Army must work harder to achieve an understanding of the situation on the ground at an early stage and to ensure common understanding across all involved agencies in order to move quickly enough to receive authorities.

---

<sup>36</sup> Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, accessed December 2, 2015.

Figure 2: US vs. Russian Operational Phases

Russian “New Generation Warfare” Doctrine <sup>37</sup>		Hybrid Threat	US Operation Planning Doctrine <sup>38</sup> (See Appendix B)	
Phase 1:	Non-military asymmetric warfare to establish favorable political, economic, and military set up	Gray-Zone Hybrid Threats	Phase 0: Shape	Joint and Multinational operations—inclusive of normal routine military activities—and various interagency activities performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies
Phase 2:	Special operations to mislead political and military leaders			
Phase 3:	Intimidating, deceiving, and bribing government and military officers to make them abandon their service duties		Phase 1: Deter	Deter undesirable enemy adversary action by demonstrating capabilities and resolve; includes activities to prepare forces and set conditions for deployment and employment of forces
Phase 4:	Destabilizing propaganda to increase discontent among population; arrival of Russian militants			
Phase 5:	Establishment of no-fly zones over country to be attacked, imposition of blockades, use of private military companies		Phase 2: Seize Initiative	Seize initiative through application of appropriate joint force capabilities
Phase 6:	Commencement of military action			
Phase 7:	Combination of targeted information, electronic warfare, space operations, combined with use of high-precision weapons		Phase 3: Dominate	Break the enemy’s will for organized resistance or control the operating environment
Phase 8:	Destruction of remaining enemy points of resistance		Phase 4: Stability	Stabilize environment when there is no fully functional, legitimate civil government authority present
			Phase 5: Enable Civil Authorities	Support legitimate civil governance in theater; enable viability of civil authority

<sup>37</sup> Janis Berzins, “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy” (National Defence Academy of Latvia Center for Security and Strategic Research, April 2014).

<sup>38</sup> The Joint Staff, “Joint Publication 5-0, *Joint Operational Planning*,” August 2011.

Some may argue that comparing the Gerasimov Doctrine to the US phasing construct is unfair because the US phasing construct does not always take place in a linear fashion. Furthermore, the most likely US elements to operate in the gray zone are special operations forces, in particular US Army special forces. Consequently, comparing the Gerasimov Doctrine to the phases of unconventional warfare (Preparation, Initial Contact, Infiltration, Organization, Buildup, Employment, and Transition)<sup>39</sup> may seem like a better way to identify issues relating to operations in the gray zone. However, viewing the Gerasimov Doctrine through this lens does not provide the proper insight into the misalignment of US doctrine with Russian doctrine. In order to execute an unconventional warfare campaign, the US Army must staff its proposal through the National Security Council and have its operations approved by the president. The difficulties that arise in the gray zone from the Gerasimov Doctrine come from the fact that the US bureaucracy can't act quickly enough to get to this approval in new theaters of operation. Thus, a comparison between the Gerasimov Doctrine and the US phases of unconventional warfare would only be appropriate for gray-zone conflict in which the United States has

already received approval from the president to conduct an unconventional warfare campaign and would already have the authorities and shared responsibilities in place to execute operations in the gray zone. The fundamental problem with countering operations in the gray zone takes place when the United States cannot clearly identify gray-zone actors and actions (ambiguity) nor develop a clear common operating picture of actions taking place. In this case, the United States will be constrained by a bureaucracy that will likely not authorize operations until there is a clear threat. At this point, it is too late and the adversary has already used gray-zone operations to shape the battlefield and achieve its strategic objectives.

Further, without a concerted effort to coordinate actions, fuse intelligence, and have a well-developed and shared common operating picture across multiple agencies (e.g. Department of Defense, Department of State, National Security Council, Central Intelligence Agency, etc.), the US military would be hard-pressed to take action prior to Phase 5 of Russian operations (i.e. the deterrence phase of US operations, Phase 2). At this point, the Russians will have already set the conditions needed to commence military action through the use of hybrid tactics encompassing all elements of national power to include covert military actions. Additionally, any US actions to

<sup>39</sup> United States Army Special Operations Command, "Unconventional Warfare Pocket Guide," April 2016.

deter the Russians at this phase may be seen as provocative and inflame the situation as the Russians have already begun transitioning to overt operations (e.g. a “no-fly” zone).

For example, let's use a fictional scenario using Latvia, a Baltic, NATO member state with a large number of ethnic Russians (approximately 26 percent).<sup>40</sup> Russia has publicly stated that it will defend its “compatriots”: ethnic Russians, Russian speakers, their families, and others who have cultural or other connections with the Russian federation.<sup>41</sup> Furthermore, it has historically pursued a strategy of defense-in-depth and shown a willingness to disrupt and/or overthrow pro-Western governments such as that in Ukraine.<sup>42</sup> While Latvia is a NATO member state and could use Article IV or V to counter Russian aggression, Russia could execute New Generation Warfare in the gray zone if it viewed Latvia as a large enough threat to Russian interests. Russian operations would attempt to destabilize the country and achieve

---

<sup>40</sup> Central Intelligence Agency, “CIA World Fact Book,” February 5, 2016.

<sup>41</sup> Vera Zakem, Paul J. Saunders, and Daniel Antoun, “Mobilizing Compatriots: Russia’s Strategy, Tactics, and Influence in the Former Soviet Union” (Center for Strategic Studies, November 2015).

<sup>42</sup> Janis Berzins, “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy” (National Defence Academy of Latvia Center for Security and Strategic Research, April 2014).

strategic objectives without causing Latvia to invoke Article V. To do this, Russia could execute something like the following scenario:

*Phase 1:* Russia engages ethnic Russian politicians and political groups to mobilize and protest against Latvia’s pro-Western government. Additionally, Russian agents or proxies get pro-Russian businesses to work against Latvia and Russia uses cyber operations to disrupt the economy and electrical grid in pro-Russian enclaves, thus, sowing discord against the Latvian government.

*Phase 2:* Russia conducts information operations through special operators, diplomats, social media, and pro-Russian print, radio, and TV media to discredit the Latvian government and begin to foment resistance.

*Phase 3:* Russia bribes military officers and government officials to abandon their duties or to sabotage counter-Russian operations/narratives/legislation.

*Phase 4:* Russia floods Latvia’s pro-Russian population with propaganda alleging atrocities and repression by the Latvian government.

*Phase 5:* Russia establishes a no-fly zone over pro-Russian territory in Latvia in order to protect their “compatriots.” Though some may view this as an act sufficient to trigger NATO Article V, if the Russians are defending their “compatriots” in the absence of large-scale Latvian forces, it may not be enough to tip the scales of international condemnation and lead to the invocation of Article V.

Obviously, these phases may happen concurrently and may take months or years; success wouldn't be instantaneous. However, why hybrid tactics in the gray zone are so effective is that Russia has set the conditions for a successful “defense” of its ethnic population in Latvia through the use of all elements of national power and without firing any shots or crossing any “red lines” which would create conflict and could possibly result in the invocation of NATO's Article V. Furthermore, the majority of these actions were taken within Phase 0 of US military operations. It is likely that, given the current authorities and interagency construct, the US military would not be authorized to move larger numbers of troops or implement a counter to Russian aggression until Phase 4 of the Russian operations. At this point, any large movement of US forces would likely be seen as a

provocation and an attempt to seize territory held by Russian “compatriots.” As a result of this provocation, it is possible that Russia would quickly move to establish a no-fly zone (Phase 5) which would, in turn, further provoke the United States and NATO.

Clearly, Russia is able to accomplish its objectives in Latvia (seize territory held by pro-Russian populations, create a buffer between itself and a NATO state, and disrupt a pro-Western government on its border) without firing a shot or provoking the West. Furthermore any overt action taken by the United States and/or NATO could actually be seen as a provocation and inflame the situation. The “sweet spot” for engaging an adversary in the gray zone is towards what the Russians would classify as Phase 4. However, in order to take action here the United States must have the right conditions: a common understanding of what the Russians are doing amongst all agencies in both the United States and host-nation governments, a solid campaign plan prepared to be executed, the appropriate authorities to act within the affected country, and, most importantly, the requisite number of US forces in place with the capabilities and equipment necessary to execute their mission.

### *Findings and Recommendations*

The Russian concept of “New Generation Warfare” is designed to use gray-zone hybrid threats. It is focused on using non-military means of achieving political and strategic goals as well as military means “of concealed character” to include the open use of forces “often under the guise of peacekeeping and crisis regulation” to accomplish objectives. These tactics and techniques are particularly effective against the United States in the gray zone due to laws and regulations affecting our ability to act in Phase 0. Specifically, our bureaucracy and the lack of agility in the interagency process allow the Russians to execute their doctrine and get within our decision cycle.

Without concerted efforts to coordinate actions, fuse intelligence, and develop a common operating picture across all agencies, the US Army will have difficulty responding to Russian gray-zone actions prior to Phase 5 of Russian operations (i.e. the deterrence phase of US operations, Phase 2 as outlined in Figure 3). This is problematic because introduction of US troops into the region during this phase may escalate the situation instead of deterring Russian aggression. Consequently, the US Army needs to work with interagency partners to understand the threat and take actions to dissuade and deter the threat as early in Phase

0 as possible. Ideally, this would happen prior to or early in Phase 4 of Russian operations—the use of propaganda and introduction of Russian militants.

In order to align doctrine with gray-zone hybrid threats, the Army first needs to conduct an analysis of gray-zone doctrine from the most likely gray-zone adversaries (Russia, China, and Iran). If commonalities are found in the doctrine related to actions in Phase 0 of US operations, it would be pertinent to look at the US phasing construct and/or likely actions within Phase 0 to see if they are adequate to counter actions by these likely aggressors and address current and future threats. Secondly, the US Army needs to look at systems and processes used to fuse intelligence and create shared understanding across multiple agencies. If the systems and processes are inadequate to quickly and efficiently share information, then these issues need to be addressed.

Finally, when it comes to gray-zone operations, more academic research and thought needs to be done to determine where countries cross the line between competition and conflict. For example, in the South China Sea, China is finishing the construction of islands that may include lucrative fisheries and mineral deposits within what it claims as its exclusive economic zone. Is this considered competition

between China and its South China Sea neighbors or conflict? As it currently stands, it is unclear where this line is and it appears that the international community is upset with China but unwilling to take action that would lead to conflict. However, what is clear is the transition between the gray zone and open conflict: when ambiguity disappears, shooting starts, and countries begin to conduct limited or theater conventional war. Therefore, the right limits of the gray zone are clearly defined but the left limit, the transition between competition and conflict, is still unclear. Consequently, it would benefit the US Army to clearly define this transition from competition to conflict in order to best posture itself to counter emerging gray-zone hybrid threats.

### **IV: Improving US Army Capacity to Counter Gray-Zone Hybrid Threats**

In addition to the recommendations given in previous chapters, there are five things the US Army can do to improve its capacity to counter gray-zone hybrid threats. These recommendations are based on identifying and understanding the threat in order to create shared understanding and a common operating picture as well as reducing the risk undertaken by the United States and its allies in the gray zone. Furthermore, the majority of these

recommendations lie in the human domain. As countering gray-zone hybrid threats is largely dependent on stripping an aggressor of ambiguity and, thus, reducing his ability to operate, improving capacity in the human domain is essential to building networks, relationships, and systems necessary to identify and communicate aggressor actions upward and across multiple organizations.

#### *Identifying and Understanding the Threat*

Special operations forces are essential in providing understanding of the human terrain. They are able to engage early, understand what is happening, and identify options to shape, deter, and influence actors in the gray zone.<sup>43</sup> This is essential to identifying and understanding aggressor actions in the gray zone and stripping the aggressor of ambiguity, a key component of gray-zone hybrid threats. Because of their unique capabilities, special operations forces are the quintessential force for actions in the gray zone and the US Army must continue to build upon their unconventional warfare capabilities in order to

---

<sup>43</sup> Howard Altman, "'Gray zone' Conflicts Far More Complex to Combat, Says SOCOM Chief Votel," *Tampa Tribune*, November 28, 2015, <http://www.tbo.com/list/military-news/gray-zone-conflicts-far-more-complex-to-combat-says-socom-chief-votel-20151128/>.

successfully counter aggressive actors in the gray zone.

The two missions of US Army special operations are special warfare and surgical strike.<sup>44</sup> Surgical strike is as it sounds: “the execution of activities in a precise manner that employ special operations forces in hostile, denied, or politically sensitive environments to seize, destroy, capture, exploit, recover or damage designated targets, or influence threats.”<sup>45</sup> Special warfare, on the other hand, “is the execution of activities that involve a combination of lethal and non-lethal actions taken by a specially trained and educated force” and includes unconventional warfare, foreign internal defense, counter-insurgency operations, stability operations, special reconnaissance, and security force assistance.<sup>46</sup>

Unconventional warfare (UW) is defined as “activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerilla force in a denied area.”<sup>47</sup>

<sup>44</sup> Headquarters, Department of the Army, “ADP 3-05: Special Operations” (HQDA, August 2012), [http://armypubs.army.mil/doctrine/DR\\_pubs/dr\\_a/pdf/adp3\\_05.pdf](http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp3_05.pdf).

<sup>45</sup> Ibid

<sup>46</sup> Ibid

<sup>47</sup> Ibid

In the gray zone, many of the tactics, techniques, procedures, and capabilities needed to counter an aggressor are the same as those needed to enable a resistance movement to disrupt or overthrow a government using unconventional warfare.

Recent uses of UW by the US Army special forces include the beginning of the war in Afghanistan, when US special forces enabled the Northern Alliance to overthrow the Taliban, and working with the Kurds in northern Iraq in 2003. However, the majority of US Army special forces operations over the past fifteen years were focused on counter-terrorism, stability operations, or foreign internal defense. It wasn’t until the recent operations against ISIS in Syria that US special forces regularly conducted unconventional warfare. Consequently, their ability to conduct UW has atrophied and the institutional knowledge about UW that resided among enlisted special forces members has largely disappeared. As a result, the US Army Special Operations Command and the US Army Special Forces Command have worked to re-establish unconventional warfare capabilities within the special forces by adjusting force structure and creating units that focus specifically on unconventional warfare.<sup>48</sup>

<sup>48</sup> Joseph Trevithick, “The US Army Has Quietly Created a New Commando Division,” *Medium*, November 26, 2014, <https://medium.com/war-is->

## Countering Gray-Zone Hybrid Threats

In addition to the special forces, the Army must prevent further cuts and, if possible, increase its civil affairs and military information support operation capabilities. Similar to special forces, these members of the special operations community are able to go into environments, build networks, identify organizations that would be helpful in resisting an aggressor, and conducting operations to influence at-risk populations. Consequently, they possess skill sets that are essential to countering hybrid threats in the gray zone and the Army should work to preserve them in any future changes to force structure.

Additionally, the Army should continue to increase broadening opportunities focused on advanced civil schooling for officers and senior non-commissioned officers serving in special operations forces. Hybrid threats in the gray zone, and operations in the gray zone in general, pose significant challenges to the United States. Because these techniques allow adversaries to operate within the constraints of international norms and laws, often in an ambiguous manner, it is difficult for the United States to attribute actions to a specific nation and even more difficult to piece multiple actions together and understand them as a campaign plan to achieve specific objectives without

---

boring/the-u-s-army-has-quietly-created-a-new-commando-division-2b90961b4821.

conflict. Consequently, it is important that we have highly competent, educated personnel who can think critically and put individual actions of an adversary into the context of a broader strategy while operating in the gray zone. Furthermore, these individuals must be able to communicate their findings upwards and across multiple agencies in order to achieve the shared understanding necessary to react in time to counter gray-zone hybrid threats. Given the current force structure and where the US Army's unconventional warfare capacity resides, it is likely that the soldiers operating in the gray zone will be NCOs and officers serving in military intelligence, special forces, civil affairs, and military information support operations specialties.

Institutional training, such as the Special Forces Qualification Course and the respective courses for civil affairs and military information support operations soldiers, are important. However, institutional training is limited in its ability to provide depth on different subject areas due to time and resource constraints. A way to acquire depth in specific subject areas and improve critical and creative thinking skills is the advanced civil schooling program (ACS). ACS provides the opportunity for officers to become fully immersed in an academic environment and focus on specific areas of expertise.

However, the ACS program is relatively limited as it is only open to officers and offers the opportunity to only 412 students each year.<sup>49</sup> Outside of the ACS program, there are a few US Army broadening opportunities that provide the opportunity for a very limited number of officers and non-commissioned officers to receive an advanced degree. However, there are no widespread programs which offer advanced degrees to junior officers prior to company or detachment command, to non-commissioned officers, or that allow non-commissioned officers time to complete an in-residence bachelor's degree. This is an issue because, in the gray zone, the soldiers on the ground making the majority of assessments and executing US policy are not likely to be field grade officers with advanced degrees but young officers serving as special forces and civil affairs team commanders and their non-commissioned officers. While capable and competent, the soldiers at this level serving in the gray zone would be well served with more advanced civil schooling as it increases critical thinking skills and provides expanded opportunities for cultural immersion and developing social networks comprised of both foreign and domestic entities.

---

<sup>49</sup> United States Army, "My Army Benefits: Advanced Civil Schooling," n.d..

Furthermore, in accordance with current Army policy, the officers that lead these teams hold those positions for only 12–24 months. During this timeframe, the maximum time that the leader could be deployed is twelve months. Consequently, the most educated member of the team serving in the gray zone has little time to develop the cultural nuances, relationships, and institutional knowledge of the country he or she is serving in. The backbone of these teams, who have multiple deployments and, sometimes, years of deployed time in countries where gray-zone aggressors may take action are the non-commissioned officers. Consequently, it would be advantageous, and a tremendous force multiplier, for the Army to expand the educational opportunities for senior non-commissioned officers with a focus on those senior non-commissioned officers serving in special operations forces.

Some may argue that educational programs are too expensive and that, given a shrinking Army budget, there are competing priorities for funding. While I acknowledge the shrinking budget, the comparative cost of educating officers and non-commissioned officers is little and the return on investment is large. For example, a program that sent 1,000 officers and non-commissioned officers to a two-year academic program at a major university in the United States costing \$30,000

per year to attend would cost the Army \$30 million per year, without taking into account any increases in basic allowance for housing rates (the median cost of in-state tuition for an undergraduate degree is \$9,410/year<sup>50</sup> and the average cost for a master's degree in international relations is \$50,000/year<sup>51</sup>). This cost is less than one Apache helicopter (\$35 million) and a little more than one Paladin/FAASV Integrated Management system (\$25 million).<sup>52</sup> However, the return on investment for the education of these officers and senior non-commissioned officers is tremendous. While the Apache and the Paladin system may not be used in the gray zone, a large cohort of soldiers with advanced critical and creative thinking skills who have an expertise in the area in which they are operating would bring tremendous capabilities to interpreting and countering gray-zone actions by adversaries of the United States. As ARSOF 2022 so eloquently states in its "SOF Truths," humans are more important than

---

<sup>50</sup> "2015-16 In-State Tuition and Fees at Public Four-Year Institutions by State and Five-Year Percentage Change - Trends in Higher Education - The College Board," accessed March 18, 2016.

<sup>51</sup> "How Much Does a Master's in International Relations Cost? - CostHelper.com," *CostHelper*, accessed March 18, 2016.

<sup>52</sup> Office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer, "Program Acquisition Cost By Weapon System" (US Department of Defense, March 2014).

hardware<sup>53</sup> and, consequently, the investment in their education is well worth the cost.

Additionally, some may argue that conventional forces are finding themselves operating in the gray zone at a much higher rate and, as a result, also deserve increased opportunities for advanced civil schooling. While this is true, special operations forces are a better starting point for the expansion of the ACS program to junior officers and non-commissioned officers due to the relative complexity of their mission set compared to the average conventional force unit operating in the gray zone. Additionally, special operations forces non-commissioned officers are, generally, more educated and have a greater probability of successfully completing a rigorous collegiate-level education program than their conventional counterparts.

### *Reducing Risk*

As outlined in the challenges posed by hybrid threats in the gray zone, one of the main issues is the risk of escalation once the United States has identified an adversary is taking actions in the gray zone. In order to minimize the risk of escalation, it is prudent for the US

---

<sup>53</sup> United States Army Special Operations Command, "ARSOF Operating Concept 2022," 26 September 2014, p. 23.

## Countering Gray-Zone Hybrid Threats

Army to position forces in countries susceptible to gray-zone incursions by adversaries. The number of US forces in susceptible countries does not have to be great as they act as a deterrent just by being there. The presence of US forces in an at-risk country amplifies the risk for a potential aggressor because they will be worried about a miscalculation resulting in an engagement of the US forces. An action such as this would result in a loss of ambiguity, the crossing of a “red line” with the most powerful actor in the world, and a possible escalation of the conflict. Consequently, the presence of US forces greatly changes the calculus employed by aggressors in the gray zone.

Some may argue that pre-positioning US forces in at-risk countries may needlessly increase tensions with adversaries. This may be the case, but, pre-positioning US forces in at-risk countries before gray-zone actions begin is less likely to increase the chance of conflict due to their pre-positioning than moving in forces after gray-zone actions are well underway (e.g. after Phase 4 of Russian operations). Consequently, the pre-positioning of forces incurs less risk than positioning forces when conflict is already underway.

An example of what positioning US forces in at-risk countries could look like is Operation Atlantic Resolve (OAR). OAR is a

multitude of multinational training and security cooperation activities taking place throughout Eastern Europe in support of US and NATO allies.<sup>54</sup> The presence of US forces amplifies the risk involved for the Russians in executing operations in the gray zone because of the consequences of potential miscalculations and/or the potential loss of ambiguity. As a result, these forces serve as a deterrent to Russia aggression by changing the calculus used to decide what actions the Russians are willing to take in Eastern Europe.

However, positioning of US forces in at-risk countries does have some drawbacks. First, it is expensive. The European Reassurance Initiative, which pays for Operation Atlantic Resolve, cost the Department of Defense \$985 million in FY 2015 with another \$789 million requested for FY 2016.<sup>55</sup> Secondly, positioning forces in at-risk countries to serve as a deterrent obviously runs the risk of not deterring an aggressor. If the aggressor still takes action that engages the US forces, then the United States will have little choice but to engage in further conflict against the aggressor.

---

<sup>54</sup> US Army Europe, “Operation Atlantic Resolve,” n.d..

<sup>55</sup> Office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer, “European Reassurance Initiative,” Department of Defense Budget FY 2016 (US Department of Defense, n.d.).

## Countering Gray-Zone Hybrid Threats

This creates an issue if the forces are engaged in a country in which the political environment at home in the United States does not support going to war over. Though the risk of US forces being engaged in an at-risk country is low, it does exist and these consequences should be considered prior to deploying forces.

If pre-positioning forces is not feasible due to cost or political constraints, the US Army should, at a minimum, create an unconventional warfare campaign plan for at-risk countries that is staffed and approved by all relevant organizations and authorities (e.g. Department of State, intelligence agencies, National Security Council, etc.). The plan should clearly delineate and outline responsibilities and authorities in an at-risk country should an adversary begin to take action in the gray zone. The purpose of this advance planning should be to reduce the time needed for the US governmental bureaucracy to approve operations to counter adversary actions in the gray zone and, thus, greatly improve the ability of US forces to counter adversaries in the gray zone.

In addition to pre-positioning forces in at-risk countries, the United States should also work with host nations to integrate minority ethnic groups and other at-risk populations. As outlined in the challenges posed by gray-zone hybrid threats, ethnic groups, especially Russian

ethnic groups which are marginalized and not integrated into society, are at particular risk to be engaged and manipulated by an adversary when conducting operations in the gray zone. These ethnic groups are at risk because they share cultural, language, and historical ties with a potential aggressor and are located in a country that may be a target for hybrid threats in the gray zone. An aggressor, such as Russia, may exploit these ties in order to manipulate the population to help it achieve its strategic objectives. An example of this was in Crimea where Russia used cultural and historical ties with ethnic Russians to encourage them to denounce the government of Ukraine and legitimize Russia's annexation of Crimea.<sup>56</sup> Additionally, in eastern Ukraine, the Russians used an "unidentified military force" to take over key buildings and then brought in unarmed, pro-Russian civilians who set up barricades and staged sit-ins and demonstrations.<sup>57</sup>

Examples of pro-Western countries with large Russian ethnic minority populations include: Estonia (25 percent), Latvia (26

<sup>56</sup> Janis Berzins, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy" (National Defence Academy of Latvia Center for Security and Strategic Research, April 2014).

<sup>57</sup> Maciej Bartkowski, "Nonviolent Civilian Defense to Counter Russian Hybrid Warfare" (The Johns Hopkins University Center for Advanced Governmental Studies, March 2015).

percent), Kazakhstan (23 percent), and Ukraine (17 percent) [See Appendix D].<sup>58</sup> In some of these countries, particularly Kazakhstan and Latvia, the ethnic Russian minorities feel that the government discriminates against them by pressuring them to not speak their native language (Russian) and that they are underrepresented in political positions of power.<sup>59</sup> By discriminating against the ethnic Russians, or at best, making them feel as if they aren't natives and part of that country, these states are creating ripe opportunities for aggressors to manipulate and subvert these marginalized ethnic populations to take action to disrupt their governments in order to give Russia an advantage in the gray zone. To further demonstrate this point, a recent example of marginalized ethnic groups being undermined and taking actions against the government are Muslims in Belgium. Members of this minority group were subverted by ISIS and are responsible for the 2015 terror attacks in Paris and Brussels.

Integrating ethnic minorities takes away significant capabilities for adversaries attempting to operate in the gray zone. First,

their ability to mobilize civic groups and organizations through propaganda and misinformation is severely limited. Furthermore, their ability to achieve ambiguity by posing as an ethnic minority group upset with the host-nation government is severely hindered. If the ethnic minority population is well integrated and accepted in society, protests and demonstrations against the host nation will be out of the ordinary and quickly arouse suspicion.

In order to decrease the vulnerability of these ethnic groups the US Army needs to work with the State Department and host nations to encourage governments to integrate these at-risk ethnic groups. By integrating them into society and respecting their ties to their countries of origin, the host nation is actually ensuring that the ethnic minorities feel accepted and represented in society. If this is the case, they will feel a part of society and be much more difficult to subjugate and manipulate for the purpose of setting the conditions for an adversary to achieve strategic objectives in the gray zone. Furthermore, research has shown that increasing social integration decreases the ability of minority groups to undertake collective action.<sup>60</sup>

---

<sup>58</sup> Central Intelligence Agency, "CIA World Fact Book," February 5, 2016.

<sup>59</sup> Michael Birnbaum, "In Kazakhstan, Fears of Becoming the next Ukraine," *The Washington Post*, (May 1, 2015).

<sup>60</sup> Rahsaan Maxwell, *Ethnic Minority Migrants in Britain and France: Integration Trade Offs* (Cambridge University Press, 2012).

## Countering Gray-Zone Hybrid Threats

Consequently, integration reduces the ability of aggressor states to mobilize minority groups to take collective action to achieve strategic objectives for the aggressor.

On a strategic level, working to integrate at-risk ethnic groups could involve the State Department working with the host nation to ensure better political representation for at-risk ethnic groups or encouraging the host nation to be more inclusive of ethnic and religious minorities. In nations in which the military has a stronger relationship with the host nation, the Army could take the lead on these initiatives with the support and advice of the State Department. On the tactical level, working to integrate at-risk ethnic groups could include providing civil affairs or conventional soldiers (i.e. manpower) to help run outreach/integration programs supported by the host nation and/or working with the State Department to provide funding for local programs which encourage better integration of at-risk ethnic and religious minorities.

Additionally, the United States government should work to build non-violent civil resistance capabilities. In the gray zone it is possible that an aggressor may move to seize territory before the United States can respond or has the political will to respond. In order to help undermine the ability of the aggressor to

seize and hold this terrain, it is necessary to build capabilities in countries that may not have the military force to resist the aggressor nation (for example, small countries in Eastern Europe). One way to do this is to build the capacity to conduct non-violent civil resistance.

Non-violent civil resistance is the use of non-violent actions such as protests, sit-ins, traffic jams, work stoppages or slows, and other types of disturbances to disrupt the activities of an occupier and achieve strategic objectives without the use of violence. Studies have shown that non-violent resistance is twice as effective as violent resistance in achieving stated goals.<sup>61</sup> Strategic goals of non-violent civil resistance can include preventing or delaying an adversary from achieving campaign objectives, undermining an adversary's willingness or ability to continue a campaign, and unifying occupied territories and society.<sup>62</sup> Examples of successful non-violent civil resistance campaigns in the past include the Danish resistance of the Nazis in World War II and the

---

<sup>61</sup> Erica Chenoweth and Maria Stephan, "Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict," *International Security* 33, no. 1 (2008): 7–44.

<sup>62</sup> Maciej Bartkowski, "Nonviolent Civilian Defense to Counter Russian Hybrid Warfare" (The Johns Hopkins University Center for Advanced Governmental Studies, March 2015).

people of Czechoslovakia's resistance of the Soviets in 1968.<sup>63</sup>

In order to build capacity for non-violent civil resistance, the US Army would have to work with the State Department and at-risk nations to develop a concept for implementing non-violent civil resistance should an aggressor invade them. Some of the main challenges of implementing a plan of non-violent civil resistance include getting government officials and citizens to understand that an armed approach may not be effective, communicating the plan prior to hostilities and then executing it without clear channels of communication, and, finally, convincing the population that non-violence is not a sign of weakness, but, a more effective way of reasserting unity and opposition to the aggressor state.<sup>64</sup>

Special forces Operational Detachment-Alpha's (ODAs) and civil affairs teams are in a unique position to help build capacity for non-violent civil resistance, as one of their core missions is unconventional warfare. The main goal of unconventional warfare is to enable a resistance movement to disrupt a government or occupying power. As such, special forces ODAs are uniquely equipped and trained to facilitate non-violent civil resistance. In order to

build capacity within host countries, special forces ODAs and civil affairs teams should work with host nations to develop plans for non-violent civil resistance, identify and build relationships with community leaders and organizations that could be mobilized to implement a non-violent civil resistance plan, and train host-nation military forces in conducting unconventional warfare. This can be done either overtly or covertly depending on the specific country situation and political landscape.

On a positive note, steps have been made to implement non-violent civil resistance techniques in some NATO countries in Eastern Europe. In particular, Latvia introduced a manual in 2015 that highlights what institutions can do and what actions civilians can take to non-violently challenge an aggressor who occupies their territory.<sup>65</sup> The US Army should build on this manual and help distribute it or recreate it in states at risk of being occupied by an aggressor. This will help build the capacity within those countries to disrupt aggressors and buy the United States time to come to a diplomatic solution or deploy forces to oust the aggressor.

---

<sup>63</sup> Ibid.

<sup>64</sup> Maciej Bartkowski, January 8, 2016.

---

<sup>65</sup> Maciej Bartkowski, "Nonviolent Civilian Defense to Counter Russian Hybrid Warfare" (The Johns Hopkins University Center for Advanced Governmental Studies, March 2015).

In addition to enabling countries to help resist an aggressor should it take action and try to occupy territory, building networks capable of non-violent civil resistance bears other fruit. First, building relationships between the host nation and the network decreases the likelihood that an aggressor can subvert these segments of the population. This inherently decreases the capacity for a gray-zone aggressor to use cultural norms and laws as a weapons system. For example, if an aggressor tries to use unarmed civilians to protect its gains, those civilians are less likely to participate if they are part of a non-violent civil resistance network. Furthermore, networks developed ahead of hostilities for non-violent civil resistance could be used for unconventional warfare against an aggressor if an objective cannot be achieved through non-violent means. For example, if time is of the essence, special operations forces could tap in to the non-violent civil resistance network to organize action against an aggressor or facilitate infiltration of friendly forces into enemy territory.

Building capacity for non-violent civil resistance may not be as sexy as other responses to hybrid threats in the gray zone. However, it is a relatively low-cost initiative that can be achieved with minimal troop commitment and has the potential to be more successful than armed conflict. Furthermore, it

is a strategy that buys the United States and international institutions time to formulate a response and/or build the political will before undertaking operations to counter an aggressor who has taken actions that are incongruent with international norms and laws.

### V: Summary: The Future of Hybrid Threats

Hybrid threats will continue to dominate future conflict. States and non-state actors have seen the success of hybrid threats in places such as Ukraine, Lebanon, and the South China Sea. Because of this success, aggressors will continue to pursue these tactics to achieve their strategic objectives.

In the gray zone, hybrid tactics have been and will continue to be the tactic of choice moving forward. Since 1918, less than 20 percent of all conflicts have been state-on-state conventional conflicts and there is nothing hinting that this will change in the future.<sup>66</sup> Consequently, the US Army must take action to counter hybrid threats by working with at-risk states to integrate vulnerable ethnic minorities, building the capacity to execute non-violent civil resistance, improving unconventional warfare

---

<sup>66</sup> David Maxwell, "Congress Has Embraced Unconventional Warfare: Will the US Military and The Rest of the US Government?," *Small Wars Journal*, December 29, 2015.

## Countering Gray-Zone Hybrid Threats

capabilities, expanding educational opportunities for officers and non-commissioned officers, positioning US forces in at-risk countries to act as a deterrent to hybrid actions in the gray zone, and developing unconventional warfare plans.

In order to be effective in countering hybrid threats in the gray zone, the Army must do three things: (1) adequately define hybrid threats and the gray zone; (2) identify and adapt to challenges posed by gray-zone hybrid threats due to laws, norms, and processes; and (3) improve capacity to counter gray-zone hybrid threats. These three lines of effort will effectively posture the US Army to counter gray-zone hybrid threats and achieve its strategic objectives as outlined by US defense policymakers.

The Army must adequately define hybrid threats and the gray zone in order to achieve shared understanding amongst strategists, leaders, and policymakers. When doing this, the Army should consider that the gray zone is the space between peace and war. Furthermore, the gray zone is not a specific type of conflict, but an operational environment in which the United States and aggressor states operate. The Army must recognize that there is a distinct difference between hybrid threats in the gray zone and open-warfare hybrid threats.

The characteristic of ambiguity causes this dichotomy. In the gray zone, aggressor states strive to remain ambiguous and achieve their strategic objectives without adversaries or international institutions being able to attribute their actions to the aggressor. Finally, in defining gray-zone hybrid threats, the Army should study the following characteristics: ambiguity, exploitation of adversary weaknesses through DIME, attacks in five domains, use of criminal organizations and networks, and using laws and cultural norms as a weapons system.

Gray-zone hybrid threats take advantage of the US government's bureaucracy and the fact that multiple agencies have a say in how operations are conducted in the gray zone. Specifically, "New Generation Warfare," conducted by Russia, focuses on taking action and achieving strategic objectives within Phase 0 of US military operations. To counter this, the US Army must align its doctrine to combat gray-zone hybrid threats. This entails conducting an analysis of gray-zone doctrine from the most likely gray-zone adversaries (Russia, China, and Iran) and then looking at the US phasing construct and options for action within Phase 0 to decide if they are appropriate to counter gray-zone hybrid threats. Secondly, the US Army needs to look at systems and processes used to fuse intelligence and create shared

## Countering Gray-Zone Hybrid Threats

understanding across multiple agencies. If the systems and processes are inadequate to quickly and efficiently share information, then these issues need to be addressed.

Finally, the US Army must improve its capacity to counter gray-zone hybrid threats. It can do this by focusing on identifying and understanding the threat through the rebuilding of unconventional warfare capacity within the special operations forces and increasing broadening opportunities for education among special operations junior officers and non-commissioned officers. Secondly, the Army can reduce risk by pre-positioning US forces in at-risk countries, working with the Department of

State and host nations to integrate at-risk ethnic populations, and working with the Department of State and host nations to introduce and expand non-violent civil resistance capabilities in at-risk countries.

Hybrid threats and the gray zone are issues that have existed in warfare for centuries. However, their recent emergence in the discussion of conflict amongst strategists, scholars, and policymakers highlights their renewed importance. Consequently, it is important that the US Army accurately describes these concepts, aligns doctrine against them, and ensures it is properly postured to counter the threats they pose.

## Appendix A: Select Definitions

Combined Arms Maneuver: The application of the elements of combat power in unified action to defeat enemy ground forces; to seize, occupy, and defend land areas; and to achieve physical, temporal, and psychological advantages over the enemy to seize and exploit the initiative (ADP 3-0, Unified Land Operations).

Decisive Action: Actions conducted through the simultaneous combination of offensive, defensive, and stability operations (or defense support of civil authorities) appropriate to the mission and the environment (ADP 3-0, Unified Land Operations).

Irregular Warfare: A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s) (JP 1, Doctrine for the Armed Forces of the United States).

Operational Environment: A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Also called OE. (JP 1-02, Department of Defense Dictionary of Military and Associated Terms)

Special Warfare: The execution of activities that involve a combination of lethal and nonlethal actions taken by a specially trained and educated force that has a deep understanding of cultures and foreign language, proficiency in small-unit tactics, and the ability to build and fight alongside indigenous combat formations in permissive, uncertain, or hostile environment (ADRP 1-02: Terms and Military Symbols)

Traditional Warfare: a violent struggle for domination between nation-states or coalitions and alliances of nation-states typically involving force-on-force military operations in which adversaries employ a variety of conventional forces and special operations forces against each other in all physical domains as well as the information environment. (JP 1, Doctrine for the Armed Forces of the United States)

## Countering Gray-Zone Hybrid Threats

Unconventional Warfare: Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerilla force in a denied area. (JP 1-02, Department of Defense Dictionary of Military and Associated Terms)

Unified Land Operations: How the US Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution (ADP 3-0, Unified Land Operations).

Wide Area Security: The application of the elements of combat power in unified action to protect populations, forces, infrastructure, and activities; to deny the enemy positions of advantage; and to consolidate gains in order to retain the initiative (ADP 3-0, Unified Land Operations).

**Appendix B: US Operational Phases from Joint Publication 5-0, Operational Art and Design**

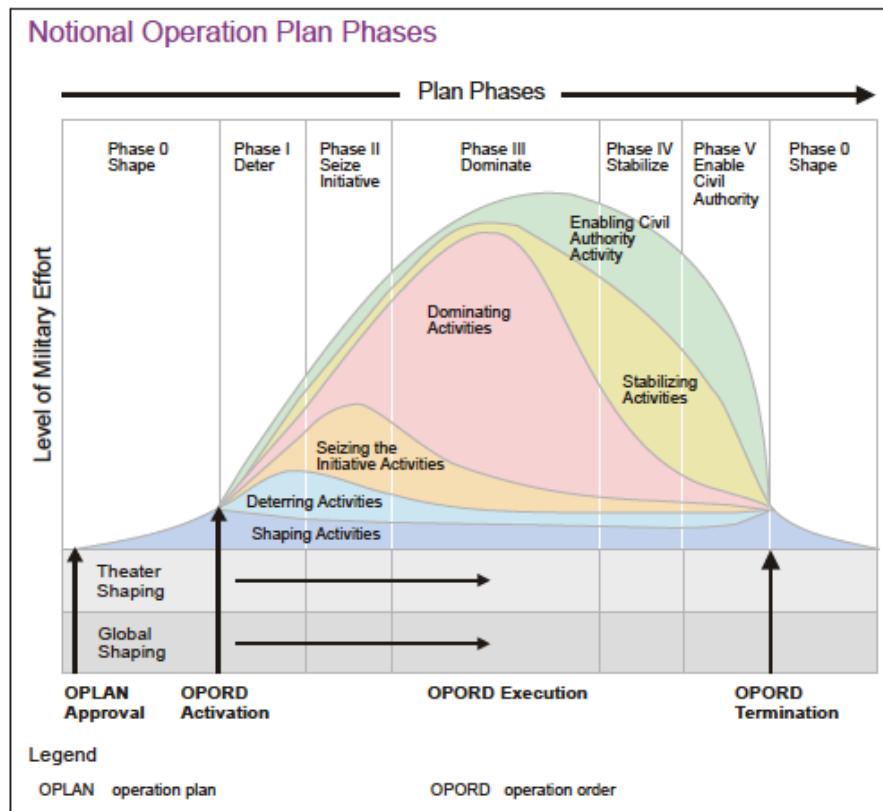
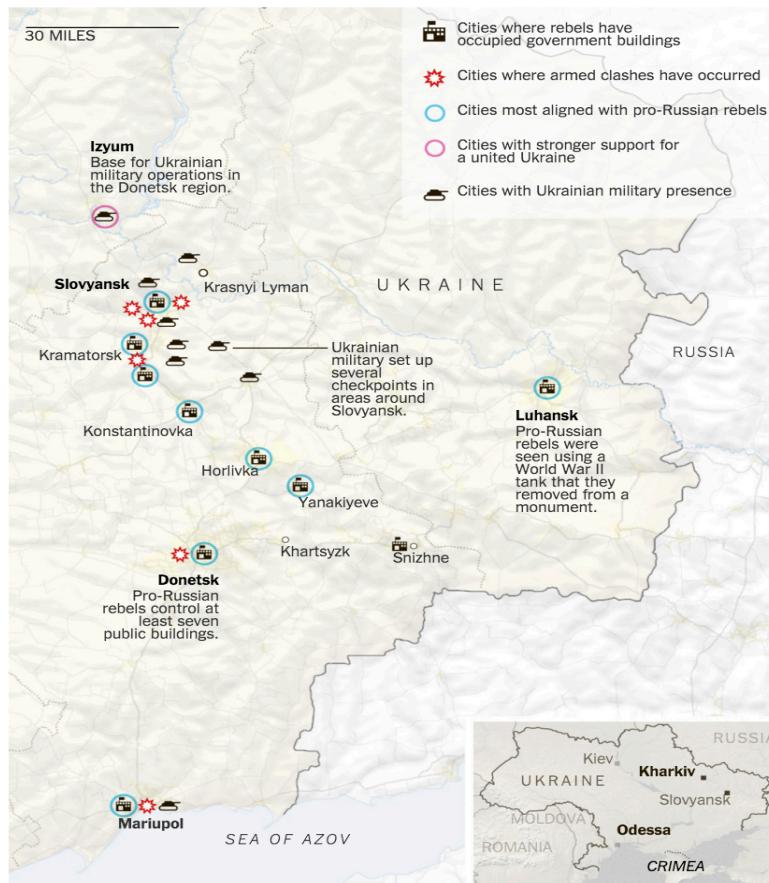


Figure III-16. Notional Operation Plan Phases

## Appendix C: Ukraine Crisis Maps



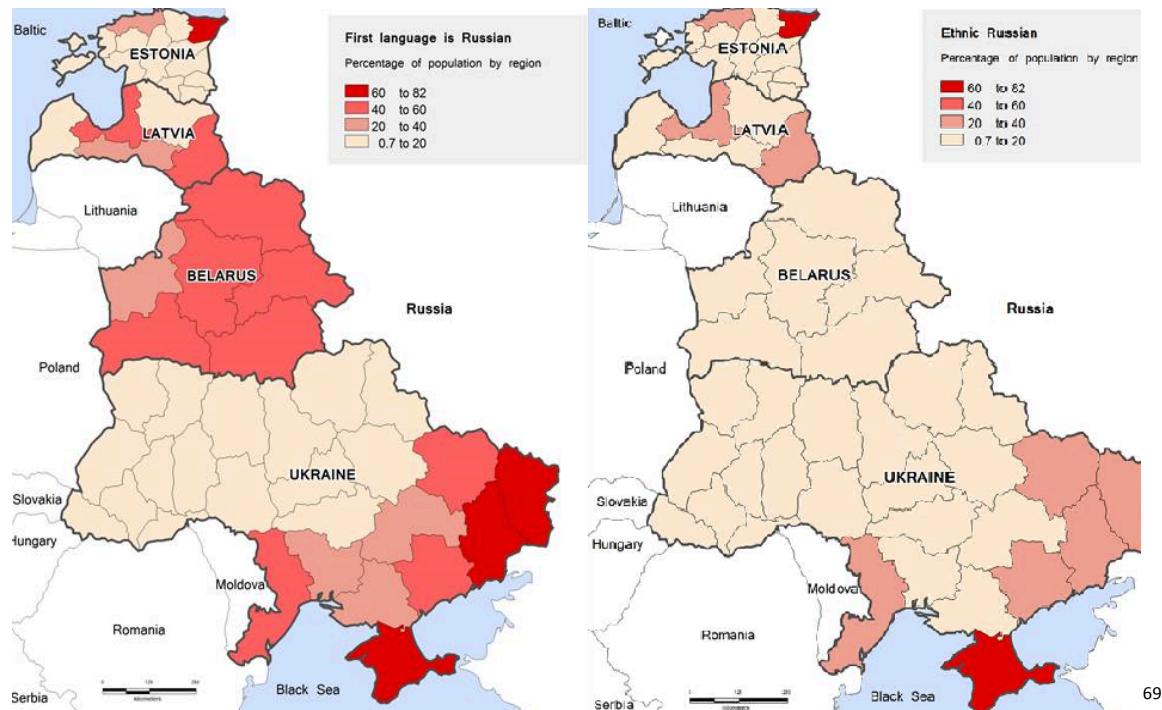
67



68

<sup>67</sup> “Ukraine Crisis in Maps,” *The New York Times*, February 27, 2014.

**Appendix D: Ethnic Russian Populations in Eastern Europe**



69

<sup>68</sup> Ibid.

<sup>69</sup> “Ethnic Russian Population in Eastern Europe,” *OneEurope*, accessed February 7, 2016.

### **Appendix E: Methodology & Acknowledgements**

This analysis uses a mix of research, interviews, and working group participation. The research consisted mainly of reading and analyzing scholarly journal and newspaper articles written by members of academia, think tanks, and military strategists. Additionally, the analysis uses extensive research on the Russian military's use of hybrid tactics in eastern Ukraine and the implementation of the Gerasimov Doctrine also known as "New Generation Warfare." Interviews for the project focused on experts in unconventional warfare, hybrid warfare, military strategy, non-violent civil resistance, and Russian affairs. Finally, participation in two working groups at the US Army War College played a large role in thinking about the problem and developing concepts and findings of the report. Participants in the working groups consisted of Army War College students, academics, and military strategists. When evaluating possible solutions for the US Army to counter gray-zone hybrid threats, the analysis only looked at options that the chief of staff of the Army could reasonably implement. For example, his ability to influence and change federal law or command relationships between the Department of Defense and the Department of State is relatively limited. However, his ability to improve the capabilities of the Army to conduct unconventional warfare is significant. Consequently, the solution set was narrowed by these constraints.

The author would like to thank everyone who helped contribute to this project and without whom it would not have been possible. There are countless people who provided interviews, reviewed drafts, and/or shared discussions about Hybrid Warfare and the Gray Zone throughout the length of this project. Specifically, he would like to thank his Policy Analysis Exercise advisors at the Harvard Kennedy School, Mr. William Tobey, Dr. Robert Piccard, and Dr. Thomas Patterson, and Mr. Nathan Freier of the Strategic Studies Institute at the Army War College. Additionally, he would like to thank the staff of the United States Military Academy's Modern War Institute, particularly Dr. Lionel Beehner and John Amble, for their support in bringing this project to fruition. Finally, he would like to thank his wife, Stacie, for putting up with all the long hours needed to finish this project.

## Bibliography

"2015-16 In-State Tuition and Fees at Public Four-Year Institutions by State and Five-Year Percentage Change - Trends in Higher Education - The College Board." Accessed March 18, 2016.

<http://trends.collegeboard.org/college-pricing/figures-tables/2015-16-state-tuition-and-fees-public-four-year-institutions-state-and-five-year-percentage>.

Allison, Graham, and Dimitri Simes. "Russia and America: Stumbling to War." Text. The National Interest. Accessed November 22, 2015. <http://nationalinterest.org/feature/russia-america-stumbling-war-12662>.

Altman, Howard. "'Gray zone' Conflicts Far More Complex to Combat, Says SOCOM Chief Votel." Tampa Tribune, November 28, 2015. <http://www.tbo.com/list/military-news/gray-zone-conflicts-far-more-complex-to-combat-says-socom-chief-votel-20151128/>.

Arbatov, Alexei G. "The Transformation of Russian Military Doctrine: Lessons Learned from Kosovo and Chechnya." George C. Marshall European Center for Security Studies, July 2000. <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA478927>.

Bartkowski, Maciej. "Nonviolent Civilian Defense to Counter Russian Hybrid Warfare." The Johns Hopkins University Center for Advanced Governmental Studies, March 2015.

Bartkowski, Maciej, Interview, January 8, 2016.

Bartles, Charles. "Getting Gerasimov Right." Military Review 96, no. 1 (January 2016): 30–38.

Bendavid, Naftali. "Images Appear to Show Russian Artillery Targeting Ukrainian Town." Wall Street Journal, February 14, 2015, sec. World. <http://www.wsj.com/articles/images-appear-to-show-russian-artillery-targeting-ukrainian-town-1423930491>.

Bershidsky, Leonid. "Moscow Strategists View World as War Theater." BloombergView, August 29, 2014. <http://www.bloombergview.com/articles/2014-08-29/moscow-strategists-view-world-as-war-theater>.

Berzins, Janis. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy." National Defence Academy of Latvia Center for Security and Strategic Research, April 2014.

Birnbaum, Michael. "In Kazakhstan, Fears of Becoming the next Ukraine." The Washington Post, May 1, 2015. [https://www.washingtonpost.com/world/europe/in-kazakhstan-fears-of-becoming-the-next-ukraine/2015/05/01/10f7e73c-e878-11e4-8581-633c536add4b\\_story.html](https://www.washingtonpost.com/world/europe/in-kazakhstan-fears-of-becoming-the-next-ukraine/2015/05/01/10f7e73c-e878-11e4-8581-633c536add4b_story.html).

Bomba, Tyrone. "Abandon All Hope, Ye Who Enter Here: You Cannot Save the Gray Zone Concept." War on the Rocks. Accessed January 12, 2016. <http://warontherocks.com/2015/12/abandon-all-hope-ye-who-enter-here-you-cannot-save-the-gray-zone-concept/>.

Borger, Julian, and Luke Harding. "Baltic States Wary as Russia Takes More Strident Tone with Neighbours." The Guardian, September 18, 2014, sec. World news.

## Countering Gray-Zone Hybrid Threats

<http://www.theguardian.com/world/2014/sep/18/baltic-states-wary-russia-strident-estonia-latvia-lithuania-nato>.

Center for Strategic and International Studies. “The Ukraine Crisis Timeline,” n.d. <http://ukraine.csis.org>.

Central Intelligence Agency. “CIA World Fact Book,” February 5, 2016. <https://www.cia.gov/library/publications/the-world-factbook/>.

Chenoweth, Erica, and Maria Stephan. “Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict.” *International Security* 33, no. 1 (2008): 7–44.

“China Explains Why It’s Building Islands in the South China Sea.” Accessed January 22, 2016. <http://www.businessinsider.com/china-explains-why-its-building-islands-in-the-south-china-sea-2015-4>.

Coalson, Robert. “Top Russian General Lays Bare Putin’s Plan for Ukraine.” *The Huffington Post*, September 2, 2014. [http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine\\_b\\_5748480.html](http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html).

Dubik, LTG(R) James. “Winning the War We’ve Got, Not the One We Want.” *ARMY Magazine*, January 12, 2016. <http://www.armymagazine.org/2016/01/12/winning-the-war-weve-got-not-the-one-we-want/>.

Elkus, Adam. “50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense.” *War on the Rocks*. Accessed December 16, 2015. <http://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/>.

Erickson, Andrew S., and Conor M. Kennedy. “Beware of China’s ‘Little Blue Men’ in the South China Sea.” *Text*. *The National Interest*. Accessed January 22, 2016. <http://nationalinterest.org/blog/the-buzz/beware-chinas-little-blue-men-the-south-china-sea-13846>.

“Ethnic Russian Population in Eastern Europe.” *OneEurope*. Accessed February 7, 2016. <http://one-europe.info/eurographics/ethnic-russian-population-in-eastern-europe>.

Evans, Ryan. The State of Russian Strategy: Ukraine, Syria, and Beyond. *War on the Rocks*. Accessed January 7, 2016. <http://warontherocks.com/2015/09/the-state-of-russian-strategy-ukraine-syria-and-beyond/>.

Faith, Scott. “GEN McChrystal On ISIS: Four Tips From Someone Who Actually Knows How To Fight Terrorists.” *The Havok Journal*. Accessed November 22, 2015. <http://www.havokjournal.com/national-security/gen-mcchrystal-on-isis-four-tips-from-someone-who-actually-knows-how-to-fight-terrorists/>.

Ferris-Rotman, Amie. “How to Disappear a Country.” *The Atlantic*, 07/21/20105. <http://www.theatlantic.com/international/archive/2015/07/russia-ukraine->

[donetsk/398942/?utm\\_source=Sailthru&utm\\_medium=email&utm\\_term=%2ASituation%20Report&utm\\_campaign=SitRep0722](http://donetsk/398942/?utm_source=Sailthru&utm_medium=email&utm_term=%2ASituation%20Report&utm_campaign=SitRep0722).

Freier, Nathan. "The Defense Identity Crisis: It's a Hybrid World." *Parameters*, no. Autumn 2009 (2009): 81–94.

Gady, Franz-Stefan. "'Little Blue Men' Doing China's Dirty Work in the South China Sea." *The Diplomat*. Accessed January 22, 2016. <http://thediplomat.com/2015/11/little-blue-men-doing-chinas-dirty-work-in-the-south-china-sea/>.

Galeotti, Mark. "Russia's New National Security Strategy: Familiar Themes, Gaudy Rhetoric." *War on the Rocks*. Accessed January 8, 2016. <http://warontherocks.com/2016/01/russias-new-national-security-strategy-familiar-themes-gaudy-rhetoric/>.

Galeotti, Mark. "'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't." *E-International Relations*, ARP 2015. <http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/>.

Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War." In *Moscow's Shadows*. Accessed December 2, 2015. <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>.

Galeotti, Mark. "Time to Think About 'Hybrid Defense.'" *War on the Rocks*, July 2015. <http://warontherocks.com/2015/07/time-to-think-about-hybrid-defense/>.

Gertz, Bill. "Russian Troop Movements Near Eastern Ukraine Trigger Fears of Imminent Invasion." *The Washington Free Beacon*. Accessed September 11, 2016, <http://freebeacon.com/national-security/russian-troop-movements-near-eastern-ukraine-trigger-fears-of-imminent-invasion/>.

Gibbons-Neff, Thomas. "The 'new' Type of War That Finally Has the Pentagon's Attention." *The Washington Post*, July 3, 2015. [https://www.washingtonpost.com/world/national-security/the-new-type-of-war-that-finally-has-the-pentagons-attention/2015/07/03/b5e3fcda-20be-11e5-84d5-eb37ee8eaa61\\_story.html?tid=themost\\_item\\_5](https://www.washingtonpost.com/world/national-security/the-new-type-of-war-that-finally-has-the-pentagons-attention/2015/07/03/b5e3fcda-20be-11e5-84d5-eb37ee8eaa61_story.html?tid=themost_item_5).

Goble, Paul. "Stalin Invented Hybrid War, Not Vladimir Putin, Archival Record Shows." *The Interpreter*. Accessed July 6, 2015. <http://www.interpretermag.com/stalin-invented-hybrid-war-not-vladimir-putin-archival-record-shows/>.

Gorenberg, Dmitry. "Valery Gerasimov | Russian Military Reform." Accessed October 22, 2015. <https://russiamil.wordpress.com/tag/valery-gerasimov/>.

Gorenberg, Dmitry, Interview, 15 JAN 16.

Griswold, Eliza. "Can General Linder's Special Operations Forces Stop the Next Terrorist Threat?" *The New York Times*, June 13, 2014. <http://www.nytimes.com/2014/06/15/magazine/can-general-linders-special-operations-forces-stop-the-next-terrorist-threat.html>.

## Countering Gray-Zone Hybrid Threats

Headquarters, Department of the Army. "ADP 3-0: Unified Land Operations." HQDA, October 2011. [http://armypubs.army.mil/doctrine/DR\\_pubs/dr\\_a/pdf/adp3\\_0.pdf](http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp3_0.pdf).

Headquarters, Department of the Army. "ADP 3-05: Special Operations." HQDA, August 2012. [http://armypubs.army.mil/doctrine/DR\\_pubs/dr\\_a/pdf/adp3\\_05.pdf](http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp3_05.pdf).

Headquarters, Department of the Army. "ADRP 1-02: Terms and Military Symbols." HQDA, December 2015.

[http://armypubs.army.mil/doctrine/DR\\_pubs/dr\\_a/pdf/adrp1\\_02.pdf](http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adrp1_02.pdf).

Hoffman, Frank. "Conflict In The 21st Century: The Rise of Hybrid Wars." Arlington, VA: Potomac Institute for Policy Studies, December 2007.

[http://www.potomacinstitute.org/images/stories/publications/potomac\\_hybridwar\\_0108.pdf](http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf).

Hoffman, Frank. "Countering Full Spectrum Conflict in the 21st Century." November 17, 2015.

Hoffman, Frank. "Hybrid vs. Compound War." Armed Forces Journal, October 1, 2009.

<http://www.armedforcesjournal.com/hybrid-vs-compound-war/>.

Hoffman, Frank . "The Contemporary Spectrum of Conflict: Protracted, Gray zone, Ambiguous, and Hybrid Modes of War." 2016 Index of US Military Strength. The Heritage Foundation, October 2015. <http://index.heritage.org/military/2016/essays/contemporary-spectrum-of-conflict/>.

Hoffman, Frank, Interview, January 12, 2016.

"How Marines Are Preparing for Hybrid Wars," March 1, 2006.

<http://www.armedforcesjournal.com/how-marines-are-preparing-for-hybrid-wars/>.

"How Much Does a Master's in International Relations Cost? - CostHelper.com." CostHelper. Accessed March 18, 2016. <http://education.costhelper.com/ma-international-relations.html>.

Hunter, Eve, and Piret Pernik. "The Challenges of Hybrid Warfare." International Centre for Defence and Security, April 2015.

"'Hybrid Warfare' Tests Pentagon." Stars and Stripes. Accessed July 6, 2015.

<http://www.stripes.com/news/US/hybrid-warfare-tests-pentagon-1.356378>.

Hybrid War - Hybrid Response? NATO Review Magazine, 2014.

<http://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/EN/index.htm>.

"Instructing Ukrainian Troops a Wake-up Call for Canadian Soldiers." The Globe and Mail. Accessed January 11, 2016. <http://www.theglobeandmail.com/news/national/instructing-ukrainian-troops-a-wake-up-call-for-canadian-trainers/article28048695/>.

## Countering Gray-Zone Hybrid Threats

Kazianis, Harry J. "China's 50,000 Secret Weapons in the South China Sea." Text. The National Interest. Accessed February 7, 2016. <http://nationalinterest.org/feature/china%20%99s-50000-secret-weapons-the-south-china-sea-10973>.

Killebrew, Robert. "A New Kind of Warfare." Armed Forces Journal, March 1, 2012. <http://www.armedforcesjournal.com/a-new-kind-of-warfare/>.

Killebrew, Robert. "Hybrid Warfare Demands an Indirect Approach," June 1, 2008. <http://www.armedforcesjournal.com/good-advice/>.

Killebrew, Robert. Statement Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities on Understanding Future Irregular Warfare Challenges, n.d. [http://armedservices.house.gov/index.cfm/files/serve?File\\_id=6a00f38f-6902-4379-b788-76004dc6e64](http://armedservices.house.gov/index.cfm/files/serve?File_id=6a00f38f-6902-4379-b788-76004dc6e64).

Kim, Lucian. "The Battle of Ilovaisk: Details of a Massacre Inside Rebel-Held Eastern Ukraine." Newsweek, November 4, 2014. <http://www.newsweek.com/2014/11/14/battle-ilovaisk-details-massacre-inside-rebel-held-eastern-ukraine-282003.html>.

Kofman, Michael, and Matthew Rojansky. "A Closer Look at Russia's 'Hybrid War.'" Kennan Cable. Kennan Institute at the Woodrow Wilson Center, April 2015. <https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf>.

Kokoshin, Andrey Afanasyevich. We will Think About The Future. Interview by Viktor Litoykin. Independent Military Review Online, May 20, 2011.

Lewis, James. "The Role of Offensive Cyber Operations Weapons in NATO' Collective Defense." NATO Cooperative Cyber Defence Centre of Excellence, 2015. [https://ccdoe.org/sites/default/files/multimedia/pdf/TP\\_08\\_2015\\_0.pdf](https://ccdoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf).

Lindberg, Tod. "The Answer to 'Hybrid Warfare,'" May 18, 2015. [http://www.weeklystandard.com/articles/answer-hybrid-warfare\\_941115.html](http://www.weeklystandard.com/articles/answer-hybrid-warfare_941115.html).

Mattis, James N., and Frank Hoffman. "Future Warfare: The Rise of Hybrid Wars." Proceedings Magazine. Accessed July 6, 2015. <http://milnewstbay.pbworks.com/f/MattisFourBlockWarusNINov2005.pdf>.

Maxwell, David. "Unconventional Warfare Does Not Belong to Special Forces." War on the Rocks, August 12, 2013. <http://warontherocks.com/2013/08/unconventional-warfare-does-not-belong-to-special-forces/>.

Maxwell, David. "Congress Has Embraced Unconventional Warfare: Will the US Military and The Rest of the US Government?" Small Wars Journal, December 29, 2015.

Maxwell, David, Interview, January 8, 2016.

## Countering Gray-Zone Hybrid Threats

Maxwell, Rahsaan. *Ethnic Minority Migrants in Britain and France: Integration Trade Offs*. Cambridge University Press, 2012.

Mazarr, Michael. "Struggle in the Gray Zone and World Order." *War on the Rocks*. Accessed January 12, 2016. <http://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/>.

Montalbano, Elizabeth. "Auditors Find DoD Hasn't Defined Cyber Warfare." *Dark Reading*, September 14, 2010. <http://www.informationweek.com/government/security/auditors-find-dod-hasnt-defined-cyber-wa/227400359>.

Office of the Assistant Secretary of Defense for Readiness & Force Management. "Defense Manpower Requirements Report." US Department of Defense, June 2014.  
<http://prhome.defense.gov/Portals/52/Documents/RFM/TFPRQ/docs/F15%20DMRR.pdf>.

Office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer. "European Reassurance Initiative." Department of Defense Budget FY 2016. US Department of Defense, n.d.  
[http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2016/FY2016\\_ERI\\_J-Book.pdf](http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2016/FY2016_ERI_J-Book.pdf).

Office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer. "Program Acquisition Cost By Weapon System." US Department of Defense, March 2014.  
[http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/fy2015\\_Weapons.pdf](http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/fy2015_Weapons.pdf).

Oliker, Olga. "Unpacking Russia's New National Security Strategy." Center for Strategic and International Studies, January 7, 2016. <https://csis.org/publication/unpacking-russias-new-national-security-strategy>.

Parameswaran, Prashanth. "Are We Prepared for 'Hybrid Warfare'?" *The Diplomat*, February 13, 2015. <http://thediplomat.com/2015/02/are-we-prepared-for-hybrid-warfare/>.

Pindjak, Peter. "Deterring Hybrid Warfare: A Chance for NATO and the EU to Work Together?" *NATO Review*. Accessed July 6, 2015. <http://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm>.

Robinson, Linda. "The Future of US Special Operations Forces." Council Special Report. Council on Foreign Relations, April 2013. <http://www.cfr.org/special-operations/future-US-special-operations-forces/p30323>.

"Russians in the Baltics: Forever Foreigners." Accessed February 5, 2016.  
[http://in.rbth.com/world/2013/04/02/russians\\_in\\_the\\_baltics\\_forever\\_foreigners\\_23433](http://in.rbth.com/world/2013/04/02/russians_in_the_baltics_forever_foreigners_23433).

Schadlow, Nadia. "Peace and War: The Space Between," August 18, 2014.  
<http://warontherocks.com/2014/08/peace-and-war-the-space-between/>.

Shuster, Simon. "Putin's Man in Crimea Is Ukraine's Worst Nightmare." *Time*, March 10, 2014.  
<http://time.com/19097/putin-crimea-russia-ukraine-aksyonov/>.

Special Forces Officer A, Interview, January 10, 2016.

Special Forces Officer B, Interview, February 6, 2016.

Strategic Studies Institute. "Hybrid Warfare / Grey Zone Threats I." US Army War College, November 4, 2015.

Strategic Studies Institute. "Hybrid Warfare / Grey Zone Threats II." US Army War College, January 27, 2016.

The Joint Staff. "Joint Publication 1, Doctrine for the Armed Forces of the United States," March 25, 2013. [http://www.dtic.mil/doctrine/new\\_pubs/jp1.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1.pdf).

The Joint Staff. "Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms," November 15, 2015. [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf).

The Joint Staff. "Joint Publication 3-0, Joint Operations," August 2011.  
[http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf).

The Joint Staff. "Joint Publication 5-0, Joint Operational Planning," August 2011.  
[https://fas.org/irp/doddir/dod/jp5\\_0.pdf](https://fas.org/irp/doddir/dod/jp5_0.pdf).

Thomas, Timothy. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" Journal of Slavic Military Studies 27, no. 1 (March 10, 2014): 101–30.

TRADOC G-2 Intelligence Support Activity – Complex Operational Environment and Threat Integration Directorate. "Threat Tactics Report: Islamic State of Iraq and the Levant." November 2014.

Trevithick, Joseph. "The US Army Has Quietly Created a New Commando Division." Medium, November 26, 2014. <https://medium.com/war-is-boring/the-u-s-army-has-quietly-created-a-new-commando-division-2b90961b4821>.

"Ukraine Crisis in Maps." The New York Times, February 27, 2014.  
<http://www.nytimes.com/interactive/2014/02/27/world/europe/ukraine-divisions-crimea.html>.

"Ukraine Crisis in Maps." BBC News. Accessed February 7, 2016. <http://www.bbc.com/news/world-europe-27308526>.

Understanding Future Irregular Warfare Challenges - Mar 27th, 2012. Washington, DC, 2012.  
[http://armedservices.granicus.com/MediaPlayer.php?view\\_id=2&clip\\_id=63](http://armedservices.granicus.com/MediaPlayer.php?view_id=2&clip_id=63).

United States Army. "My Army Benefits: Advanced Civil Schooling," n.d.  
[http://myarmybenefits.US.army.mil/Home/Benefit\\_Library/Federal\\_Benefits\\_Page/Advanced\\_Civil\\_Schooling\\_\(ACS\).html?serv=147](http://myarmybenefits.US.army.mil/Home/Benefit_Library/Federal_Benefits_Page/Advanced_Civil_Schooling_(ACS).html?serv=147).

US Army Europe. "Operation Atlantic Resolve," n.d. <http://www.eur.army.mil/atlanticresolve/>.

## Countering Gray-Zone Hybrid Threats

United States Army Special Operations Command. “ARSOF Operating Concept 2022.” September 2014. [http://www.soc.mil/Assorted%20Pages/ARSOF2022\\_vFINAL.pdf](http://www.soc.mil/Assorted%20Pages/ARSOF2022_vFINAL.pdf).

United States Army Special Operations Command. “Unconventional Warfare Pocket Guide.” April 2016.

[http://www.soc.mil/ARIS/Unconventional%20Warfare%20Pocket%20Guide\\_v1%200\\_Final\\_6%20April%202016.pdf](http://www.soc.mil/ARIS/Unconventional%20Warfare%20Pocket%20Guide_v1%200_Final_6%20April%202016.pdf).

US Department of Defense. “2014 Demographics: Profile of the Military Community,” n.d. <http://download.militaryonesource.mil/12038/MOS/Reports/2014-Demographics-Report.pdf>.

Victor, Robert Lee. “South China Sea: Satellite Images Show Pace of China’s Subi Reef Reclamation.” The Diplomat. Accessed January 22, 2016. <http://thediplomat.com/2015/06/south-china-sea-satellite-images-show-pace-of-chinas-subi-reef-reclamation/>.

Votel, GEN Joe, LTG(R) Charles Cleveland, COL Charles Connett, and LTC(R) Will Irwin. “Unconventional Warfare in the Gray zone.” Joint Forces Quarterly 80, no. 1st Quarter (January 17, 2016): 101–9.

Wall, Andru. “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, and Covert Action.” Harvard National Security Journal, Vol 3 (2011): 86-142.

Walker, Shaun. “Riga Mayor: ‘I’m a Russian-Speaking Latvian and Patriot of My Country.’” The Guardian, June 15, 2015, sec. World news. <http://www.theguardian.com/world/2015/jun/15/riga-mayor-im-a-russian-speaking-latvian-patriot-nils-usakovs>.

Weselowsky, Tony, and Mark Krutov. “Activist Says Russia using ‘Hybrid Warfare’ In Syria.” RadioFreeEurope/RadioLiberty, November 11, 2015. <http://www.rferl.org/content/russia-syria-cybersleuth-hybrid-warfare/27358490.html>.

Zakem, Vera, Paul J. Saunders, and Daniel Antoun. “Mobilizing Compatriots: Russia’s Strategy, Tactics, and Influence in the Former Soviet Union.” Center for Strategic Studies, November 2015.