Exploiting Vulnerabilities in the Russian Approach to Hybrid Warfare

by

Colonel Robert A. Culp II
United States Army

Under the Direction of:
Colonel Robert E. Hamilton

United States Army War College
Class of 2016

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.
Exploiting Vulnerabilities in the Russian Approach to Hybrid Warfare

This paper outlines the Kremlin's hybrid warfare strategy, operational design and associated tactics. Included are how Moscow integrates unconventional warfare, information operations and cyber operations along with diplomatic and economic coercion to achieve political and military objectives. Understanding the Kremlin's hybrid warfare strategy offers the United States and its allies opportunities for exploiting vulnerabilities embedded in the ways and means of Russian hybrid warfare. Recommended are actions, all of which fit into a Political Warfare strategic construct, to exploit vulnerabilities associated with Russian hybrid warfare. Implementing them aligns the ways and means necessary to successfully counter future Russian hybrid warfare and achieve our political objectives. Recommendations include changing personnel policies to better enable Strategic Landpower by making long-term investments in human capital to successfully engage in the human domain. Additional recommendations include organizational and policy changes to better organize the US Army, Cyber Command and our information operations enterprise across the Interagency to conduct Irregular Warfare and counter hybrid threats. Also recommended are changes to our intellectual culture and the professional military educational that underpins it.
Exploiting Vulnerabilities in the Russian Approach to Hybrid Warfare

(29,631 words)

Abstract

This paper outlines the Kremlin’s hybrid warfare strategy, operational design and associated tactics. Included are how Moscow integrates unconventional warfare, information operations and cyber operations along with diplomatic and economic coercion to achieve political and military objectives. Understanding the Kremlin’s hybrid warfare strategy offers the United States and its allies opportunities for exploiting vulnerabilities embedded in the ways and means of Russian hybrid warfare. Recommended are actions, all of which fit into a Political Warfare strategic construct, to exploit vulnerabilities associated with Russian hybrid warfare. Implementing them aligns the ways and means necessary to successfully counter future Russian hybrid warfare and achieve our political objectives. Recommendations include changing personnel policies to better enable Strategic Landpower by making long-term investments in human capital to successfully engage in the human domain. Additional recommendations include organizational and policy changes to better organize the US Army, Cyber Command and our information operations enterprise across the Interagency to conduct Irregular Warfare and counter hybrid threats. Also recommended are changes to our intellectual culture and the professional military educational that underpins it.
Exploiting Vulnerabilities in the Russian Approach to Hybrid Warfare

After the Vietnam War, we purged ourselves of everything that had to do with irregular warfare or insurgency, because it had to do with how we lost that war. In hindsight, that was a bad decision. … We have responsibility.

—General Jack Keene

In March 2014, Russian military and paramilitary forces successfully achieved strategic surprise when they swiftly annexed the internationally recognized Ukrainian territory of Crimea. This successful application of a hybrid warfare strategy was followed by the execution of a similar Russian hybrid operation in Eastern Ukraine; a former Soviet Union state that was on a path to North Atlantic Treaty Organization (NATO) membership. The world watched to see the reactions of the United States and NATO. When Moscow’s challenges went unanswered with anything other than harsh rhetoric and promises to implement economic sanctions serious questions arose regarding the strength of the NATO alliance. In particular, the resolve of the United States to support countries aspiring to membership in NATO, such as Georgia or Montenegro, or to support countries newly granted NATO membership, such as the Baltic States, was in doubt.

A strategic objective of Moscow is to weaken the NATO alliance by creating situations that cause NATO member countries to doubt the strength of the mutual defense guarantees in NATO’s Article 5. Putin sees this as a way to demonstrate Russia’s return to great power status. Failure to address this aggression may incentivize continued Russian coercion of countries, such as the Baltic States, on its periphery. If it becomes clear that the NATO allies will not live up to collective defense commitments in the face of Russian aggression then the viability of the NATO alliance may be questioned, leading to its fracture. Europe’s outlook as a united, nonviolent, and
economically thriving society stands on the collective security provided by NATO and the United States to respond to Russia’s belligerence.³

Russia’s increasingly coercive foreign policy and military adventurism in its near abroad has leaders across Western Europe worried that the post-World War II period of peace and prosperity is at risk. Russia’s hybrid warfare actions in the gray zone are a destabilizing influence because international institutions such as NATO, the European Union (EU), the Organization for Security and Co-operation in Europe (OSCE) and the United Nations (UN) have proven incapable of deterring Putin’s moves to secure territory. Worse, Russia’s successful use of a hybrid warfare strategy has called into question the resolve of the United States to stand by its obligations to its treaty allies. Future Russian hybrid warfare in countries aspiring to membership in NATO poses “an existential threat to the Alliance.”⁴

Russian President Putin and his strategic military leadership clearly recognize that the United States, European Union states and international organizations are governed by democratic processes that adhere to constitutional limits of power and the rule of law. Thus, they have very effectively crafted ‘hybrid warfare’ strategies that seek to operate in the ‘gray zone’ just below the threshold for the implementation of a United Nations Security Council Resolution or a NATO Article 5 declaration. While the use of hybrid techniques is not necessarily new, our vulnerability to them, as evidenced by the Russians’ actions in Crimea and Eastern Ukraine, is real and growing. Our traditional models and theories regarding warfare fail to adequately address confronting these hybrid strategies and our mechanisms for creating and implementing foreign policy and leveraging international organizations are not agile enough to sufficiently react when
faced with an adversary implementing a hybrid strategy in the gray zone. General Joseph Votel, while still commanding the US Special Operations Command, called our ability to address hybrid threats in the gray zone a “critical policy gap.” The stakes are high given the importance of our strategic partners and allies in NATO and the European Union. Our strategic approach to addressing our adversaries’ employment of a hybrid warfare strategy must adapt or we risk catastrophic failure.

In *Military Misfortunes: The Anatomy of Failure in War*, Eliot A. Cohen and John Gooch categorize military failure in three ways: 1) failure to learn, 2) a failure to anticipate, and 3) a failure to adapt. Cohen and Gooch contend that when two types of failure happen concurrently, an “aggregate” failure results. “Catastrophic” failure occurs when all three types of failure happen together. The lessons of how the Russians have successfully employed a hybrid warfare strategy over the past decade-plus are laid out before us to examine. We would be foolish to anticipate that the Russians will not hone their techniques and employ a similar strategic approach in the future. Taking this idea one step further, we would be incredibly foolhardy to assume that our other adversaries such as China, Iran, North Korea (et. al.) have failed to watch and learn from the Russians’ techniques and our inability to successfully deter aggression and deny them achieving their objectives. What if the Kremlin were to implement its hybrid warfare strategy in one of the ethnically Russian areas in one of the Baltic States? Have we learned the lessons of Moscow’s approach to hybrid war in Ukraine? Have we anticipated that Putin may conduct hybrid warfare somewhere in a NATO country in Russia’s near abroad? What are the vulnerabilities associated with the Kremlin’s approach to a hybrid warfare strategy that we can potentially exploit? Considering the
possible answers to these questions, what actions did we take to deter Russia or to deny the Kremlin from achieving its objectives? The stakes are high and failure is not an option. We must adapt our policies, strategic approach and the ways and means we are applying to successfully counter future hybrid threats or we risk the catastrophic failure of a fracturing NATO alliance. Studying the Russian approach to hybrid warfare offers us opportunities to avoid the *Military Misfortunes* articulated by Cohen and Gooch by learning from the past, anticipating our adversary’s next move and adapting our approach so that we are able to win at the strategic level and achieve our policy objectives.

Knowing how the Russians implement their hybrid warfare strategy in the 21st century reveals vulnerabilities associated with their strategy, their operational design and their associated tactics. Understanding this offers the United States and its allies opportunities for exploiting vulnerabilities embedded in the ways and means Russia chooses to implement its policy objectives. It is intended for this paper to outline the emerging Russian hybrid warfare strategy while highlighting the vulnerabilities associated with their approach. Sun Tzu stated in *The Art of War* “what is of supreme importance is to attack the enemy’s strategy.” 8 This is perhaps the most critical element of Sun Tzu’s theory of warfare. Failing to understand the enemy’s strategy and neglecting to select a strategy to counter the enemy’s strategic aims ensures that all further analysis regarding the ways and means employed to achieve political objectives will not be optimized to defeat the enemy. With this understanding, the paper recommends some specific actions, all of which fit into a Political Warfare strategic construct that the US and its allies should adopt.9 Implementing these
recommendations will align the ways and means necessary, thus enabling us to successfully counter future Russian use of a hybrid warfare strategy and achieve our political objectives.

What is ‘Hybrid Warfare’ and Where is the ‘Gray Zone’?

Hybrid Warfare

Much has been written about hybrid warfare. Many have sought to define what it is; or is not. Others have offered explanations of why hybrid warfare is a new form of conflict while still others have asserted that it has existed since the dawn of time. In Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present, esteemed military analysts Peter Mansoor and Williamson Murray opine that hybrid warfare is not some new type of threat, complete with fresh tactics and techniques, but has existed for “hundreds, if not thousands of years.” Indeed, the US military has been defining the various forms of warfare for decades and has variously labeled operations short of traditional, conventional force-on-force combat involving nation states and their armies as Military Operations Other Than War (MOOTW), non-linear war, and asymmetric war. There are probably other labels as well. The hybrid warfare term has existed in various military documents and texts for over a decade and, since 2006, has been used to describe how our adversaries are blending the use of various tactics in a variety of operational environments and domains.

Former Secretary of Defense Robert Gates and other top military scholars, such as Lieutenant General H. R. McMaster, have used the term hybrid warfare to define the complicated and changing nature of war. Former Chief of Staff of the US Army, General Ray Odierno, recently remarked that it was important for the Army to understand hybrid war because “…one of the most costly lessons [the Army] has learned over the last
decade: how to deal with the challenge of hybrid warfare. It will be increasingly common for the army to operate in environments with both regular military and irregular, paramilitary or civilian adversaries, with the potential for terrorism, criminality and other complications." Fortunately, the US Army doctrine offers us a working definition of hybrid threats that allows military units to focus their training efforts at countering the tactics that our adversaries employ as part of a hybrid warfare strategy.

US Army Training and Doctrine Command’s Training Circular 7-100, *Hybrid Threats*, defines hybrid threats as a “diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects.” It goes on to describe how hybrid threats “can combine state-based, conventional military forces—sophisticated weapons, command and control, and combined arms tactics—with attributes usually associated with insurgent and criminal organizations.” Adding to the complexity associated with this mix of forces and tactics is the fact that international law, military tradition, and customs regulate the use of state armies while irregular forces are ungoverned and free to operate without legal constraint on the use of violence or selection of targets. But beyond the tactical aspects of the legal application of force, there are critical legalistic and bureaucratic considerations that create a gray zone that makes it especially difficult at the operational and strategic levels to address our adversaries’ use of a hybrid warfare strategy.

**The Gray Zone**

In their *Joint Forces Quarterly* article “Unconventional Warfare in the Gray Zone” General Votel and Lieutenant General Cleveland explain that the gray zone is “a space in the peace-conflict continuum…where our current adversaries, [with] a finely tuned risk calculus, choose to engage us in an asymmetrical manner…without triggering a
North Atlantic Treaty Organization Article 5 response, a belligerent U.S. or allied response.\textsuperscript{13} Our adversaries have determined that our national-level decision making process is not agile and that our collective definitions of ‘an act of war’ provide them a seam of ambiguity where they can operate.

Professor Hal Brands, in his online article “Paradoxes of the Gray Zone” for \textit{Foreign Policy Research Institute}, stated that there are numerous contemporary examples of how our adversaries are operating the gray zone. These include China’s hybrid warfare strategy for increasing their influence and control over the South China Sea, Moscow’s use of proxy forces and militia in Crimea and Eastern Ukraine and Iranian use of proxy forces and a wide range of subversive activities throughout the Middle East to shift the balance of power in their favor. For Brands, “gray zone challenges…are ambiguous and usually incremental aggression. They represent that coercion that is, to varying degrees, disguised; they eat away at the status quo one nibble at a time.”\textsuperscript{14}

Dr. Mike Mazarr characterizes how our adversaries wage hybrid warfare in the gray zone as having a number of qualities. For him, it is the “[pursuit] of political objectives through cohesive, integrated campaigns…[employing] mostly nonmilitary or non-kinetic tools [while striving] to remain under key escalatory or red line thresholds to avoid outright, conventional conflict and, [moving] gradually toward its objectives rather than seeking conclusive results in a specific period of time.\textsuperscript{15}

Having discussed working definitions of hybrid warfare and the gray zone, along with some of the legal, bureaucratic and intellectual challenges associated with understanding the context in which our adversaries are choosing to operate, we must
examine a framework for considering a hybrid warfare strategy in the gray zone. This framework for understanding our adversaries’ efforts to employ a hybrid warfare strategy in the gray zone, combined with our definitions of what hybrid warfare is and where the gray zone exists, allows us to turn to an examination of how the Russians have employed various hybrid warfare strategies in the past decade-plus. This examination will lead us to identifying exploitable vulnerabilities associated with the Russian approach to hybrid warfare.

**Approaches to Hybrid Warfare in the Gray Zone**

**What Would Sun Tzu and Clausewitz Say?**

The classical military theorists Sun Tzu and Clausewitz offered us some critical insights into what the ingredients for a successful hybrid warfare strategy in the gray zone might look like. Our comparison of how both the Chinese and the Russians conduct hybrid warfare will begin with a review of the critical tenets of warfare espoused by Sun Tzu and Clausewitz.

Sun Tzu is noted for his advocacy for using the “indirect approach” to attack the enemy. In order to successfully accomplish this, Sun Tzu heavily emphasized the importance of laying the groundwork for success before the outbreak of hostilities. In Sun Tzu’s definition of war deception before the outbreak of hostilities is a key to success. Sun Tzu believed that employing deception operations is essential. For Sun Tzu, deception operations included political and diplomatic efforts to attack the enemy’s alliances, disrupt his strategy and confuse him as to your intent.

Sun Tzu’s prescription for understanding the enemy’s strategy, the successful execution of deception operations and the use of the indirect approach was continuous intelligence collection and analysis which he discusses in detail throughout all of chapter
Sun Tzu heavily emphasized that intelligence enabled an understanding of the enemy’s strategy thus facilitating the implementation of deception aimed at misleading the enemy and disrupting his alliances. Sun Tzu’s concept of deception operations and intelligence before the battle is nested within his tenet of using the indirect approach to target one’s enemy. For Sun Tzu, “to subdue the enemy without fighting is the acme of skill.”

Like in the maxims put forth by Sun Tzu about how politics and diplomacy are a part of the strategy of warfare, Carl Von Clausewitz developed what he referred to as the paradoxical trinity to explain his political framework for the study of war. Clausewitz’ trinity consisted of the people (representing primal violence and the mobilization and support of the people); the commander and his army (providing the ingenious management of probability, chance and risk in conceiving and executing war); and the government (proscribing the outcomes and policies of war and reassessing these in terms of costs versus benefits). He believed that each of the trinity’s components possessed its own independent rationality of operation and that one could only achieve victory when the proper balance amongst the three dimensions was achieved. Clausewitz professed that any methodology that sought to establish an arbitrary relationship between the elements of the trinity, or ignored the realities of one or more of them, would conflict with actuality and render it completely worthless. From this, the reader can see that both Clausewitz and Sun Tzu understood the importance of the relationship between the people, the army and the government. What both Clausewitz and Sun Tzu say about the linkage of military strategy to political objectives is equally important. Both the Russian and Chinese practitioners of hybrid warfare in the gray
zone recognize the primacy of political objectives and use them to guide their selection of the ways and means needed to achieve the end state desired. Further, both the Chinese and Russian application of a hybrid warfare strategy uses the indirect approach while balancing the trinity in recognition of the importance of linking military action to the will of the people in order to achieve political objectives.

**Chinese Three Warfares**

The Three Warfares (san zhong zhanfa), was approved in 2003 by the Chinese Central Military Commission (CMC) and it provided the concept and direction for the People’s Liberation Army’s (PLA) execution of information operations. The Three Warfares foundation rests on three complimentary strategies: 1) the synchronized use of psychological operations; 2) overt and covert mass media influence; and 3) legal action intended to influence an adversary’s strategy, foreign policy, and the perceptions of overseas target audiences. 21 The original impetus behind the development of what is, ostensibly, the Chinese version of hybrid warfare, was the February 1999 publishing of a book entitled Unrestricted Warfare (literal translation - ‘War without Borders’) by a pair of Chinese Colonels, Qiao Liang and Wang Xiangsui. The book was exceptionally critical of Western constructs for war and was intended as a rejoinder to the swift 1991 Gulf War multi-national coalition victory against Saddam Hussein’s Army in Kuwait and Iraq. The book opined that the coalition relied too heavily on technology for warfighting. 22 The authors advance the idea that the Gulf War is not a viable model for future warfare; instead arguing that technological advances, combined with growing globalism is leading to the dispersion of power outside of nation-states. These factors, combined with technological advances in weapons have merged; creating a new paradigm for warfare. Thus, they put forth a concept for future warfare which
incorporates the use of information, diplomacy and financial levers to achieve political objectives instead of overreliance on technology.  

Notably, the book suggests that in the future the methods used for waging unrestricted warfare must be unified in order to achieve victory. The authors posit that wars will be won beyond the traditional field of battle. They further outline that success can be achieved by successfully combining four separate means for waging warfare in order to reach the required effects and achieve the desired end state. Liang and Xiangsui label these combinations of means as 1) Supra-National, 2) Supra-Domain, 3) Supra-Means and 4) Supra-Tier. Taken a step further, *Unrestricted Warfare* states that the methods used in war may also be used in peacetime and that capabilities traditionally used at the tactical level may also be successfully employed at the strategic level.  

To understand this concept of unrestricted warfare we must examine what the authors mean by these four combinations of means.

The use of national-level, international and non-state organizations is a Supra-National combination according to Liang and Xiangsui. Examples of this are for a country to build a coalition and seek UN resolutions sanctioning a particular country or a UN resolution authorizing the use of force to enforce such sanctions. Choosing a Supra-Domain combination is deciding the domains (land, sea, air, space, cyber, financial, economic, information) where unrestricted warfare will be fought. Supra-Means combinations involve the employment of legal, cultural, technological, diplomatic, economic and military means to achieve political objectives. Supra-Tier combinations are where tactical, operational and national/strategic-level capabilities are brought
together in the selected domain combinations in order to achieve political objectives or objectives articulated in grand strategy.  

Liang and Xiangsui offer that there are eight principles of unrestricted warfare. In their opinion, the first principle was *Omnidirectionality*. For them, the future battlefield was omni-directional; meaning that warfare could be military, para-military or non-military. Taking this idea a step further, the authors believe that, in unrestricted warfare, there is no distinction between non-combatants and combatants. The second principle of unrestricted warfare was the concept of *Synchrony*, which they used to describe the fact that actions need to be arranged in time and space to achieve the desired effects and that some actions could be simultaneous rather than phased. The principle of *Limited Objectives* is used by the authors to emphasize the importance of using enough means to ensure that objectives were met. The *Unlimited Measures* principle stipulates that, in unrestricted warfare, no real restrictions exist on the type of means a nation may employ to achieve objectives. The proper execution of unrestricted warfare involves employing the principle of *Asymmetry* by finding and exploiting an adversary’s vulnerabilities by attacking them indirectly. The *Minimal Consumption* principle specifies the use of only the means necessary to achieve objectives. Unrestricted warfare requires *Multidimensional Coordination*. For Liang and Xiangsui, all means, in all domains and tiers must act in a unified and synchronized manner to achieve desired outcomes. Finally, the eighth principle of unrestricted warfare is the *Adjustment and Control of the Entire Process*, which implies that a continuous assessment of the evolving situation informs the leadership’s use of their intuition to recalibrate the application of required means, in the necessary combinations to achieve success. 
The Chinese have operationalized their Three Warfares strategy in a number of ways. The ways and means they have employed have been calibrated to achieve the political ends they have sought. For instance, the Chinese PLA’s General Political Department’s Liaison Department (GPD/LD), have used “affiliated civilian and business platforms working to ‘promote Chinese culture’ abroad. These include the China Association for Promotion of Chinese Culture (CAPCC); China Association for Friendly International Contacts (CAIFC); China-U.S. Exchange Foundation (CUSEF), The Centre for Peace and Development Studies (CPDS), External Propaganda Bureau (EPB), and China Energy Fund Committee (CEFC).” Another example of how China is operationalizing its Three Warfare’s strategy occurred in mid-December 2010 when Chinese hackers associated with the PLA accessed Google’s password system stealing source code which controls worldwide user access to almost all of Google’s Internet services. Additionally the hackers accessed Gmail accounts associated with human-rights activists and hacked the networks of 33 companies. An analysis of these attacks indicates that they were likely pre-operational reconnaissance to facilitate a longer-term goal of affecting US military plans or US economic policy. But Chinese hybrid warfare isn’t only limited to cyber-attacks, information operations, ‘lawfare’ or economic warfare. Some Chinese hybrid warfare tactics have come close to instigating military conflict at sea.

In the South China Sea there are numerous instances where the Chinese have used commercial fishing vessels to challenge US and Japanese freedom of navigation in areas that China claims as its exclusive economic zone by ramming Japanese Coast Guard vessels or by cutting the towed sonar array of US Navy hydrographic survey
vessels. These aggressive tactics, combined with the Chinese efforts to stake claims in the Spratly Islands by building an island on a partially submerged reef – complete with an airfield capable of hosting a Peoples Liberation Air Force fighter wing – are examples of how China is executing its hybrid warfare strategy in the gray zone by choosing to use their full range of national power, in all domains, and at the strategic, operational and tactical ‘tiers’ to achieve its national political objectives.

Designing Strategy the Russian Way: Defining Political Ends and Aligning Ways and Means

Putin

Studying the Kremlin’s desired political ends associated with Moscow’s grand strategy objectives is important to understanding how Russia is employing a hybrid warfare strategy in the gray zone. “Putin’s Grand Strategy is to preserve Russian global power while maintaining and perpetuating the current system of power and wealth distribution.”29 Key to this is preserving legitimacy amongst the Russian people and reinvigorating the idea of Russian greatness by emphasizing Russian nationalism while securing revenue streams to drive the Russian economy. President Putin does this by grasping openings to consolidate power, while preserving strategic flexibility by establishing economic linkage to China. The Kremlin controls the narrative stream to the domestic media outlets. Furthermore, Putin safeguards national control of critical aspects of Russian industry and the economy while waging economic warfare abroad using the Russian petroleum industry. Putin has supported military reform and increases in military spending to build capability and readiness to support proxy wars. Finally, Putin must keep former Soviet Union republics reliant on Russia; both economically and politically. Thus, Putin views NATO enlargement and the expansion of
the European Union as threats to Russian interests and control over its traditional sphere of influence.³⁰

Russia’s hybrid warfare tactics in the gray zone use deception and disinformation to avoid the potential of a swift response from the US or her allies. This was the case in Georgia in 2008, and both Crimea and Eastern Ukraine in 2014. Even in the face of significant evidence to the contrary, Putin repudiated that the “little green men” were Russian troops until operations to seize these territories were successful. This allowed Moscow to operate more rapidly than NATO, the EU or the US was able to make political-military decisions. Consequently, Russia retained the initiative. Because Putin believed that using conventional troops was too risky, he instead used paramilitary forces; thus exploiting the seam between the US, NATO and the EU. Putin’s hybrid warfare strategy worked in Crimea and, to a lesser extent in Eastern Ukraine. ³¹ Both conflicts were a form of coercive communication where a wide variety of ways and means (military and nonmilitary) were used to communicate political messages and change people’s opinions. The emphasis was on influencing opinions and political positions rather than on military action. But the military and paramilitary components of this strategy were important because the threat of a potential invasion was a coercive measure in and of itself.³² Hybrid warfare in the gray zone is where the Kremlin chooses to operate in order to achieve its strategic objectives. In Putin’s words, “these methods will be as effective as nuclear weapons, but more morally acceptable.”³³

Russian Information Warfare and NetWar

Information warfare has emerged as a key component of Russian strategy. Propaganda has long been a key instrument of information warfare in Russia, but its format and content have evolved to complement the hybrid warfare strategy Russia is
waging in the gray zone. The unique characteristics of modern Russian propaganda are that it uses the language of emotions and judgments while targeting the Russian-speaking diaspora who have maintained cultural, linguistic and emotional bonds with Russia. Ideologically, the content supports the concept of ‘conservative revolution’ by appealing to the ideas of restoring Russia’s rightful place as a global power. It does so by building nostalgia for the power and glory of the former Soviet Union and advocates for supporting ethnic Russians and Russian speakers, wherever they may be. Lastly, it promotes the ideas of the pre-eminence of the Eastern Orthodox Church in Russian society, Pan-Slavism and Eurasianism. The primary theorists behind developing Russian information warfare concepts are Igor Panarin and Alexandr Dugin. Panarin and Dugin are the creators of the NetWar concept and were instrumental in leveraging the Internet and transforming Russia’s use of mass media to suit the target audiences they are seeking to influence. Similarly, Dugin and Panarin’s writing and teaching have shaped the content of Russian propaganda and their neoconservative ideas have influenced Russian grand strategy.34

Dugin

Dr. Alexandr Dugin is a Russian political scientist that worked at Moscow State University from 2008-2014. The author of over thirty books, his teaching and prolific writing have profoundly influenced Russian information warfare theory. His academic achievements can be accessed on the Centre for Neoconservative Studies website. In his book, Post-Modern Geopolitics he coined the term, ‘NetWar’ which was drawn from his analysis of the US concept of net-centric warfare. Dugin asserted that the US and its Western allies were using a network in order to attack Russia with information. Thus, he reasoned that Russia needed a similar network approach to counter Western
messaging. Critical to the success of Dugin’s NetWar approach was simultaneously modernizing Russian information content and dissemination, political institutions, secret services and armed forces to synchronize efforts and achieve unity of effort. The ideological component to Dugin’s NetWar appeals to Russian patriotism by justifying claims on new territories by distorting history and its chronology so that target audiences come to see Russian claims as legitimate. Tied to this are Dugin’s ideas about Russia being the ‘third Rome,’ as well as the concepts of Eurasianism and Pan-Slavism. Dugin put forth these concepts for information warfare to counter what he viewed as efforts in former Soviet Union states to eliminate ethnic Russian minorities.

Dugin’s presence on the Internet has developed a significant network of like-minded contacts of political activists that have assisted him with spreading his ideas exponentially. Dugin’s supporters have ranged from sociology and philosophy students from Moscow State University, to fascism-inclined ‘Natsbols,’ as well as the Russian diaspora in Eastern Europe. Dugin’s Internet sites provide links to his extensive publications, recent announcements made by other neo-conservative Russian leaders and Dugin associates. He maintains an information warfare portal associated with the International Eurasian Movement as well as a website linked with the National Bolshevik Party. Each of these have numerous Internet mirror sites such as Ivan the Terrible Brotherhood’s ‘Oprichnina.’ He is also featured on numerous news and analytical portals such as Vesti TV, Eurasia TV and Knigi Evrazii. Dugin’s announcements are tweeted and re-tweeted on Twitter and his blog posts and writings are posted to social networking services such as Odnoklassniki, VKontakte and Facebook where he has
created discussion groups. During the Russian intervention in Crimea, Dugin was an outspoken opinion leader.\textsuperscript{35}

**Panarin**

Professor Igor Panarin, while at the Russian Diplomatic Academy of the Ministry of Foreign Affairs, wrote Russia’s Information Security Doctrine. His later writing supported the idea that Russia needed to counter Western information operations with its own form of information warfare. Panarin believes that there were two significant phases of Western information operations directed at weakening Russia. The first began with the advent of perestroika and concluded with the dissolution of the Soviet Union. The second phase began in 2000 and, in his view, will last until 2020. Panarin claimed in his book, *Information World War II – War Against Russia*, that the West – in particular the US and the CIA – were behind the color revolutions in the Commonwealth of Independent States and that the Arab Spring resulted from Western-backed social control efforts spread via social networking on the Internet.

To counter these Western-backed, anti-Russian information operations Panarin developed concepts that he believed must be imbedded in Russian information operations doctrine. As such, he defines the principles of *social control* as influencing society, *social maneuvering* as gaining certain benefits through intentional control of the public and *information manipulation* as using legitimate information in a manner that leads to false implications. Additionally, Panarin articulated the principle of *disinformation* as disseminating manipulated or manufactured information and the *fabrication of information* as creating false information. Complementing these principles are the techniques of *extortion of desired information, lobbying and blackmail*.\textsuperscript{36}
The Gerasimov Model

In a January 2013, General Valery Gerasimov, the Russian Federation’s chief of the general staff, penned an article titled “The Main Trends in the Forms and Methods of the Armed Forces.” It was here that he argued that the Arab Spring and the color revolutions demonstrated that the distinctions between peace and war were dissolving and becoming increasingly different from warfare in World War II or the Cold War. Thus, Gerasimov opined that Russian warfare strategy must evolve to place the weight of Moscow’s efforts on domination of the information space and the use of intelligence. Gerasimov believed that Russia’s objectives would more likely be realized in a contactless war through actions at the tactical, operational and strategic levels. For him, the distinction between offense and defense was less evident and he believed that asymmetric activities against adversaries would become more commonplace. He reasoned that the growth of information technology served to reduce the dimensional and cognitive information gaps between the government and the army.37

Gerasimov judged that the Russian military must see war as more than just military conflict. As such, he offered that the ratio of nonmilitary and military means used in war is now approximately 4:1. Included in these nonmilitary means are the use of economic sanctions, diplomacy and political pressure. Noteworthy is Gerasimov’s distinction that Russia should consider these nonmilitary means as part of warfare, while the West uses nonmilitary measures to avoid war. Gerasimov’s advocacy for the use of nonmilitary means in combination with military forces included some prescriptions for doctrinal and organizational change both within the military and within Russian civilian and governmental institutions. Noteworthy among these are task organizing units for combat in peacetime; attacking critical infrastructure to reduce the
economic potential of a state; use of precision guided munitions; use of special operations forces, robotics and incorporation of civil-military operations. Additionally, he stressed the importance of asymmetrically and simultaneously attacking the enemy throughout the depth of the battlespace and the use of information operations. Finally, Gerasimov emphasized the importance of unified action in information operations and for synchronizing information operations with combat in the physical domains.38

Based on these underlying principles, General Gerasimov authored “The Role of Nonmilitary Methods in Interstate Conflict Resolution” in which he proposed a new model for Russian warfare. This model outlined six phases of campaign structure. Each of these phases emphasizes the leading role of nonmilitary means to achieve objectives. The six phases can be seen as a model for the escalation of ‘force’ used to achieve objectives with the increasing use of military means as the phases progress. Gerasimov’s six phases are described as follows: 1) Covert origins. Form political opposition using labor/trade unions, coalitions and political parties. Shape the environment using sustained information warfare. 2) Escalations. Use political and diplomatic pressure against the adversary if the situation escalates. Means available include diplomatic and economic measures. Expect the level of political activity to grow thus revealing political positions of the various players 3) Start of conflict activities. Characterized by both sides’ use of paramilitary engagements, assassinations, demonstrations, sabotage and subversion. Intensification of conflict may pose a military threat to Russian security and interests. Begin strategic deployment of forces if necessary. 4) Crisis. Start military operations combined with significant economic and diplomatic sanctions. Use information operations to shape environment favorable to
military intervention. 5) Resolution. National-level leadership seeks options for altering the political and military landscape within the target region or state. The objective is altering the social reality, economic situation and political environment favorably so that peace and normal diplomatic relations are possible. Phase 6) Restoration of peace involves peacekeeping operations combined with political and diplomatic means to reach a post-conflict agreement.39

Russian military theory for the conduct of a hybrid warfare strategy in the gray zone seeks to wage a ‘contactless war’ by causing an opponent to ‘decay from within’ through information and cyber operations. Information operations is the main effort within this strategic construct with the intent of “projecting a positive national image through culture and public relations [while using a] strategic narrative to keep your opponent intimidated, confused, and dismayed—of exploiting ubiquitous information to appear bigger, scarier, and more indispensable than reality would suggest.”40 The concepts for hybrid warfare in the gray zone put forth by Dugin, Panarin and Gerasimov have informed the formation and development of Russian military doctrine. It is illustrative to examine this doctrine in order to properly evaluate how the Russians have attempted to execute their hybrid warfare strategy in Estonia (2007), Georgia (2008) and the Ukraine (2014).

Russian Military Doctrine

As early as 2010, Russian military doctrine described contemporary warfare as an integrated use of military force and nonmilitary means, to include information operations, in order to achieve political objectives. The goal is to achieve objectives without resorting to military force while simultaneously shaping world opinion to favor the use of force if deemed necessary.41 In 2014, this doctrine was updated to include
the use of “irregular armed force elements and private military companies in military operations,” and the “use of indirect and asymmetric methods of operations.” Many have attributed this shift in military doctrine to the writings of General Gerasimov. His advocacy for the use of nonmilitary tools to achieve political objectives because they are potentially more effective than weapons is a probable catalyst for this noteworthy change in doctrine. Lessons learned in Georgia and Estonia likely informed this doctrinal revision, in addition to the influence of Gerasimov. Regardless, the important take-away is the fact that Russian hybrid warfare in Crimea and Eastern Ukraine in 2014 included the use of irregular forces, mercenaries and criminal gangs in order to achieve Russian political objectives. It is assessed that the use of paramilitary forces and other non-military groups is an effort to give the Russian Federation the ability to operate in a seam of ambiguity and deniability about the Russian state sponsorship of these activities; thus, avoiding triggering UN Security Council Resolutions or NATO Article 5 considerations.

In their December, 2013 paper titled "The Nature and Content of a New-Generation War" which was originally published in the Russian journal of military studies *Military Thought*, authors Col. S.G. Chekinov and Lt. Gen. S.A. Bogdanov outline how the doctrine for Russia’s New Generation Warfare is organized into eight phases. These phases are roughly analogous to the six phases articulated in the Gerasimov model with some notable additions. The eight phases describe an escalation of force model with progression from one phase to the next based on conditions and ability to achieve desired objectives. A full explanation of the 8 phases follows:
• First Phase: Asymmetric warfare comprised of information operations, diplomacy, and economic means to set advantageous military, political and economic conditions

• Second Phase: Use of special operations to conduct psychological operations and deception operations

• Third Phase: Coercing government and military officials to quit their posts through bribes, intimidation or deception

• Fourth Phase: Information operations directed at the civilian population to undermine their support for the regime. The information operations effort is supported by subversion conducted by paramilitary or gangs

• Fifth Phase: Use of no-fly zones and blockades if required. Increased use of paramilitary, gangs or private military companies in conjunction with local resistance forces

• Sixth Phase: Reconnaissance and surveillance in conjunction with subversion directed at the local government to set conditions for military operations. Military operations include the use of SOF, intelligence services, and all types of enabling forces operating across all domains (air, land, space, cyber, etc.)

• Seventh Phase: Employment of required combinations of information warfare, electronic warfare, space operations, use of precision guided weapons and non-lethal capabilities such as biological agents, radiation and microwaves

• Eighth Phase: Conduct of reconnaissance in order to direct special operations forces terminal guidance operations for precision guided munitions, artillery strikes and conventional bombing to destroy remaining resistance forces⁴⁴
As we can see from a review of the writings of notable military theorists and leaders, as well as military doctrine, the Russians have been working to refine their own hybrid warfare strategy. To better understand the evolution of Moscow’s hybrid warfare strategy over the past decade we will examine the Kremlin’s actions in Estonia (2007), Georgia (2008) and Ukraine (2014).

**Russian Hybrid Warfare in Estonia, Georgia and Ukraine**

**Estonia 2007**

Russian hybrid warfare has evolved and modernized through closely watching and analyzing Western techniques as well as the various operations Russia involved itself in since the dissolution of the USSR. Moscow has drawn on lessons learned in Lithuania (1991), Transnistria (1990–1992), South Ossetia (1991-1992), Abkhazia (1992-1993), the first Chechen war (1994–1996) and the second Chechen war (1999–2009). While these lessons learned have ultimately impacted how Russia incorporates aspects of unconventional warfare into its hybrid warfare strategy (Ukraine 2014), we begin our examination of Russian hybrid warfare in the gray zone with a review of the cyber-attacks directed against the Government of Estonia in 2007 because it is the first instance of what is likely a Russian state-sponsored cyber-attack on a NATO country. This event was significant because it raised, for the first time, issues of NATO’s collective defense policy regarding a cyber-attack; while simultaneously foreshadowing the cyber operations, information operations and denial and deception operations that would become key components of future Russian hybrid warfare in Georgia and Ukraine.

The 2007 cyber-attacks against Estonia were ostensibly spawned by a disagreement between Russians and Estonians over Estonia’s movement of a bronze
statue to a less prominent and visible location in Tallinn. This monument commemorates the Soviet Union’s success in driving the Nazis out of the region at the end of World War II and the war deaths resulting from German occupation. To Estonians, the war memorial represented Soviet subjugation, but to the ethnic Russian minority the repositioning of the statue signified further ostracism of ethnic Russians in Estonia. This action resulted in demonstrations perpetrated by ethnic Russian minorities and cyber terrorism targeting Estonia's critical economic and political infrastructure.46

The cyber-attacks directed against the Estonian government are thought to have been conducted by the Russian Business Network (RBN). The most likely scenario is that the RBN conducted the attacks on behalf of the Russian government; providing the government with plausible deniability.47 While not the first cyber-attack in history, nor the largest, it was the first time that a both a country’s government and business cyber infrastructure had been targeted in a coordinated fashion; thus, requiring a state-level response to the attack. In addition to a wide variety of official government websites, affected by the attacks were all major commercial banks, telecommunications companies, mass media and Internet Domain Name Servers. The attacks affected the majority of the Estonian population and posed a threat to Estonia’s national security.48

Estonia responded to the attacks by cutting Internet access from sites external to Estonia in order to restore service to local users. Firewalling an entire county off from the rest of the global Internet had potentially more damaging affects to the country’s economy than the limited sanctions against Estonia that Russia had imposed. Certainly, cutting off access to the Internet outside of Estonia limited the Estonian Government’s ability to counter Russian propaganda.49
Estonian government officials swiftly accused Russia of orchestrating the attacks, but technical experts from both NATO and the European Commission were unable to find definitive evidence of Moscow’s hand behind the cyber-attacks. Not surprisingly, the Russian Government denied involvement in orchestrating and directing the attacks. Ene Ergma, the speaker of the Estonian parliament in 2007, speculated that the attacks may have been a test of NATO’s defenses and ability to respond to cyber-attack. Indeed, the attacks called into question whether or not a cyber-attack on a NATO member country would trigger a NATO Article 5 response. The collective Estonian / NATO response to this virtual aggression demonstrated the weakness of a NATO member states’ cyber defenses and NATO’s lack of readiness to counter the attack; even with cyber emergency response team support. Most importantly, it highlighted to the Russians the fact that even “NATO’s Article 5 [collective defense protection] and U.S. nuclear umbrella guarantees cannot ensure the protection of a nation-state’s sovereignty in cyberspace.”

Georgia 2008

Conflict Background and Russian Hybrid Warfare Campaign Overview

Beginning in 1994, Georgia embarked on a path to inclusion in NATO. The relationship with NATO began shortly after Georgia gained independence from the Soviet Union. In 1992, Georgia joined the North Atlantic Cooperation Council and in 1994 it became a NATO Partnership for Peace country. Since 1994, Georgia has been actively included within the auspices NATO’s Science for Peace and Security (SPS) Program and has hosted a number of multinational Partnership for Peace training exercises. Beginning in 1999 Georgian military forces participated in peacekeeping operations in Kosovo. Georgia’s inclusion in KFOR only ended after the 2008 Russian
military action in Georgia. Beginning in 2002, Georgia’s efforts to gain full membership in NATO intensified when the Georgian government declared an intent to join NATO and develop a NATO Individual Partnership Action Plan; which was approved in 2004. In 2003 Georgia participated in the NATO-led International Security Assistance Force in Afghanistan during the Afghan elections. The outcome of the NATO summit in Bucharest in April 2008 likely presented a red-line for Putin when NATO published in its post-summit communique that “NATO leaders agree Georgia will become a member of NATO, provided that it meets all the necessary requirements.” Georgia’s trajectory for inclusion in NATO was very troubling for Russia, as was the cooperation between the EU and Georgia that had been growing since 1992. Not only was Georgia likely slipping from Moscow’s security orbit, but Russia saw Georgia’s inclusion in the EU as weakening the Kremlin’s economic influence in Georgia.

Georgia and the European Union have maintained relations since 1996 when Georgia was included in the INOGATE structure. INOGATE is an energy cooperative organization existing which includes the European Union (EU), the coastal republics along the Caspian and Black seas as well as their neighboring countries. In 2006, the EU approved a five year action plan, under the auspices of the European Neighborhood Partnership Initiative (ENPI). The ENPI is an EU vehicle for foreign relations outreach with the goal of linking European countries not currently included in the EU for eventual membership in the EU. Russia’s strategic sphere of influence was threatened by the possibility of Georgian membership in NATO because, not only was Georgia on a path to joining an alliance dedicated to countering the Soviet Union during the Cold War, but a Georgia
aligned with NATO had the potential to block Russian access to the Middle East. Additionally, Georgia embodies historic and emblematic importance for Russia since Georgia’s annexation by Russia at the beginning of the 19th Century. Militarily, economically and symbolically, Russia was unwilling to cede Georgia to the EU and NATO. This was counter to Putin’s goal of restoring Russia’s great power status and reviving Russian nationalism. Additionally, the memory of the breakup of both the Soviet Union and Yugoslavia in 1991 was still fresh in the minds of Putin and his key advisors. Not the least of Moscow’s reasons, the color revolutions (popular nonviolent uprisings) in Serbia (2000), Georgia (2003), Ukraine (2004), Kyrgyzstan (2005) and Belarus (2006), combined with the political unrest they inspired in the Caucuses, all served to worry the Kremlin that a similar wave of discontent could arise in Russia. Accordingly, this all factored into Putin’s risk calculus as he considered military options to secure Abkhazia and South Ossetia. In August 2008 Putin chose to act to secure Russian interests in its near abroad. An examination of Russia’s political objectives helps us understand, not only how the Georgian campaign fit into overall Russian grand strategy, but how Moscow’s political objectives drove the hybrid warfare strategy that Putin chose.

The two main goals of the Russian incursion into Georgia in August 2008 were to end the expansion of NATO while restoring Russian regional power and influence. The Kremlin chose to exert its influence in the breakaway regions of South Ossetia and Abkhazia given that there was already an anti-Georgian movement nascent in these regions and because these are areas in Georgia where a majority of the population are ethnically distinct from Georgians. Achieving these broad objectives included ending
Georgian President Saakashvili’s reign and replacing his government with a more pro-Russian regime. Additionally, Moscow believed that controlling the land and airspace of both South Ossetia and Abkhazia enabled them to project power, if necessary, elsewhere in the South Caucasus. Finally, the economic component to Russia’s objectives was to dominate the east-to-west energy corridor in the South Caucasus enabling Moscow to control the critical Baku-Erzerum gas pipeline and the Baku-Tbilisi-Ceyhan oil pipelines.\textsuperscript{57} Controlling these was central to the Kremlin’s aim of leveraging its control over petroleum resources feeding Western European industry and homes for long-term political gain throughout Europe. The means chosen for the campaign included the use of all instruments of Russia’s national power to achieve its strategic ends. The ways that President Putin and his close circle of advisors selected was a strategy of hybrid warfare in the gray zone. We will now turn to an examination of how Russia employed the ways and means associated with this hybrid warfare strategy.

In the summer of 2008, Moscow orchestrated a series of activities designed to set the conditions for the annexation of Georgia. This included military training, airspace violations and information operations on a wide scale. The Kremlin directed cyber operations and heavy propaganda intended to limit Georgia’s decision options by portraying the Georgians as being aggressive toward South Ossetia and Abkhazia.\textsuperscript{58}

Concurrently, the Russian military undertook a series of activities that continued to allow them to set conditions for their attack. These tasks included the staging of additional military forces on the border of Abkhazia and South Ossetia, infiltration of advance party elements of units that would take place in the main attack, reconnaissance of objectives and securing critical infrastructure required for their invasion. Much of this activity was done under the guise of
peacekeeping operations and/or exercises and the Russians used plausible deniability built into the tasks. One such example was using Russian railway repair troops to secure the southern entrance to the Roki tunnel. This tunnel is key terrain because it is a chokepoint along the one viable route, the Transkam road, which crosses the Greater Caucuses Mountains and runs from North Ossetia (in the Russian Federation) into South Ossetia (in Georgia); leading to the South Ossetian capital city of Tskhinvali.59

These preparatory activities were key to the initial success of Russia’s hybrid warfare strategy. Foremost, the low-level, deniable activities allowed the Kremlin to set conditions on the battlefield for initial success while staying below the threshold for international intervention or alerting Western powers and other international organizations, like the OSCE, that a major operation was pending. Secondly, Moscow’s information operations, subversion and diplomatic activity had placed sustained pressure on the Georgian military and political leadership. This degraded their ability to achieve a common operational picture, reach consensus about what was happening, what Russian intentions were and what actions must be taken. Lastly, Russia’s preparatory activities had subtly and quietly changed the military balance of power in both South Ossetia and Abkhazia prior to executing operations.60

The five day campaign in Georgia that involved the use of conventional military forces conducting kinetic operations against the Georgian military wasn’t particularly noteworthy in terms of specific lessons learned regarding how Russia was implementing its hybrid warfare strategy. The use of conventional ground troops and air force capability was only one small component of the overall campaign. What is particularly noteworthy was how Russia employed the use of information warfare, Russian SOF, paramilitary forces, criminal gangs and other irregular forces to accomplish its
objectives. Likewise, Russian use of cyber warfare, propaganda, political and economic warfare to support achieving its desired ends are of significance and this paper will focus more on these aspects to uncover the vulnerabilities associated with Russia’s hybrid warfare strategy.

The Irregular Warfare Component to Russia’s Hybrid Warfare Strategy

Little has been published regarding the part that Russian SOF played in the Georgian war. Some Georgian military reporting indicated that troops in black uniforms were inserted behind Georgian lines via Russian rotary wing aircraft. It is possible they may have been involved in direct action operations, sabotage or subversion, but their actual tasks and purpose are unknown. Both Georgian and Russian media reports also indicate that Russian SOF operated in Georgia, but the details of their activities are unclear.61

There is considerably more reporting regarding the activities of the Caucasus Volunteer Forces. Both the ‘Chechen East and West Battalions,’ working alongside the militia forces of Abkhazia and South Ossetia, were actively in support of achieving Russian objectives during the war. The irregular forces from both Russia and the breakaway regions in Georgia were active in Abkhazia and South Ossetia prior to the outbreak of hostilities and were probably involved in conducting reconnaissance and advance force operations for their Russian confederates.62

Paramilitary forces in the South Ossetian capital city of Tskhinvali harassed Georgian security forces using hit and run style attacks. The use of civilian clothes by militia made it easier for them to melt into the civilian population. The most significant violations of the law of armed conflict were perpetrated by South Ossetian partisans and Chechen volunteer units. This took the form of ‘ethnic cleansing’ by burning the homes
and villages of ethnic Georgians. These violations are well documented by the United Nations and the European Union and both of these organizations have alleged that Russian military forces did little to stop the abuses.  

Despite the official criticisms levied by international organizations on the irregular forces and their Russian allies’ ability to control them, there are alternate sources that indicate that the coordinated use of Russian military forces, combined with paramilitary forces, were successful in accomplishing assigned objectives. Clearly, the Russian military’s prior experiences training with the North Caucasus volunteer forces contributed to their success on the battlefield due to the Russian military being well aware of the advantages and disadvantages associated with employing them.  

Russian Cyber Warfare and Information Operations Support to Hybrid Warfare

The Russian war in Georgia in 2008 is where Moscow successfully integrated the use of information and cyber operations – on a large scale – with military operations and the diplomatic and economic aspects of their emerging hybrid warfare strategy. While information operations and cyber operations, by themselves had been employed in numerous other instances by the Kremlin, they had not been successfully integrated into a cohesive campaign plan involving military forces; from the strategic, to the operational, and on down to the tactical levels.

The Kremlin’s cyber operations were coordinated with the initiation of hostilities on 8 August and they ended when Moscow announced a cease fire on 15 August. Russian cyber-attacks were centrally directed and targeted political, military, judicial, economic and diplomatic websites and Internet services throughout Georgia and its diplomatic missions abroad. Most of the cyber-attacks were carried out by the Russian Business Network (RBN); an organization that is not directly affiliated with the Russian
government and has been involved in a wide variety of hacking and cyber-crime. The form of cyber-attacks directed at the Georgian government was predominantly a Distributed Denial of Service (DDoS) attack. The RBN is the same organization that was widely blamed for the DDoS cyber-attacks directed at the Estonian government in 2007.

Despite the scale and sophistication of the cyber-attacks, Russia’s cyber operations were not as effective as they could have been and thus, had limited positive effects on the overall outcome of the campaign. The principal reason they were not as effective as they could have been was because Moscow placed constraints on their cyber targeting. After the initial cyber-attacks against Georgian government web services, the Georgian government moved quickly to reestablish web services on servers owned and operated outside of Georgia. Complicating Russian targeting was the fact that most Georgian government officials used their personal web-based email accounts from US owned email Internet Service Providers for official business. Similarly, Russia proved unwilling to target the Internet infrastructure of NATO member countries such as Poland, or the Google servers that hosted other Georgian government web services. The paradoxical result of the Kremlin’s self-imposed constraint on targeting, combined with the Georgian government’s quick work to reestablish web services, was the backlash of pro-Georgian blog activity across the Internet. The fact that the Russians were only able to cause short-term disruptions to the flow of information about what was really going on inside Georgia limited the effectiveness of the cyber-attacks and enabled truthful information to undermine the Kremlin’s legitimacy.
Moscow’s information operations in support of their hybrid warfare strategy were synchronized with the phases of their campaign plan. The Kremlin’s information operations messaging stressed three major points: 1) Georgia was the aggressor; 2) Russia was forced to intervene on humanitarian grounds to protect ethnic minorities persecuted by the ethnic Georgian majority and, 3) Moscow’s actions were justified and no different than the US and NATO’s interventions in Bosnia and Kosovo. This narrative did gain traction in Russia and amongst the Russian diaspora despite the overwhelming evidence that surfaced after the war that Russia had indeed been the aggressor. 

The fact that the Kremlin placed significant emphasis on media relations had a positive impact on Moscow’s ability for its information operations narrative to gain traction. The Russian military provided press briefings modeled on the US-style Public Affairs Officer briefings given to the media in Afghanistan and Iraq. Additionally, the Kremlin employed a limited form of an embedded media outreach program by flying approximately fifty reporters to Tskhinvali days before the initiation of hostilities. While Moscow’s contact with Western media was only periodic, the Kremlin did use Russian television to paint Georgia as a US proxy by highlighting the presence of American equipment in Georgia that had really been there for the Partnership for Peace exercise Immediate Response ’08. As a result of these efforts, the Russian information operations effort successfully propagated its messaging and this narrative was predominant through media coverage early on in the war. After the ceasefire, a significant amount of information was brought to light, by numerous sources, that discounted key assertions made in Russian information operations. In the long run, these falsehoods undermined Moscow’s legitimacy; particularly in Western countries.
However, inside Russia, the Kremlin’s information operations storyline became the accepted reality. 69

Russian Lessons Learned in Georgia 2008

Moscow and its military forces learned a number of lessons from their experiences at employing a hybrid warfare strategy in Georgia. These lessons served to spur military modernization and reorganization. Most importantly, the Russian experience in Georgia spawned a renaissance in Russian military doctrine. Evidence of this is the prolific writing of Alexandr Dugin and Igor Panarin and ‘The Gerasimov Doctrine’ which gained significant attention, both inside and outside Russia, after its release in 2013. Following the release of General Gerasimov’s articles on his hybrid warfare model, the Russian military went to work incorporating these new hybrid warfare concepts and lessons learned into future strategies.

Regarding the employment of conventional troops, the Russians learned many lessons. These findings resulted in significant modernization initiatives, organizational changes and training reforms that improved the performance of general purpose forces in Crimea and Eastern Ukraine in 2014. The shortfalls identified in the Georgia war of 2008 span across all of the Russian Army’s warfighting functions as well as joint and combined interoperability issues. 70 There were also lessons learned that are more specific to the information, cyber and unconventional warfare components of Moscow’s emergent hybrid warfare strategy. These will be discussed in more detail.

Joint interoperability between the radios used by the various services of the Russian armed forces, combined with the radios’ vulnerability to electronic warfare drove military commanders to rely on commercial cell phone networks to report information and command and control their formations. This represents a significant vulnerability for the Russians because use...
of commercial cellular networks exposes them to electronic attack, deception operations and intelligence collection.\textsuperscript{71}

While Russian cyber operations succeeded in disrupting Georgian government web services, the speed with which the Georgians recuperated their web capability had unintended consequences for the Russian cyber operations and information efforts. Foremost, the self-imposed constraints on not targeting non-Georgian Internet sites limited the Russians’ efforts to disrupt Georgian Internet access. The quick restoration of Georgian web pages on non-Georgian web servers led to an exponential growth of the ‘blogosphere’ where a free flow of information about what was really going on in Georgia occurred. In the long run, this free flow of information served to undermine Moscow’s narrative abroad about what was actually happening in Georgia; thus, undermining the legitimacy of Russian actions.

The suppression of Georgian Internet dissemination led to the rise of the importance of television news broadcasts. Western media outlets were very amenable to getting the Georgian government accounts of what was happening inside Georgia and these accounts undermined the Kremlin’s claims in Russian media about what was happening. The Western media’s willingness to broadcast the Georgian message undermined Russian legitimacy with the international organizations and the population of Western countries.\textsuperscript{72}

Russian military and political leaders learned three principal lessons from the information operations component of their hybrid war strategy: 1) Using verified, factual information that supported the Russian narrative on the Internet or the media. 2) Uncontrolled embedded media can be a blessing or a curse because they can either
support the ‘official’ narrative by reporting/corroborating official narrative of events or by reporting factual information that undermines the ‘official’ themes and messages. 3) Cameras are everywhere and authentic. First hand videos and pictures can easily support, or undermine, any government efforts to manipulate the narrative with information operations.

Russian political and military leaders reached a consensus that the principal threats to Russian security are popular uprisings in the North Caucasus and unrest and social reform demonstrations in the Commonwealth of Independent States. Thus, the Kremlin and the Russian military prioritized the modernization of the Russian military to optimize it to meet these threats. The most significant organizational change that Moscow implemented to improve use of conventional military forces in future hybrid warfare scenarios was to increase the use of contract, or professional enlisted soldiers, instead of relying on conscripts.73

Additionally, the Kremlin altered the rules for recruiting military manpower when President Putin issued an order authorizing foreign citizens to serve as contract Soldiers in the Russian military. This change allowed the military greater capability for unconventional warfare by allowing more people with language, ethnic and/or family ties to surrounding countries to serve in the military. Clearly, Russia recognized the importance of how important the human factor would be in future conflicts. Additionally, Putin’s decree legitimized the practice of raising paramilitary forces to assist the Russian military in accomplishing its objectives abroad.74

To increase its ability to respond to future requirements to implement its hybrid warfare strategy the Kremlin embarked on a project to reorganize portions of its tactical
units into mobile strike groups. In essence, these units are rapidly deployable and are task organized at the regimental-level and below to operate as an organic, integrated combined arms team that is supported by organic enabling capability. This is very similar to the US Army modular Brigade Combat Team concept in which brigades are organically organized as a combined arms team with assigned artillery, engineer, intelligence, signal and logistics capability. The Russians took this concept a step further and added dedicated attack and lift helicopter support to the mobile strike groups.\textsuperscript{75} By 2009, Moscow’s military had reorganized eighty-five brigades; forty of which were reorganized into mobile strike groups. Additional restructuring included creation of specialized brigades for rocket artillery, artillery, electronic warfare, air defense, missiles, engineers, special forces and reconnaissance.\textsuperscript{76}

Lastly, Russia invested in equipping its tactical units with kit suited to the modern battlefield in order to be more effective in future hybrid warfare scenarios. Major end items include unmanned aerial vehicles, improved armored vehicles and precision guided munitions.\textsuperscript{77} Individual Soldier equipment was also improved with the fielding of the ‘Ratnik Future Soldier Individual Equipment Gear’ which provides improved protection against small arms, increased reconnaissance equipment, global positioning systems, night vision and communications equipment.\textsuperscript{78}

Crimea and Eastern Ukraine 2014

Conflict Background and Russian Strategic Objectives

Following the dissolution of the Soviet Union, NATO began a dialog with Ukraine and implemented a process of increasing cooperation after Kiev joined the North Atlantic Cooperation Council in 1991. Subsequent to that, in 1994 Ukraine entered NATO’s Partnership for Peace program. Beginning in 1997, Ukraine and NATO signed
the Charter on Distinctive Partnership thus establishing the NATO-Ukraine Commission (NUC). President Kuchma signaled his intent to move toward NATO membership with his announcement at the 2002 NUC meeting in Reykjavik. Later in 2002, the NATO-Ukraine Action Plan agreed to at the NATO foreign ministers meeting further deepened Ukraine’s involvement in NATO and set Ukraine on a path to integration in the Eurozone. For Putin, NATO likely crossed a red line when, in April, 2008 allied leaders attending the NATO summit in Bucharest announced in their end-of-summit communique that Ukraine would eventually become a member of NATO. The August 2009 Declaration to Complement the Charter on a Distinctive Partnership between NATO and Ukraine formalized both NATO and Ukraine’s intent for Ukraine’s inclusion as a NATO member. This process was put on hold after the new Ukrainian government under President Yanukovych decided to take membership in NATO off of the table. This track was further solidified in 2010 after a motion in the Ukrainian parliament was approved that excluded Ukraine’s integration into NATO.79

John Mearshimer asserts that Putin’s actions in both Crimea and Eastern Ukraine were, from the Russian point of view, completely reasonable. He takes this idea a step further and asserts that, had NATO not been so aggressive about expansion into countries traditionally inside Russia’s security sphere then Moscow would have not resorted to the use of force to secure its objectives. Mearshimer also attributes the Kremlin’s trepidation regarding Western intentions in Ukraine to the expansion eastward of the EU and the overt support the West provided to the pro-democracy movements, such as the 2004 Orange Revolution in Ukraine.80
Numerous Ukrainian domestic political, economic and cultural factors converged to create conditions that very likely contributed to Moscow’s decision to annex Crimea and then push into Eastern Ukraine. For sure, these domestic factors created conditions inside Ukraine that were favorable for Russian intervention. From 2004 onward a conflux of factional competition amongst oligarchs, mafia and public officials led to a series of scandals, assassinations and electoral challenges. These dynamics, combined with discontent over Ukrainian government and business expanding economic ties to the West, undermined popular support for the government and created social unrest. This was particularly true amongst the ethnic Russian population (approximately 25% of the national population) that resides principally in the eastern provinces. Following Viktor Yanukovych’s narrow 2010 victory over Yulia Tymoshenko in the presidential race, he submitted a bill to the Ukrainian parliament, which was approved in early June 2010 that reversed the country’s trajectory toward NATO membership although the law allowed for continued NATO cooperation. Yanukovych further slowed Ukraine’s progress toward NATO and EU inclusion in late 2013 when he declined to sign the EU’s Eastern Partnership agreement and instead opted for membership in Russia’s Eurasian Economic Union. These anti-Western political moves deepened the anti-Russian sentiment in Ukraine and set in motion a series of protests and violent uprisings against the Yanukovych regime which ultimately led to Yanukovych and members of his inner circle fleeing to Russia in February, 2014. The departure of Yanukovych set in motion Moscow’s preparation for the March, 2014 annexation of Crimea and the subsequent Russian intervention in Eastern Ukraine.
Russia’s strategic objective in Ukraine in 2014 was to halt NATO expansion and reassert its influence in countries on its periphery that the Kremlin has traditionally relied on to provide a strategic buffer against invasion. Additionally, Moscow’s goals in Crimea and Eastern Ukraine involved considerable geopolitical elements vital to Russia. Foremost in Crimea is the fact that the port in Sevastopol is the home of Russia’s Black Sea Fleet and is the only warm water port for the Russian Navy with access to the Mediterranean Sea, the Caucasus, Balkans and Mid-East. Crimea is an important strategic location for Russia and controlling this seaport provides significant economic and military advantages to Moscow.84

National-level political factors also served as an inducement for the Kremlin to annex Crimea and then conduct operations in Eastern Ukraine. These consisted of Russian and Ukrainian domestic politics and a strong undercurrent of discontent with Ukraine’s march toward inclusion in the EU and NATO. Moscow’s need to exert its security influence came to the forefront the closer that Ukraine came to NATO membership. Lastly, as in Georgia, Putin’s desire to return Russia to great-power status was built around growing Russian nationalism. The Kremlin’s stated pretext for conducting operations in Crimea, and especially Eastern Ukraine, was ostensibly to protect ethnic Russians that were not being treated fairly and humanely by the local government; an excuse that played to the neoconservative nationalism Putin has long been cultivating.85

Much like it did in Estonia and Georgia, Russia used a hybrid warfare strategy to achieve its political objectives. It did so by using all elements of Russian national power to exert its influence over a former-Soviet state in which the Kremlin determined it had
vital national interests at stake. The means Moscow chose to employ included information operations, economic leverage, diplomatic activity and military operations.\textsuperscript{86} The ways in which Putin employed these means in Crimea and Eastern Ukraine represented a significant departure from previous instances of using a hybrid warfare strategy. In each case, Moscow demonstrated that it had improved its capabilities significantly. The initial effectiveness of Putin’s hybrid warfare strategy will be examined in more detail.

Russia’s application of a hybrid warfare strategy in Crimea and Eastern Ukraine in 2014 was similar to its operations Georgia in 2008 with notable improvements. Moscow’s 2014 campaign was organized into three main phases: 1) identification and arrangement of political and social groups, resistance movements and ethnic Russians whose interests aligned with Moscow’s objectives; 2) movement of paramilitary forces to link up with resistance forces in critical areas adjacent to initial objectives and 3) commencing military operations. The first two phases are critical because they enabled the Kremlin to evaluate resistance potential, build a base of popular and local political support while conducting reconnaissance, and conduct operational preparation of the environment and advance force operations. When combined with information operations and cyber, the initial phases enabled Russia to set the conditions for execution of military operations if necessary.\textsuperscript{87} As we will see in our examination of Russia’s operation to annex Crimea, the military operations phase of the operation proceeded unopposed due, in part, to the work Moscow had done during the first two phases to set the conditions for success.
Russian Operations in Crimea

In Crimea, ethnic, linguistic and political factors worked in Moscow’s favor as they executed their hybrid warfare strategy. Foremost was the fact that the population in Crimea was largely a Russian-speaking majority that has historically been favorably aligned with the Kremlin. These pro-Russian separatists became increasingly disaffected from the pro-Western government in Kiev and began a series of demonstrations while claiming that ethnic Russians in Crimea were at risk. Following the departure of Yanukovych, the principal leader of a sizeable paramilitary unit in Crimea, Sergei Aksyonov, urged Putin to help. Seeing the resistance potential in the local Crimean population encouraged the Kremlin to act to secure its interests in Crimea. 88

On 23 February 2014, Crimean paramilitary forces, assisted by Russian Special Forces and intelligence services, secured critical infrastructure and key terrain, such as military bases, airports and government offices. Moscow’s troops were essentially unopposed and these actions occurred with minimal violence and no loss of life. Seeing the futility of militarily confronting the paramilitary forces, the Ukrainian government directed the military not to intervene. By 11 March, 2014 a joint resolution between the Supreme Council of Crimea and Sevastopol declared their intent to sponsor a referendum on joining Russia. Less than a week later, Crimea and the Russians approved a treaty incorporating Sevastopol and the rest of the Crimean peninsula into Russia. 89

An analysis of the Kremlin’s execution of its hybrid warfare strategy reveals significant improvements in Russian military performance as well as synchronization of the diplomatic and informational aspects of their strategy. To set the conditions for the
military phase of the operation Moscow leveraged the use of information operations and cyber warfare.

The narrative the Kremlin directed at the West and the international community was that Russia’s action to annex Crimea was supported by both the local people in Crimea and by Russian citizens. Further, the storyline included assertions that the annexation was legitimate and legal because Russia was only acting to protect the safety of ethnic Russians that were being marginalized and mistreated by the Ukrainian Government.

To build the support of the local Crimean population and amongst Putin’s domestic audience, the Kremlin sought to bolster the strength of the ties ethnic Russians in Crimea had to Russia. To this end the Kremlin highlighted the long history of Russian involvement in Crimea. Key to the overall success of the regional information operations aspect of the hybrid warfare strategy was Moscow’s control over the mass media.

Russian information operations themes were organized around these three central ideas: 1) Russian values and nationalism – as opposed to the liberal values of the West; 2) Moscow’s history of linkage to Crimea and the unified nature of the Russian and Ukrainian states; and 3) Attempting to divide the West against itself by pitting the US against the EU.

Overall, the Kremlin’s actions to seize and control Crimea were wildly popular amongst Russians. This view was strengthened by the positive mass media coverage of Russia’s actions; facts which point to the efficacy of the information warfare element of the Kremlin’s hybrid warfare strategy. One criticism of the information operations
campaign was that, over the long term, Russia’s efforts at deception (ambiguously using ‘little green men’ versus operating overtly and taking responsibility for actions) in the Crimea operation undermined Russia’s credibility with Western nations and international organizations.90

The military phase of the campaign demonstrated a number of improvements in the Russian military’s ability to execute its hybrid warfare strategy. Command and control of the Russian operation in Crimea was decentralized in execution, unlike the Soviet-style centralized control during the operations in Georgia in 2008. The increased use of SOF and the higher readiness level of the Russian airborne infantry units enabled them to use this decentralized command and control structure. Joint and interagency integration was improved as demonstrated by the use of naval infantry and intelligence service forces alongside SOF and the airborne infantry. Improved ability to achieve combined arms effects was evident due to the improvements in synchronization of enabling capability (intelligence, engineers, reconnaissance, etc.) with fires and maneuver. Most significant was the Russians’ astute use of the human terrain in Crimea. Solid intelligence work beforehand enabled achieving an understanding of the resistance potential nascent in the local population. The hybrid strategy utilized an unconventional warfare military component which was executed principally by SOF and intelligence services working by, with and through local pro-Russian paramilitary groups and resistance forces.91

As part of the overall hybrid warfare strategy, Moscow used an exercise of significant size, ‘West 2013,’ which spanned from the Baltic Sea to the Ural mountains, as cover for action for the movement of the forces associated with the Crimea
operations. This deception effort, combined with the use of digital communications and electronic warfare, led to Moscow achieving strategic surprise. Both the Ukrainian and Western governments were unaware that the Crimea operation was imminent.92

**Eastern Ukraine 2014**

Following the ousting of President Yanukovych and his subsequent exile in Russia, Putin seized the opportunity presented by a wave of pro-Russian popular uprisings in Eastern Ukraine against the government in Kiev to take action to secure his interests in the region. Using security preparations already in place for the Sochi Olympics, the Kremlin took action in Crimea on February 26 2014. The actions in Crimea motivated the passions of the pro-Russian population in Eastern Ukraine to agitate for secession from Ukraine in order to become a part of Russia. With his Crimean strategic objectives in hand by the end of March 2014, Putin took advantage of the groundswell of pro-Russian and secessionist sentiment in Eastern Ukraine – and the fact that he had a substantial force poised in the Crimea ready to execute a hybrid warfare strategy – and ordered Russian SOF, paramilitary forces and Moscow’s intelligence services to assist the pro-Russian movements in Eastern Ukraine in their bid to separate from Kiev and become part of the Russian Federation.93

The principal areas in Eastern Ukraine where the pro-Russian separatists are most active is in the oblasts (provinces) of Donetsk and Luhansk. Demonstrations in February and March 2014 led to sporadic violence. These events led to an increase in anti-government demonstrations in April and the seizure of the Donetsk Regional State Administration building by pro-Russian separatists. The Security Service of Ukraine (SBU) was initially successful in retaking the building, but in April pro-Russian demonstrators launched a successful operation to seize government offices in the
Kharkiv, Donetsk and Luhansk oblasts. In Donetsk, the pro-Russian insurgents announced the establishment of the People’s Republic of Donetsk and called for a referendum on joining the Russian Federation.\textsuperscript{94}

Mid-April Ukrainian government counterattacks stalled amidst reports of Ukrainian troops refusing to fire on rebel forces or switching sides and supporting the insurgents. Another contributing factor to Ukraine’s inability to successfully counterattack was a lack of combat power. Rebel forces, supported by Russian intelligence, equipment and troops outmatched the Ukrainian military. Lacking sufficient offensive capacity, Kiev’s forces attempted to isolate the rebels in Donetsk and Slovyansk. With the situation approaching a stalemate, the insurgents focused on consolidating their positions, expanding control over government infrastructure and strengthening their defenses. On 22 May, insurgents in the Luhansk and Donetsk oblasts announced the establishment of ‘New Russia’ and ordered the nationalization of all private industry while simultaneously mandating the official religion as Eastern Orthodoxy.\textsuperscript{95}

During the first two weeks of July, the Ukrainian military launched a counteroffensive. This series of operations drove the insurgents into their redoubts in Donetsk and Luhansk. The 17 July 2014 downing of the Malaysian commercial airliner by pro-Russian insurgents brought increased international scrutiny to Russia’s involvement in supporting the insurgents. The release of information of the Russian-supplied BUK surface to air missile system being responsible for the shoot-down led to Moscow pulling back on its more overt support to the insurgents. Thus, by the first week
of August, the Ukrainian counteroffensive was successful in regaining Kiev’s control over three-quarters of the land once controlled by the rebels.96

The EU and Russia brokered a cease fire between the insurgents and Ukraine in September 2014. The cease-fire held, despite some minor skirmishes perpetrated by both sides. However, by early November indicators of a resumption of hostilities emerged and by mid-November Russian conventional forces, supported by tanks, crossed the border into Ukraine in support of the insurgents. One perspective on this is that Moscow’s conventional intervention in Ukraine represents a failure of unconventional warfare, supported by information operations. An alternate viewpoint is that the Kremlin’s unconventional warfare and information operations set the conditions for a conventional invasion; if required.97 Regardless, despite Moscow’s brief intervention with conventional forces, the military and political situation in Eastern Ukraine has essentially devolved to a stalemate with minor flare ups along the line of control or exchanges of artillery fires.

Unlike in Crimea, Russian actions in Eastern Ukraine revolved around support to a violent separatist movement in a neighboring state. Russian Special Forces leading proxy forces against Ukrainian forces permitted the pro-Russian populations of the Donetsk and Luhansk regions to proclaim their independence. Moscow’s approach to execution of a hybrid warfare strategy in Eastern Ukraine had some of the same hallmarks of the hybrid warfare strategies the Kremlin pursued in both Georgia and Crimea. SOF and intelligence services conducted unconventional warfare by supporting local resistance forces. In support of the unconventional warfare component to
Moscow’s hybrid warfare strategy was the full use of diplomatic, economic, information and cyber warfare in order to achieve its political objectives.\textsuperscript{98}

The features of Moscow’s hybrid warfare strategy in Eastern Ukraine were: 1) Robust use of information operations designed to favorably shape the narrative, encourage pro-Russian separatists and deceive NATO as to Russian involvement thus weakening the political resolve of Western nations to respond; 2) SOF and intelligence services support to pro-Russian separatists; 3) Staging substantial conventional combat power on the border as a deterrent to Kiev; 4) Use of Russian troops to support pro-Russian separatists; and 5) Achieving limited strategic objectives by securing ground in politically contested areas.\textsuperscript{99} Our analysis of Moscow’s use of a hybrid warfare strategy will focus on Russia’s use of unconventional warfare supported by information operations, cyber and intelligence in order to identify exploitable vulnerabilities associated with the Kremlin’s approach.

The Unconventional Warfare Component to Russia’s Hybrid Warfare Strategy

Russia’s unconventional warfare efforts were focused on supporting the pro-Russian separatist groups in Luhansk and Donetsk. Moscow’s Special Forces (SPETSNAZ) and intelligence services focused on equipping and training them as well as providing operational direction and intelligence support. Putin’s strategic and operational objectives aligned with the insurgents’ aims of 1) promoting and sustaining New Russia; 2) challenging the ability of the Ukrainian government to control Donetsk and Luhansk while promoting popular unrest and stymying talks to end the conflict.\textsuperscript{100}

Russian SPETSNAZ operated in both Crimea and Eastern Ukraine clandestinely and were paired with Russian military intelligence elements (GRU). These ‘little green men’ performed the most important seizures of critical infrastructure and then withdrew.
from these objectives after turning control of them over to the insurgents. This enabled Moscow to achieve plausible deniability and thus diminish international condemnation. Evidence from Russian involvement in Ukraine indicates that the Kremlin utilized some SPETSNAZ troops recruited from local eastern Ukrainian populations. These Special Forces engaged in political intimidation, psychological operations and subversion of local political officials in order to support achieving insurgents’ (and Moscow’s) political objectives.¹⁰¹

As part of the unconventional warfare aspect of Russia’s hybrid warfare strategy, Moscow supported a number of pro-Russian groups within Ukraine. Additionally, the Kremlin employed paramilitary forces. One such Ukrainian paramilitary force, raised principally from within Ukraine, was the Russian Orthodox Army. Moscow supported a paramilitary force that originated from outside of Ukraine; the Chechen ‘Vostok’ Battalion.¹⁰²

In addition to these paramilitary and insurgent forces was the Night Wolves motorcycle club with chapters throughout Russia, Ukraine, the Baltics, Caucasus, the Balkans and Germany. The Night Wolves are Russian nationalists with five thousand members who include President Putin on their rolls. Many members are former SPETSNAZ or military soldiers and the group is endorsed by the Russian Orthodox Church.¹⁰³ In March, 2014 they were involved in armed operations to seize Crimea and in May 2015 the Sevastopol city government rewarded them with a gift land in the Black Sea port city for construction of a multi-use extreme sports center.¹⁰⁴ ¹⁰⁵ In March, 2014 they were awarded Russian commendations for their actions in Crimea.¹⁰⁶ The Night Wolves have also been prominently featured in elaborately staged and heavily
resourced neo-Soviet Russian propaganda in Simferopol; Crimea; a live primetime broadcast on Russian TV. In the spring of 2014 they were involved in fighting in the Donbass region of Eastern Ukraine; paramilitary roles that earned them a number of casualties as well as US sanctions.

Cossack mercenary forces, supported and paid by Russia, also operated in Ukraine. Cossack groups operating in Ukraine were raised internal to Ukraine as well as drawn from the broader Cossack population of over six-hundred-thousand Cossacks throughout Russia. Chetnik Guards are another mercenary group that operated in both Eastern Ukraine and Crimea. The Chetnik guards are ethnic Serb volunteers and often worked alongside Cossack units in Ukraine.

Russian-associated paramilitary groups operate in Eastern Ukraine in support of Ukrainian insurgent groups. The leader of the Ghost Brigade is Alexey Mozgovoy, a Russian Cossack, whose unit includes ethnic Germans, Russians, Ukrainians, Slovaks and Bulgarians. Another Russian Cossack, Alexander Mozhaev, is known to lead the Wolf's Hundred which is a paramilitary unit fighting alongside pro-Russian insurgents. These paramilitary units are alleged to operate with the approval and support of the Kremlin, but their links to Russia are deniable thus allowing them freedom of action.

Russian military support to insurgent and paramilitary organizations in Eastern Ukraine was both direct and indirect. The indirect aspects of Moscow's support consist of information operations, cyber operations, diplomatic and political support and economic leverage and coercion.

The direct support the Kremlin provided to insurgents goes far beyond simply equipping, training, providing intelligence, advice and assistance on operations. There is
evidence that indicates Russian intelligence agents (or former agents) assumed leadership roles in the major insurgent organizations in Eastern Ukraine. For example, the man who was primarily involved in raising and leading the rebels in the Donbass region was Igor Girkin; a Russian citizen who is a well-known former member of the Russian military, FSB and GRU. Girkin is tied to involvement in a wide range of paramilitary units throughout the Balkans, Transnistria and Chechnya. Girkin became the leader of the self-proclaimed Donetsk People’s Republic in April 2014 following his involvement in raising and leading groups of pro-Russian rebels in Crimea. Another example of Russian direct involvement in organizing and leading the insurgency in Eastern Ukraine is Alexander Borodai; an associate of Girkin whom he appointed as the Prime Minister of the Donetsk Peoples Republic. Borodai is believed to have served in the Russian FSB; rising to the rank of Major General. Another emergent leader of the insurgency in Eastern Ukraine, with a pedigree in the Russian GRU is Igor Besler. Ukrainian intelligence services allege that Besler was under the authority of the GRU when he began organizing pro-Russian rebel units in Crimea in February 2014. Subsequent to Besler’s efforts in Crimea he became involved in leading an insurgent group in Eastern Ukraine.¹¹³

Russian Cyber Warfare and Information Operations Support to Hybrid Warfare

The Russians are well known for having one of the most well developed and sophisticated, national-level cyber operations capabilities in the world. Their only peer-competitors are the United States and China. Moscow’s cyber operations capabilities were used to support their hybrid warfare strategy in Crimea and Eastern Ukraine. Much like the Kremlin’s cyber operations in both Estonia and Georgia, the links back to the Russian state are inconclusive, but Russia’s official hand in supporting and directing the
cyber operations is strongly suspected given the sophistication of the attacks and their close coordination with the unconventional warfare aspects of Putin’s hybrid warfare strategy. One thing that is clear is that the sophistication and aggressive nature of the cyber operations exceeded anything previously seen in Russian hybrid warfare in Estonia or Georgia. One example is the use of malware named ‘Snake’ which is attributed to Russian efforts to gather intelligence throughout the Ukrainian government after Yanukovych fled to Russia. Another example of the sophistication of the cyber-attacks are the use of DDoS attacks to degrade Crimean government Internet services. Additionally, hacking against cellular companies, landline telephone services and Internet Service Providers disrupted communications and affected social networks as well as enabled cyber-espionage directed against the Ukrainian Prime Minister and ten Ukrainian embassies.114

Dr. Mark Galeotti’s assessment of Russian information operations in Crimea and Eastern Ukraine is that the Kremlin was keenly aware of the importance of closely coordinating the employment of information operations in conjunction with intelligence driven military operations. For Galeotti, evidence of this close coordination is the fact that, in conjunction with the thorough penetration of the Ukrainian government by Russian intelligence organizations and use of military intelligence services and SOF to support insurgent organizations, “Russian media and diplomatic sources have kept up an incessant campaign to characterize the ‘Banderite’ government in Kyiv as illegitimate and brutal, while even cyberspace is not immune, as ‘patriotic hackers’ attack Ukrainian banks and government websites. The essence of this non-linear war is, as Gerasimov says, that the war is everywhere.”115
Moscow’s use of both the Internet and mass media resulted in deceiving the West as to Russian involvement in Ukraine, thus, creating friction amongst the NATO allies about how to respond to actions in Crimea and Eastern Ukraine. The Kremlin’s information operations were an essential element to its strategy of hybrid warfare. Combined with the use of unconventional warfare, threats of conventional military involvement, political intimidation and subversion, Russian information operations achieved the effects Putin needed for his “strategy of plausible deniability” to succeed.116

Moscow’s information operations strategy was designed, in part, to ensure that NATO and its allies saw Russian actions through the Western traditional lens, in which there is a clear distinction between peace and war. The intent was to play on what Moscow perceived as a confirmation bias amongst Western intelligence and diplomatic services by ensuring an absence of the indicators they believed the West was looking for to see if or not Russia had invaded the Ukraine. Absent unambiguous indicators, Western leaders were unable to recognize what was truly occurring in Ukraine until it was too late. Information operations were essential to ensuring Russia was able to achieve its goals without unambiguously invading Ukraine with ground troops. Another way to describe how information operations fit into Russia’s hybrid warfare strategy is to see it as “a conflict of coercive communication – armed politics – in which actions are designed to send a political message, rather than militarily defeat an enemy”.117

The foundational principle upon which Russian information operations in Ukraine are based is the concept of ‘reflexive control.’ This principle is grounded in Soviet-era propaganda theory in which the propagandist uses opportunities created by the pre-

54
existing tendencies present in an adversary to adopt a particular idea or direction. In
Ukraine, the primary goal of the Kremlin’s information operations was to convince the
West not to become involved in the conflict; a predisposition that Moscow’s information
operations strategy was designed to exploit using the reflexive control concept.

The key components of this information operations campaign were: 1) Denying of
Russian military and intelligence service direct involvement in Ukraine; 2) Concealing of
the Kremlin’s goals; 3) Using plausible deniability to position Russia as a nation with
interests in mediating and thus controlling the outcome of the conflict; 4) Employing
muscular military deterrence activities and threats to dissuade NATO and the West from
military involvement; and 5) Manipulating the narrative about the nature of the conflict in
the Ukraine through mass media and the Internet. Toward these ends, the ways
underpinning the Kremlin’s information operations in Ukraine utilized a narrative
consisting of several messages and themes that supported the goals described above
while fitting into the framework under which the key components of the information
operations campaign were organized.

The narrative Moscow crafted for consumption abroad mixed the use of threats,
accusations, deception and secrecy. Consistent themes centered on denying Russian
involvement. Concurrent with this was the use of messages to portray that Russia
possessed significant military capability and therefore the West would be unwise to
become directly involved. Moscow also consistently accused the West of fomenting
Ukrainian aggression against ethnic Russians in Ukraine and portrayed the West as the
true agents behind the conflict. For audiences abroad, Russia characterized its actions
as supporting democracy the will of the people in Ukraine. Further, the Kremlin tailored
its messages abroad to portray Russia as only desiring peace and to portray its actions in Ukraine as justified due to the persecution of ethnic Russians at the hands of the illegitimate Kiev government.\textsuperscript{119}

Inside Crimea and Eastern Ukraine, Moscow used information operations to bolster the pro-Russian insurgent forces while encouraging them to reject the government in Kiev. The themes and messages centered on countering the liberal democratic alternative offered by the Ukrainian government and the West. As such, Moscow’s themes stressed how the neoconservative form of Russian autocracy was ‘true liberty’ and that Russian conservative values and traditions were a better alternative than the decadent liberal values offered by the West. Additionally, Russia countered the idea of Ukrainian membership in the EU by asserting that it would only result in an imposition of ‘austerity programs’ and negatively affect ordinary Ukrainians. As an alternative, the Kremlin offered membership in the Eurasian Economic Union along with economic aid in the form of proposals to purchase Ukrainian debt while offering significantly discounted prices on Russian gas. These themes and messages were disseminated using the Internet and mass media; particularly Moscow’s state-controlled television station, Russia Today (RT), which dominates the airwaves in Russia’s near abroad with its slick, professional production that is tailored to a youthful audience.\textsuperscript{120}

Within Russia, the Kremlin’s information operations were designed to build support for Russian actions supporting the separatists in Ukraine. This narrative focused on portraying the West and NATO as encroaching on Russia’s borders and threatening Russian security. Additionally, Moscow portrayed NATO and the West as
attending to keep the Russian people divided while denying Russia its rightful place as a global power.\textsuperscript{121}

Russian Lessons Learned in Crimea and Eastern Ukraine 2014

The Kremlin’s hybrid warfare strategy in Crimea and Eastern Ukraine was inclusive of all elements of Russian national power. Putin included the use of direct military action and unconventional warfare supported by a comprehensive cyber and information operations campaign, coercive diplomacy and economic levers to achieve his national goals and objectives.\textsuperscript{122}

Russian cyber and information operations evolved such that cyber operations were used to support information warfare and synchronized to support unconventional warfare operations. The Kremlin used coercive diplomacy and economic measures which supported its information operations goals. Moscow successfully ensured unity of effort amongst disparate elements of the Russian government and ensured both strategic-level actions and tactical activities were mutually supporting.\textsuperscript{123}

The Kremlin and the Russian military succeeded in employing SPETSNAZ and paramilitary forces to conduct unconventional warfare supporting Ukrainian insurgent organizations in Crimea and Eastern Ukraine. Russian SOF and intelligence services led the organization of political resistance movements and the formation of shadow governments to counter the rule of the Ukrainian government. Russian SOF and intelligence services worked to give Moscow deniability in Russian direct involvement in Ukraine to the extent that NATO and Western governments were unable to effectively respond to Russian actions. At the local level, the use of paramilitary forces and insurgents to conduct a campaign of coercion and subversion successfully undermined the local government while supporting insurgent political goals and objectives. Moscow
was able to effectively sustain the military and paramilitary forces in the field while providing the insurgents the funds, supplies, ammunition and equipment needed to counter Ukrainian government security forces. Finally, these tactical activities were supported by information operations, cyber-warfare and coercive diplomatic and economic means; all of which were backed up by the threat of Russian use of conventional military force to protect ethnic Russians against abuse and thus, discourage NATO and the West from intervening.\footnote{124}

A counterpoint to Moscow’s success in Ukraine is the fact that Russia has yet to resolve the conflicts in Eastern Ukraine. The military situation on the ground has devolved into what is ostensibly a frozen conflict despite skirmishing that occurs along the line of control. The current state of affairs gives the Kremlin some leverage over Ukraine if the government in Kiev begins tilting back toward the West. While Putin may have considered this a minimally successful outcome from the beginning, there is no political end in sight to the conflict and it continues to serve as a political and economic drain on Russia.

As we have seen, Moscow depends on the use of Landpower to achieve its objectives. SOF and intelligence services conducting unconventional warfare are integral parts of a Russia’s broader hybrid warfare strategy. Conventional troops are a coercive deterrent that offer Putin the flexibility to escalate the use of force, if necessary, to accomplish his national objectives. The Kremlin’s use of SOF and intelligence services, alongside the employment of paramilitary forces, to support insurgent organizations represents a qualitative shift in the means and ways that Moscow is choosing to implement its hybrid warfare strategy. Russia’s ability to successfully use
national-level information operations and cyber capabilities in a unified and
synchronized fashion to accomplish both strategic-level goals as well as support tactical
operations also represents a substantial improvement in demonstrated capability.\textsuperscript{125}

Contributing to Russian improvements are the modernization initiatives directed
by the Kremlin that significantly enhanced the readiness of its SOF and airborne units.
These initiatives include upgraded command and control equipment, modernization of
individual soldier gear, the use of GPS and precision guided weapons and the
reorganization of rapidly deployable units into organically task organized Brigade
Tactical Groups comprised of a complete, combined arms team.\textsuperscript{126}

Summary and Analysis of Russian Hybrid Warfare in the Gray Zone: Necessary
Conditions and Alignment of Ends, Ways and Means

Conditions Required for Successful Execution of Hybrid War

While a superficial examination of the ways and means that Russia approaches
implementing its strategy of hybrid warfare in the gray zone looks like a very powerful
formula for successfully achieving Putin’s objectives, a more thorough analysis reveals
that effectively executing a hybrid warfare strategy in the gray zone requires the
presence of some rather specific conditions. Additionally, even if the necessary
conditions exist, the hybrid warfare strategy must be appropriate for the political end
state desired. Absent these conditions, the Kremlin’s use of a hybrid warfare strategy is
either unsuitable, not feasible or impossible. An examination of the necessary
conditions for Russian implementation of a hybrid warfare strategy will help put into
context the political objectives a hybrid warfare strategy is aimed at achieving as well as
the ways and means that Moscow is using to achieve these objectives.
Foremost amongst the conditions required is the fact that Moscow must be in a position to militarily and economically overmatch its opponent if necessary. Absent a clear military advantage, the Kremlin is not in an advantageous position to use threats of intervention as a coercive measure in its diplomatic and information warfare efforts. As we have seen from the examples of Russian application of its hybrid warfare strategy in Georgia, Crimea and Eastern Ukraine, the ability to use coercive diplomacy and information operations – backed up with the means to make good on its threats – is an essential element of the Russian way of hybrid warfare.

Additionally, having the capability to use conventional troops to intervene, if an escalation of force is required to achieve objectives, is a necessary condition for the Kremlin to successfully execute a hybrid warfare strategy. Closely tied to this is Moscow’s requirement to be able to sustain the insurgent groups it supports, the paramilitary units it backs and the military forces it uses to conduct unconventional warfare. Logically, then we can conclude that short interior lines of communication back to a safe haven from which to push logistical support is necessary.

In order to execute coercive diplomacy and information operations Russia requires access to mass media and the Internet in the target country. Both the Internet and a functioning mass media are essential tools for the Kremlin to deliver its information operations messages in support of insurgents and to weaken governmental control over the people. A lack of Internet, cellular and landline communications complicates or negates Russia’s cyber and information operations capabilities, thus weakening their ability to employ these critical components of their hybrid warfare strategy.
Another component of the conditions necessary are existing economic links to the target country, organization or individual that the Kremlin is attempting to coerce into action(s) favorable to Moscow’s interests. A lack of existing economic ties means that Moscow is unable to use coercive economic policies as leverage for achieving its goals.

Finally, the presence of a pro-Russian portion of the population in the target country is essential for Moscow because the Kremlin’s hybrid warfare strategy is built on its ability to use unconventional warfare, supported by information operations and cyber warfare, to support organic resistance movements in the country. Closely tied to the importance of leveraging the pro-Russian population to build a functioning shadow government and insurgent groups is the concept of legitimacy. Moscow has used its doctrine of protecting ethnic Russians from oppression as a way to build legitimacy for its actions; both inside the target country and abroad.\textsuperscript{127}

Absent these conditions, Moscow may be forced to look to other ways and means, beyond a hybrid warfare strategy in the gray zone, to accomplish its strategic objectives.

**Political Objectives and Strategic Ends**

Sun Tzu emphasized, throughout *The Art of War*, the primacy that political leaders have in determining the political end states and outcomes for war that military operations must achieve.\textsuperscript{128} Sun Tzu stressed the importance of actions taken, both by military leaders and politicians, to shape the battlefield and set conditions for success before fighting commences.\textsuperscript{129}

Russia’s use of a hybrid warfare strategy is designed to achieve Putin’s strategic political objectives and Sun Tzu would be pleased at how the Kremlin succeeded in Crimea by setting the conditions for success while aligning the ways and means needed
to achieve political objectives. The recognition of the primacy of the political objectives drives Moscow to align the necessary ways and means needed to achieve the end state desired. The Russian application of a hybrid warfare strategy uses the indirect approach while balancing the Clausewitzian trinity in recognition of the importance of linking military action to the will of the people in order to achieve political objectives. Accordingly then, we can see that there are some overarching political objectives that are common to the Russian’s use of a hybrid warfare strategy.

Foremost amongst these strategic objectives is for Putin to maintain his base of power in Russia and what has been called Moscow’s near abroad. Absent this, Putin is unable to achieve his second overarching political objective of restoring Russia to great power status. To do this, the Kremlin must accomplish the objective of limiting and / or halting the expansion of NATO into its traditional security zone while preserving Russia’s economic strength by preventing the encroachment of the EU into its sphere of economic influence; the budding Eurasian Economic Union. So, one can see that, the required combinations of political objectives and underlying conditions create a fairly narrow set of opportunities to successfully employ a hybrid warfare strategy in the gray zone.

Russia’s Use of Ways and Means for Executing a Hybrid Warfare Strategy

Diplomatic and Political

Examining the ways and means Moscow uses on the political and diplomatic fronts of its hybrid warfare strategy reveals that the Kremlin is deeply invested in the success of these aspects of its strategy. The employment of these ways and means requires significant time in order to collect the intelligence necessary to drive operations. Similarly, significant time is needed to cultivate the relationships needed so that, at the
proper time, Moscow can leverage these political relationships to achieve the effects Putin requires in order to accomplish his objectives.

The Kremlin’s techniques span the gamut from soft power to the use of subversion, violence and black propaganda. Their employment is synchronized with the use of information operations and cyber operations – as well as the use of military force, or threat to do so – as part of Moscow’s coercive hybrid strategy. In Russia’s near abroad, where pro-Western trends are counter to Putin’s political objectives, the Kremlin seeks to use coercive diplomacy and political action to create ‘managed instability.’ Moscow does this through the use of front organizations such as the Institute for Democracy and Cooperation, the Eurasian Institute, Nashi and Rusky Mir.

The Kremlin has also sought to co-opt senior political figures as a means to achieve its ends. A prominent example of this is Gerhard Schroeder, the former German Chancellor who now sits on the board of Gazprom. Additionally, the Kremlin has built relationships with a number of political parties throughout Europe who share Russian antipathy toward the EU and its agenda of expansion into Eastern Europe.

Shifting to an examination of Russia’s use of more muscular forms of political coercion we can see that subversion of sitting political figures that do not support Moscow’s agenda is an often-used way that the Kremlin chooses to use coercive politics to achieve its objectives. The means behind these subversive activities are linked to the Russian intelligence services’ penetration of target governments as well as aggressively using information operations and cyber-espionage. Leaking intercepted telephone calls and emails are tied into the information operations campaign supporting these politically subversive efforts. The synchronization of the use of all of these political
and diplomatic ways and means is critical to achieving the overarching objectives of Russia’s hybrid warfare strategy. The importance of achieving political objectives is further reflected in how the Russians approach integration of information warfare into their hybrid warfare strategy.

Information, Influence and Deception

The primacy of political objectives is reflected in Russia’s implementation of its concept of Reflexive Control in information operations. At its core, Reflexive Control is an understanding of an adversary’s thought process and way of making decisions and then tailoring information operations to induce them to make a decision they are already pre-disposed to make. Moscow uses information operations, not only to support the execution of hybrid warfare but to create opportunities for freedom of action while shaping public opinion to accept Moscow’s approach and mistrust the intentions of Western institutions and governments. To achieve this, the Kremlin has made significant, national-level, long term investments in the Internet and mass media infrastructure needed to achieve information dominance. So, having addressed how Moscow’s information operations are tied to its desired political end states, we will now examine the ways and means the Kremlin is using to implement its strategy.

The ways and means Moscow is choosing to conduct information warfare are a combination of techniques derived from the Soviet experience during the Cold War and new methods developed from Russian study of Western concepts such as net-centric warfare and effects based operations and the ways that the West has employed these concepts in contemporary operations. Information warfare doctrine is taught as an academic discipline in Russia’s Military University of the Ministry of Defense in the Military Information and Foreign Languages Department. The doctrine, titled
*petzpropaganda*, emphasizes that information operations must be multidisciplinary in their approach; using all aspects of “politics, economics, social dynamics, military, intelligence, diplomacy, psychological operations, communications, education, and cyberwarfare.”\(^{133}\) Driving the methods that Russia uses for information warfare execution is the ‘NetWar’ concept promulgated by Alexandr Dugin. In Dugin’s view, the Russians must counter Western efforts to dominate the information domain. To do this, Dugin insists that a ‘network approach’ is required to defeat the net-centric method that the West is employing. This NetWar methodology is adapted to the Russian situation, goals and values in order to be successful.\(^{134}\)

Russia’s approach to implementation of information warfare utilizes all domains to deliver its messages to achieve both political and military effects. Russia’s emphasis on the use of influence operations in the informational domain is implemented through subversion, propaganda, political protests and Internet-based Twitter campaigns and ‘trolling’ designed to shape the narrative both domestically and abroad. A central feature of Russian information warfare is propaganda whose key characteristics are the use of the language of judgement and emotion with an emphasis on complying with the Russian program while delegitimizing Moscow’s opponents. Russian propaganda has proven effective, in the short term, when directed at ethnic Russians and Russian speakers in the diaspora.\(^{135}\)

The means the Kremlin uses in delivering its information operations narrative and propaganda include the following:

- “Agents of influence including politicians, businessmen, corporations with a stake in Russia’s localization program, energy sector etc.;
- Networks of journalists who may be sectarian Communists (such as Seumas Milne), or social conservatives attracted by Putin’s superficially Christian agenda (such as Peter Hitchens);
- Sectarian left wing sites (such as Counterpunch and Global Research) which exploit a linguistic disconnect to create a sanitized Russia and a conversely stigmatized Ukraine;
- Political proxies (such as Stop the War and numerous politicians);
- PR Agencies and consultancies;
- The Troll army of paid internet commentators, all working to a script."

The content of the information operations narrative that is prevalent in Russian use of mass media is oriented along the following central themes: undermining trust in Western institutions and governments; justification of Russian actions as humanitarian in nature because Moscow is only acting to prevent abuse and atrocities directed at ethnic Russians; undermining the legitimacy of the target nation government in order to build support for a pro-Russian agenda; use of nationalist themes to build pride in Russia and support Russian return to global power status.137

Russian Unconventional Warfare

The centerpiece of the way that Russia has chosen to implement the military component of its hybrid warfare strategy in the gray zone is unconventional warfare. To be clear, there is a conventional military element to Moscow’s hybrid warfare strategy, but is principally used as a deterrent to outside involvement and as a fail-safe option to ensure success in the event that other ways and means have failed to achieve political
objectives. The means associated with the unconventional warfare component of Russia’s hybrid warfare strategy is the use of SPETSNAZ and intelligence services to link up with indigenous resistance forces to turn them into a viable insurgent organization; complete with a political wing. The Kremlin’s approach to unconventional warfare is to use all elements of national power to achieve success by using a whole of government approach. Our previous treatment of the diplomatic / political and informational aspects of the Russian approach to hybrid warfare are evidence of the interagency nature of Russian unconventional warfare. Noted expert in unconventional warfare and special operations, COL (R) David Maxwell argues that, in the Ukraine, “what we are really seeing is unconventional warfare employed in support of political warfare. George Kennan described political warfare as all means at a nation’s command, short of war, to achieve its national objectives. The Russians have not gone to war but they are clearly employing all elements of national power to achieve national objectives.”¹³⁸ There is great merit to Maxwell’s observations and his characterization is more than an academic argument about what label to put on Russian actions. This description of the Russian approach to hybrid warfare / unconventional warfare / political warfare is central to understanding the Russian strategy. Going forward, as Sun Tzu cautioned us to do, our strategy must be designed to counter our adversaries’ strategy. As General Votel identified, the gray zone is a seam where the Russians are engaging its adversaries using hybrid warfare to avoid triggering Western intervention. General Votel warned that our capacity to respond to hybrid threats in the gray zone is a “critical policy gap.”
In Robert R. Leonhard and Stephen P. Phillips monograph, ““Little Green Men”: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014,” they outline the key principles of Russian unconventional warfare as follows:

- **“Primacy of nonmilitary factors: politics, diplomacy, economics, finance, information, and intelligence”**
- **Primacy of the information domain: use of cyberwarfare, propaganda, and deception, especially toward the Russian-speaking populace**
- **Persistent denial of Russian operations**
- **Use of unidentified local and Russian agents**
- **Use of intimidation, bribery, assassination, and agitation**
- **Start of military activity without war declaration; actions appear to be spontaneous actions of local troops/militias**
- **Use of armed civilian proxies, self-defense militias, and imported paramilitary units (e.g., Cossacks, Vostok Battalion) instead of, or in advance of, regular troops**
- **Asymmetric, nonlinear actions**

There are a number of strategic advantages to utilizing an unconventional warfare component to a hybrid warfare strategy. Included are: improved understanding and shaping of the environment, cost-imposing strategies, sustainable solutions, managed escalation and credibility risk. Applying Principal-Agent Theory concepts to devising a Counter-Unconventional Warfare strategy for responding to the Russians’ use of Unconventional Warfare in their hybrid warfare strategy is explored in the recommendations section of this paper.
Economic Leverage

A key component of Moscow’s hybrid warfare strategy is the use of coercive economic policies. Russia’s economic warfare is closely linked to its informational, political and diplomatic efforts that are among the non-military pillars of its strategy. The economic levers the Kremlin has pulled to the greatest effect are food sanctions and energy supply embargoes. Examples of these include the 2006 Russian ban on the import of Georgian wines, agricultural goods and mineral water; or the ban on importing Belarussian milk products or Ukrainian chocolate into Russia. There are numerous other similar examples of the coercive use of economic levers to achieve Russian political objectives. Russia has also used its considerable energy resources as a means of economic coercion. Gazprom is well known for supporting the Kremlin’s political objectives abroad by calibrating energy prices or the flow of energy resources as either an incentive or punishment for compliance with Russian political objectives. Russia’s hegemony as an energy supplier in Europe and Moscow’s near abroad, combined with the state control the Kremlin exerts over the energy industry in Russia, empowers Putin to weaponize Russian foreign / energy policy. It remains unclear whether or not Russia’s coercive energy policies are achieving the political results Putin seeks, but it is clear that they are an added dimension to the hybrid strategy that Russia is employing.141

Exploitable Vulnerabilities in Russian Hybrid Warfare Strategy Application

Diplomatic and Political

The principal vulnerability associated with the Kremlin’s use of coercive political and diplomatic activity is time. It is time consuming and resource intensive to mount the necessary intelligence collection efforts that enable successfully targeting political
leaders. Further, it is time consuming to develop the necessary relationships with targeted personalities with the requisite power, position and influence so that, when the time is right, Moscow can exploit these relationships to achieve its political objectives.

The intelligence operations themselves, whether they are human intelligence operations, signals intelligence or cyber operations also represent vulnerabilities. The possibility of compromising a human intelligence operation or having an agent become a double agent is an ever-present risk. Signals intelligence and cyber-espionage are vulnerable to deception operations and any cyber capability the Kremlin is using that is connected to the Internet is vulnerable to cyber-attack.

**Information, Influence and Deception**

Despite the effectiveness of propaganda on a relatively receptive, pro-Russian population, Moscow has been forced to escalate the situation by using military force to ensure compliance with the Kremlin’s programs. The impact of Russian propaganda on Western audiences has been less effective in altering opinions about the legitimacy of Russian actions. The vulnerability resident in this approach is that “disinformation campaigns erode over time” and thus undermine the legitimacy of Russian actions.\textsuperscript{142} Additionally, the Kremlin’s reliance on proxies, such as the Russian Business Network, or the ‘troll army,’ poses vulnerabilities to both Russian information and cyber operations.\textsuperscript{143}

A key vulnerability is the assumption that the proxies’ interests are aligned with Moscow’s, thus making them reliable partners. Second, the cyber resources that Russia relies on to disseminate its messages and influence various targets are vulnerable to deception, cyber-espionage and / or cyber-attack.
Russian Unconventional Warfare

As evidenced by Russian hybrid warfare operations in Crimea and Eastern Ukraine, a key military component of the Kremlin’s strategy is the employment of unconventional warfare. This carries some attendant risks and limitations due to the reliance on the use of proxy forces, paramilitary units and other partners. Among these are: divergent partner objectives, ineffective partner capability, unacceptable partner behavior, disclosure and policy fratricide. 144 The risks and limitations of employing unconventional warfare as the key military component of a hybrid warfare strategy pose potential vulnerabilities that our own strategy may be able to exploit.

Economic Warfare

A vulnerability associated with the coercive economic policies that support its hybrid warfare strategy are the possibility that these economic levers may negatively impact the population, thus adversely effecting public opinion about Putin and his policies. While these economic sanctions may work in the short term, countries may choose to find alternative markets to buy from and / or sell to. Furthermore, economic sanctions have the potential to negatively impact the Russian economy overall and therefore they could adversely affect domestic public opinion about Putin’s policies. More likely is the fact that Moscow’s use of economic levers could negatively affect the bottom lines for powerful Russian oligarchs upon which Putin relies for his power base in Russia.

Legitimacy

The Russian way of hybrid warfare is characterized by a “lack of moral or ethical restraint displayed in the execution of adversary operations.” 145 Colonel Robert Hamilton, a Eurasia Foreign Area Officer at the US Army War College, characterizes
this failure to ground actions in an “instrumental use of ideas.” He asserts that the incongruity between what Russia’s actions are, and the morals and values espoused in the Russian’s information operations narratives, undermines Moscow’s legitimacy.\textsuperscript{146} Thus, it is assessed that the most significant vulnerability associated with the ways and means Russia employs in its hybrid warfare strategy is legitimacy. Virtually all of the other ways and means Moscow uses (unconventional warfare, paramilitary forces, proxy forces, information operations, economic warfare, etc.) have significant potential to undermine the legitimacy of the Kremlin’s actions, policies and ideology. As an example, the Kremlin began to lose control over some of its proxy forces the longer that the campaign in Eastern Ukraine dragged on. Additionally, increasing Russian involvement undermined initial Russian claims that it wasn’t involved in the conflict.\textsuperscript{147} Similarly, the Kremlin’s information operations capability, while substantial, is not immune to making mistakes nor is it bashful about telling outright lies. Examples of this in Eastern Ukraine include the use of imagery from Kosovo to depict so-called Russian refugees fleeing Ukraine or using Photoshop to depict Donetsk in flames.\textsuperscript{148} A further illustration of the legitimacy vulnerability embedded in the Russian approach to hybrid warfare is the fact that, despite a robust information operations capability, the Kremlin is vulnerable to grass-roots organizations that mobilize to counter the narrative coming out of Putin’s propaganda machines. The activists in Ukraine behind Euromaidan.com and Stopfake.org are but a couple of examples.\textsuperscript{149} Critical to our ability to attack the legitimacy of Putin’s actions in a hybrid war are our own information operations and cyber capabilities. In order to be effective, we must make significant organizational
changes as well as decentralize our efforts at undermining the perception of Russian legitimacy through a concerted information operations campaign.

**Costs – Political, Economic and Human**

There are other inherent vulnerabilities embedded in the use of a hybrid warfare strategy in the gray zone. Because the nature of a hybrid warfare strategy is to incrementally use increasingly muscular forms of coercion to achieve objectives, the hybrid strategy itself may lead to failing to accomplish political objectives. The ‘frozen conflict’ that is developing in Eastern Ukraine is an example of this. Finally, the Kremlin’s use of a hybrid warfare strategy in the gray zone is intended to achieve political objectives without crossing the threshold that incites an international response with the potential to limit Moscow’s ability to accomplish its objectives. This risk versus gain calculus is based on assumptions about both the West’s and international organizations’ proclivity for a response to Russian actions. However, if the Kremlin’s actions violate important norms, values, customs, international agreements or laws then the risk of outside involvement – and thus obstacles to accomplishing objectives – may arise.  

**Time**

Employment of a hybrid warfare strategy in the gray zone has the potential to become a long term commitment for the Kremlin. The Russian-backed frozen conflicts in Transnistria, South Ossetia, Abkhazia and Eastern Ukraine are examples of this potentiality becoming a reality. In these frozen conflicts, absent a peace treaty or other political agreement to settle the conflicts, hostilities can resume at any time. This situation of political instability and lack of security potentially creates political problems for Putin and certainly saps Moscow of resources. The Kremlin’s approach is potentially
costly in terms of political capital, men, equipment, supplies, money and lives. The increasing costs of military adventurism abroad have the potential to undermine public support for Putin’s regime and his policies. As time wears on, the incongruities between the Kremlin’s information operations narratives and what is actually occurring on the ground have the potential to come to light, thus undermining the legitimacy of Putin’s actions, policies and validity as a leader both at home and internationally.

**Recommendations**

**Employing a Political Warfare Strategy to Counter Russia’s Hybrid Warfare Strategy**

As Political Warfare is defined and described in the United States Army Special Operations Command white paper entitled *SOF Support to Political Warfare*, both Sun Tzu and Clausewitz would recognize the central tenets of their theories on war.\(^{151}\)

As Sun Tzu directed us, employing Political Warfare against Russia’s hybrid warfare strategy must include an intense multi-lateral, interagency intelligence effort to penetrate into the leadership, underground and auxiliary of the resistance movements the Kremlin supports to better understand their capabilities and intentions. This would enable us to direct efforts using denial, deception, propaganda and diplomacy in order to weaken the attractiveness of what Russia offers and break the relationships that Moscow is building with budding insurgencies. This satisfies Sun Tzu’s imperatives regarding intelligence, diplomacy and deception and addresses the people side of Clausewitz’ trinity by developing an understanding of the fears and motivations of the local population while shaping their attitudes toward the government.

Political Warfare attempts to balance the military aspect of Clausewitz’ trinity by employing US Special Operations Forces to conduct Security Sector Assistance (SSA), Information and Influence Activities (IIA), Unconventional Warfare (UW) and Counter-
unconventional warfare (C-UW) to separate the people from the insurgents and connecting the government to the people.\textsuperscript{152} These Special Operations missions are ways in which the military aspect of national power can be employed in a Political Warfare strategy to address both the army and people elements of the trinity by building partner capacity and the development of necessary underground and auxiliary elements critical to the success of any UW or C-UW campaign.\textsuperscript{153}

A Political Warfare strategy countering the Kremlin’s approach to hybrid warfare would satisfy both Sun Tzu and Clausewitz because it uses the indirect approach to attack both the enemy’s strategy and its center of gravity by shaping the enemy and synchronizing the employment of all elements of national power before hostilities. A Political Warfare strategy, supported by IIA, SSA, UW and /or C-UW, balances Clausewitz’ trinity and adheres to Sun Tzu’s teachings by employing moral authority to connect the people to their government while separating the insurgents from the people. Political Warfare seeks the path to victory with the least bloodshed, least risk and least amount of resources while attempting to achieve the acme of skill described by Sun Tzu as subduing the enemy without fighting.

The origins of Political Warfare emanate from the Cold War in a 1948 US State Department policy proposal drafted by George Kennan, in which he advocated for the creation of an interagency organization to globally counter the Soviet Union and the communist ideology. The outgrowth of this policy proposal was NSC-68, the National Security Council directive for containment of the Soviet Union which became the guiding grand strategy of the Cold War.\textsuperscript{154} In the recent past, noteworthy national security analysts such as Frank Hoffman, Dr. Michael Noonan and Max Boot have advocated for
adoption of a Political Warfare strategic approach to dealing with both terrorist threats and a resurgent Russia.\textsuperscript{155}

The concepts behind the Political Warfare strategic construct are for the US government to seek a comprehensive understanding about what problem we are collectively trying to solve and defining what our national interests and political objectives are. Once there is agreement on the nature of the problem and our desired end state, the ways and means – drawn from all elements of national power - necessary to achieve these ends are aligned to achieve the objective and “win the peace.” Unified action with a whole-of-government approach is essential to success.\textsuperscript{156}

The risks associated with adopting a Political Warfare strategy are very low. The Political Warfare approach is feasible because many of the elements of what is envisioned as part of this strategy are already being conducted by various interagency organizations. Adoption of a Political Warfare strategy is acceptable because it places emphasis on the diplomatic, informational and economic aspects of national power while limiting US direct involvement in other countries’ internal security issues. Political Warfare is suitable because it integrates interagency efforts, enables adaptability and synchronizes activities; thus increasing the likelihood of achieving US political objectives.

Organizational

Given the nature of the hybrid adversaries we face that choose to operate in the gray zone, we must adapt our structures to ensure we are organized, equipped and trained so that we are ready to win at the strategic level. As we have seen through our analysis of the Russian model for employing a hybrid strategy, fighting in a conventional warfare sense, is not the main feature of hybrid warfare yet Landpower is an essential
element of the military component of Moscow’s strategy. Thus, the recommendations made below focus on our ability to work in a unified fashion as an Interagency team at the strategic level, rebuilding our information operations enterprise across the Interagency and creating the needed structures in the US Army to employ Strategic Landpower by performing Irregular Warfare and Security Sector Assistance.

Joint Interagency Coordination Group (JIACG)

Employing a Political Warfare strategy to counter Russia’s efforts to achieve its strategic objectives must include joint, interagency and inter-governmental and multinational intelligence effort to penetrate into the leadership, underground and auxiliary of the resistance forces and criminal networks Russia leverages. This would enable the direction of interagency efforts using denial, deception, propaganda, economic leverage and diplomacy in order to weaken the popular support for resistance forces and disrupt Russia’s efforts to develop proxy forces to undermine the other sovereign nations.

Adoption of a Political Warfare strategy to counter Russian hybrid warfare orients the disparate organization of the US government on a common, unifying objective with the overarching goal of coordinating and synchronizing the long term application of all elements of national power.

To accomplish these objectives, the President must establish a central coordinating body to implement the Political Warfare strategy. The model for this Joint, Interagency Coordination Group (JIACG) is the National Counter-Terrorism Center which was formed in the wake 9/11 to coordinate interagency operations to counter terrorist organizations. The JIACG, staffed with Department of Defense personnel and representatives of other Departments and Agencies, collaborates, plans, coordinates and synchronizes the interagency efforts to achieve US strategic objectives. The proper
implementation of a Political Warfare strategy requires agility, adaptability, unity of effort amongst the interagency and close synchronization of all elements of national power. Because no such interagency organization exists, a central coordinating and synchronizing element must be created. Additionally, organizational changes are required to enable both our Cyber and information operations capabilities, as well as to the US Army Generating Force and Operating force to properly support a Political Warfare strategy.

The JIACG construct provides for more effective planning, coordination, and integration of partner efforts to achieve objectives. Additionally, it is intended to serve as an interagency enabling capability for the combatant commands, the joint staff and US Embassies abroad through its ability to leverage the expertise and capabilities of each participating organization through a reach back capability to Departments and Agencies. The author recommends using the State Department’s Center for Strategic Counterterrorism Communications as the nucleus of the Political Warfare JIACG. This entity already exists and its purpose is to coordinate, orient, and inform government-wide foreign communications activities targeted against terrorism and violent extremism.

Further, the President must appoint a Political Warfare coordinator to the National Security Staff. This would ensure that the JIACG and the individual responsible for coordinating and overseeing the implementation of a Political Warfare strategy has a seat at the table on the National Security Council and the requisite support of the President needed.
Information Operations

Whether we are countering the radical Salafist ideologies of Al Qaida or the Islamic State, or the neoconservative political agenda of Russia under the Putin regime, the United States is engaged in a war of ideas about the relationship between the state, religion and its people and the fundamental ways in which we govern ourselves and manage our economies. The US government must commit the appropriate resources to effectively engage in the information domain and win the war of ideas. The combined ideological struggles we face today are no less significant than those we faced during the Cold War. Thus, our level of effort, in people, time, money and intellectual capital must, for the State Department, the CIA and the Department of Defense, be commensurate with our level of investment during the Cold War. Unfortunately, we are significantly under-invested in this critical area.

Department of Defense spending on information operations has not met the demands required from the War on Terror; much less the added requirements presented by the need to counter Russian information operations employed as part of their hybrid warfare strategy. The difficulty in assessing the effectiveness of Defense-related information operations programs has been hampered by cutbacks in assessment programs. One example is that, despite spending more than $250 million per year on information operations and information-related capabilities at the strategic and operational levels the Defense Department struggles to assess the effectiveness of its programs and to explain the efficacy of them to Congress. Lacking clear effectiveness assessments has caused activists, DoD decision makers and the US Congress to call into question the efficacy of the Defense Department’s information operations programs. One example of this was the refusal by Congress to fund USSOCOM’s
2014 budget request for its Global Assessment Program for which SOCOM intended to assess the effectiveness of its information operations efforts in the global war on terrorism. Another such blow to the Defense Department’s information operations programs arose shortly after 9/11 over Congressional concern about the activities of the Department’s Office of Strategic Influence. This Congressional concern caused Donald Rumsfeld to close the Office of Strategic Influence in 2002. Similarly, State Department-related information operations programs have suffered a lack of resources sufficient to meet the requirements to win the war of ideas in the information age.

On 26 January 2016 former Secretary of Defense, Robert Gates, provided remarks in a question and answer session at the Council on Foreign Relations’ Paul C. Warnke Lecture on International Security. During this session, Gates provided journalist Tom Brokaw his thoughts on the effectiveness of the United States Information Agency during the Cold War and his opinions on the consequences of our weakened strategic communications. He stated:

...really since the end of the Cold War, is that we have also, for many years, starved the civilian talent pool in the government, and particularly those involved in diplomacy, in AID, and in strategic communications. So you had this Wurlitzer of strategic communications that was a big part, I think, of success in the Cold War. That's all been basically dismantled. And that whole big operation now sits in a small corner of the State Department. Those are the people also that you need to rely on in terms of how do you come up with a digital response to ISIS? How do you counter either directly or through other organizations the messaging that ISIS is sending to the West, to Europe and to the United States, that's radicalizing some of these people and so on? And we've basically disarmed that part of the national security toolkit.

An example of how the United States Information Agency successfully organized during the Cold War to attack Soviet propaganda was how the Reagan administration created the Interagency Active Measures Working Group in 1980. This organization was
designed to measure the effectiveness of our information operations which is precisely what SOCOM unsuccessfully attempted to contract for their Global Assessment Program. ¹⁶⁴

What Secretary Gates referred to when he spoke of the US having dismantled its Cold War information operations capability was the fact that beginning in 1993, President Bill Clinton disbanded USIA. Formed in 1953 and run by Edward R. Murrow, USIA had been a twelve thousand employee organization. Subsequent to President Clinton closing USIA it was transformed in 1999 by reorganizing its broadcast operations under the Broadcasting Board of Governors, while its other mass media functions reorganized under a new State Department Under-Secretary for Public Diplomacy and Public Affairs. However, cuts to our information operations capability continue. A little over a year ago, the Counter-Disinformation Team was created by the State Department within their Bureau of International Information Programs. This small organization was intended to counter Russian disinformation, however the State Department subsequently dismantled the Counter-Disinformation Team.¹⁶⁵

Currently, the combined staffing of the Under Secretary for Public Diplomacy and Public Affairs organizations is down to approximately 3,500 employees with a combined budget of $750 million with no apparent White House or Congressional support for expansion of these efforts.¹⁶⁶ While the examples Secretary Gates, et. al. have provided regarding a lack of capability to counter ISIS information operations, the implication is clear that we are equally disadvantaged at countering the Russian information operations supporting its hybrid warfare strategy.
Cyber Capability – Organization and Authorities

US Cyber Command (USCYBERCOM) has existed for over six years. On June 23, 2009, the Secretary of Defense directed the Commander of US Strategic Command (USSTRATCOM) to establish USCYBERCOM at Fort Meade, Maryland as sub-unified command of USSTRATCOM. Yet, despite the fact that USCYBERCOM achieved ‘Full Operational Capability (FOC)’ in October 2010, the vast majority of its capacity lies embedded within the National Security Agency (NSA) and USCYBERCOM lacks the offensive authorities to properly carry out its mission. Additionally, as it is currently organized, USCYBERCOM lacks the service-like capabilities needed for manning, training, equipping and planning, programming and budgeting. While Congress, the Defense Department and various Federal Agencies have been debating which agency or which Congressional committee has ownership of our Cyber programs our adversaries are aggressively conducting pre-operational cyber reconnaissance on our networks in preparation for an attack that could cripple our critical infrastructure or government functions. Virtually unchecked, cyber-crime has eclipsed the costs associated with the war on drugs and has the potential for significantly impacting the US economy.

Thus, the author recommends that the Congress and the Secretary of Defense immediately designate USCYBERCOM as a Unified Command with ‘Special Operations Command-like authorities’ that has Combatant Command authority (COCOM) over all cyber forces in the US military. Additionally, it will enable the USCYBERCOM commander to properly man, train and equip cyber forces and to direct operations approved by the President or the Secretary of Defense. Further, to enable this construct at the theater-level, the author recommends that USCYBERCOM
establish Theater Cyber Operational Commands that are COCOM to USCYBERCOM and under the Operational Control of the Geographic Combatant Commands. This will bring USCYBERCOM task organization into alignment with Joint Doctrine and US law.  

Additionally, it is strongly recommended that Congress and the President pass the Cybersecurity Information Sharing Act of 2015 and amend the Foreign Intelligence Surveillance Act law to better position the NSA to support domestic law enforcement of cyber-crime and specifically authorize the employment of USCYBERCOM to disrupt cyber-crime at the request of the Department of Justice or Department of Homeland Security; regardless of nationality or location of the actor. Lastly, it is essential that the President and the Secretary of Defense delegate authorities for USCYBERCOM to conduct offensive cyber operations to disrupt imminent cyber-attacks in certain circumstances short of what would constitute ‘war’ under the Department of Defense’s Law of War Manual and international law.

Unchecked, our adversaries operating aggressively in the cyber domain have the capability to conduct cyber-attacks that threaten our national security. Absent improved intelligence community support to law enforcement and a pre-emptive attack strategy to deter cyber-attacks and cyber-crime, the US will continue to fall short of counter our adversaries employing a hybrid strategy in cyberspace. The costs of cyber-crime, with its negative impact on our economy, will continue its exponential growth curve and is expected to reach $2 trillion globally by 2019.

Advise and Assist Brigades

The US Army must create an ‘Advisory Corps’ that is organized, manned, equipped and trained specifically to conduct Irregular Warfare. In January 2016, the
Army Chief of Staff, Gen. Mark Milley, said he is considering the development of Advise-and-Assist Brigades. Ostensibly, these units would consist of the leadership structure of a US Army Brigade Combat Team (BCT). When called upon to deploy for a mission to provide security assistance training to a foreign military, the assigned NCOs and Officers would have the requisite structure, training and experience to conduct Irregular Warfare by serving as trainers and advisors to host nation security forces. Alternatively, when additional BCTs were needed for war, these Advise-and-Assist Brigades would have the leadership structure so that they could rapidly be fleshed out with junior enlisted Soldiers thus quickly building readiness for decisive action operations. Currently, the US Army is using the leadership structure from Brigade Combat Teams to create advise-and-assist brigades for deployment to either Iraq or Afghanistan. The net result of this is that core leadership structure of Brigade Combat Teams are deployed; leaving behind a substantial part of the BCT that has been reduced to a significantly degraded state of readiness due to a lack of experienced leadership.

The creation of dedicated advisory units is not a new idea, but it is long overdue and General Milley should get the full support of the Department of Defense and Congress for this initiative. As early as 1998, professor Don Snider called for the creation of a similar capability in his June 1998 article in Army magazine entitled “Let the Debate Begin: It’s Time For An Army Constabulary Force.” In 2007, John Nagl, amongst other military leaders and civilian military analysts, reignited the debate and called for the creation of a “permanent standing Advisor Corps of 20,000 Combat
Advisors — men and women organized, equipped, educated, and trained to develop host nation security forces abroad."\textsuperscript{183}

Regardless of whether the 20,000 number that Nagl calls for is what is actually needed today, the fact remains that the requirement to assist host nation security forces’ development of capacity by conducting Irregular Warfare is a need that is not going away and should be considered a core competency of the US Army.\textsuperscript{184} Creating permanent units dedicated to conducting this mission would be infinitely better than the haphazard way individual augmentees manned the Military Assistance and Advisory Command-Vietnam; or the way the US Army organized, trained and equipped and deployed its Transition Teams, comprised of individual augmentees, to Iraq and Afghanistan.

The Army Irregular Warfare Center

Given that the US Army must establish a core capability to conduct Irregular Warfare by creating Advise and Assist Brigades, the US Army must consider reactivating the Army Irregular Warfare Center (AIWC) and continue the mission it was assigned at Fort Leavenworth, Kansas beginning in 2006. While the AIWC ran the US Army’s effort to train individuals and units for deployment to conduct counter-insurgency missions and other Irregular Warfare activities, it prepared more than forty Brigades, as well as Corps and Division headquarters for Counter-Insurgency (COIN) missions in Afghanistan and Iraq. In addition to training unit leadership, the AIWC was “the driving force that led to the analysis, development and integration of irregular warfare-related concepts, doctrine, training, leadership and education, ensuring the lessons we’ve learned permeate across the Army now through 2025 and beyond” according to MG Thomas S. James, the Director of the Mission Command Center of Excellence for the
US Army Training and Doctrine Command. As such, the AIWC’s mission included doctrine development, coordinating doctrine integration with the Joint Staff and other services, ensuring Irregular Warfare doctrine and best practices were promulgated across all areas of force structure and resourcing, integrating Irregular Warfare and COIN doctrine into training and education and conducting outreach activities to the COIN community of interest.\(^{185}\)

The AIWC performed essential functions for the generating force ensuring the Irregular Warfare and COIN were part of the US Army training base, doctrine, organization and resourcing. Given the very limited integration of Irregular Warfare theory, doctrine and history into the professional military education of non-Special Operations military occupational specialty Officers, Warrant Officers and Non-Commissioned Officers, not only should the AIWC be reactivated, but the size and scope of its impact on professional military education across the service should reflect the fact that Irregular Warfare is a core competency required of the US Army.

Tigerland

Concurrent with the creation of Advise and Assist Brigades and the reactivation of the AIWC, the US Army should reactivate the 162\(^{nd}\) Brigade and continue the mission it was assigned at Fort Polk, LA beginning in 2009. The Army decided to inactivate the 162\(^{nd}\) Brigade in 2014, but it is clear from the current state of affairs, both in the Middle East, and in Europe, that there is a significant and enduring requirement for the US Army’s ability to conduct Irregular Warfare.\(^{186}\) The 162\(^{nd}\) Brigade was an 800-soldier unit and it ran a fully functional school at its immersive training facility, Tigerland, at Fort Polk, for both individual augmentees and units assigned to Irregular Warfare missions. As such, the 162\(^{nd}\) Brigade developed a cadre of experienced professionals with
experience conducting similar missions and it was able to leverage the expertise and training venues offered by the Joint Readiness Training Center.

**Counter-Unconventional Warfare**

The key military component of the ways and means that the Kremlin is implementing its hybrid warfare strategy is by conducting UW. Thus, the capability and willingness to conduct C-UW to address the military component of the Russian strategy is required. Retired Special Forces COL David Maxwell describes C-UW as “operations and activities conducted by the U.S. Government and supported by SOF [special operations forces] against an adversarial state or non-state sponsor of unconventional warfare.” These SOF-supported government initiatives can “decrease the sponsor’s capacity to employ unconventional warfare to achieve strategic aims.” As C-UW campaigns are likely “protracted and psychological-centric in nature” they should “comprehensively employ political, economic, military, and psychological pressure” in order to degrade both the will and capability of an adversary to sponsor unconventional warfare. The chief advantage of C-UW is its focus on decreasing an adversary’s ability and will to persist in hybrid warfare or to support elements of a resistance or insurgency.187

An all-inclusive C-UW campaign could include components of these Irregular Warfare activities and operations: counterinsurgency, foreign internal defense unconventional warfare, stability operations and counterterrorism. Each can be conducted alone or simultaneously with other operations and a C-UW campaign may occur in one country or in multiple states. Political considerations and host nation considerations will have a significant influence on the type and scale of operations. The size and scope of each activity is adjustable based on the goals and domestic
considerations of host nation partners. C-UW may include conventional forces or circumstances such as the political sensitivity of operations or the permissiveness of the operational environment may dictate that SOF has an exclusive role in C-UW.\textsuperscript{188}

Special Warfare campaigns involve more than just Special Operations Forces. They can include the use of General Purpose Forces and are inherently interagency in nature and require a whole-of-government approach to succeed. They involve the comprehensive orchestration of U.S. government capabilities to advance policy objectives. Special Warfare campaigns have six characteristics: 1) Their objective is either to stabilize or destabilize a targeted country or entity. Unconventional Warfare is intended to destabilize while Foreign Internal Defense is designed to build a host nation governments capability to provide for its own security through the development of an Internal Defense and Development (IDAD) program; 2) Typically, the main effort is comprised of local partners; 3) They are small-footprint operations with minimal (or no) US military in country; 4) They are long duration missions often conducted over many months or years; 5) They are interagency in nature and often the Department of Defense is not the lead Federal Agency; and 6) They activate, neutralize, or assimilate individuals or units from the strategic down to the tactical levels.\textsuperscript{189}

Russian support to regional insurgences through UW is part of its hybrid warfare strategy. Therefore the US military must be prepared to conduct C-UW as part of a joint, interagency, inter-governmental and multinational effort. This provides our political leadership the full range of options to address our adversaries’ employment of a hybrid warfare strategy that contains an Unconventional Warfare Component.\textsuperscript{190} Counter-
Unconventional Warfare carries with it a number of potential strategic advantages as well as strategic risks.

A strategic advantage of conducting Special Warfare to counter Russian UW is that it can improve U.S. enhanced understanding of the local situation and the viability of potential partners before we are committed to a plan of action. Additionally, because of the small-footprint nature of Special Warfare, this option is relatively cost-effective compared to the potential costs the US could impose on its adversaries. Because of its small-footprint, Special Warfare is more sustainable, both monetarily and politically. Adoption of the use of Special Warfare ways and means offers policymakers options for escalation as the situation dictates. \(^{191}\)

Alternatively, there are inherent limitations and strategic risks associated with Special Warfare. Foremost amongst these is the possibility that a local partner’s interests do not align with US interests and even if our local partner’s interests align with ours, their capability or capacity may not be sufficient to achieve political objectives in the time required. Working with local partners poses risks if that partner does not adhere to our values and norms. As a consequence, criminal behavior or human rights violations undermine our legitimacy. Poorly coordinated Special Warfare campaigns run the risk of policy fratricide; particularly if they are not interagency in nature and fail to utilize a whole-of-government approach. Lastly, the proliferation of technology and the increasing velocity of information makes keeping Special Warfare activities low-profile or clandestine inherently difficult; particularly over time. \(^{192}\)

Applying Principle-Agent Theory in Counter-Unconventional Warfare

Examining the relationships between Moscow and its surrogates, as the Kremlin pursues its hybrid warfare strategies, has great potential for identifying opportunities to
vulnerabilities. Identification of fissures in these relationships, or lack of alignment of interests, are examples of exploitable vulnerabilities. Principle-Agent theory helps us understand these relationships, spot the potential for exploitation and then engineer solutions for exploiting the vulnerabilities uncovered.

In applying Principle-Agent theory to C-UW, analyzing the alignment of interests, information asymmetry and preference for risk between a principle (sponsor) and its agent (proxy) may potentially reveal exploitable vulnerabilities that exist. The costs for the principle are directly related to the incentives provided to the agent. The principle can reward an agent based on outcomes provided or behaviors provided; or a combination of the two. Rewards in an outcome-based compensation system are not tied to level of effort, but to an ability to achieve a designated end state. Rewards in a behavior-based rewards system are linked to a specified level of effort regardless of if, or not, that level of effort achieved objectives. Risks for the principle in a behavior-based reward system are greater due to the uncertainty of the outcome and the increased cost of monitoring behavior and compliance. Problems that arise related to the effectiveness of an agent in a behavior-based system are usually addressed by changing compensation levels and adjusting information flow to reduce risk and uncertainty while ensuring interests remain aligned. Each of these aspects of the principle-agent relationship (alignment of interests, shared risk, information flow and compensation) are elements that can be exploited as part of C-UW campaign.

Using the principal-agent theory in a C-UW campaign requires convincing any party to the principle-agent agreement that the risk is not worth the cost or that there is a significant divergence of interests such that, whatever compensation is being offered
to the agent is not worth the level of effort or risk required by either party.\textsuperscript{194}

Identification of who the players are, their interests, objectives and types of compensation in a principle-agent relationship in an UW campaign conducted by the Russians offers insights into potential vulnerabilities that are ripe for exploitation by information operations, double agents, black propaganda or deception operations.

Applying the principle-agent theory to analyzing a C-UW campaign is best achieved by using all elements of national power to convince both principle and agent – the two primary audiences – that whatever they are getting out of the principle-agent relationship isn’t worth it. This can range from specifically focusing on the near-term compensation aspect of the principle-agent relationship or to attacking the parties’ expectations of the value of future compensation. The latter is tied into the nature of the political relationship(s) and expected benefit(s) from promised political relationships or outcomes. As an example, if an agent can be convinced that his political objectives will not be realized in the end, then his willingness to act as an agent for a principal will likely be diminished. Similarly, if a principle can be convinced that the agents he is employing will not remain politically aligned in the future then he may be inclined to discontinue support to the agent.\textsuperscript{195}

\textbf{Time, Patience and Will}

To win at the strategic level when facing adversaries employing a hybrid warfare strategy in the gray zone we must first define what our national interests and thus, what our political objectives are. Concurrent with this is determining what success looks like and some criteria for measuring success. Given the political nature of hybrid warfare in the gray zone, the first step to countering it requires redefining what winning looks like. In the context of hybrid warfare, winning may not look at all like winning in a
conventional war scenario. Additionally, the political nature of hybrid warfare mitigates toward a potentially long time horizon to achieve success. Consider, as an example, how long it took for the US grand strategy of containment of the Soviet Union and its communist ideology to pay off. Stated simply, we must adjust our expectations and not demand immediate results from our efforts. Additionally, we must be agile and adaptable enough to re-examine our assumptions and adjust our definition of success to meet shifting political realities.

Western governments employing strategies to counter hybrid threat would be prudent to allow time to work in our favor. There are several reasons for this that are tied to the inherent vulnerabilities associated with our adversaries’ use of a hybrid warfare strategy. Foremost, Putin’s coercive energy policies and military adventurism in Russia’s near abroad, while producing short-term domestic political gains, are potentially very detrimental to Moscow’s long-term economic interests and international political standing as a responsible, reliable and trustworthy world power. A foreign policy based heavily on simply countering the West is not a prescription for long term economic and political success. Thus, the US should use the strength of its economy and the values that underpin our democratic and capitalistic way of life to erode Russia’s appeal. However, while Russian neoconservative policies and values have little appeal abroad these conservative values have great appeal in Russia and Eastern Europe. We must be very judicious in our pursuit of information operations and related democracy and economic reform initiatives. If these initiatives include pushing our liberal social values on societies whose conservative values and norms may find Western social mores (gay marriage, equality for women, etc.) abhorrent, then this may
prove very counterproductive. Returning to Russian vulnerabilities, aside from a petroleum-based export economy that is subject to market volatility Russia has no long-term economic plan. Therefore, the Kremlin is forced to rely on manufactured external threats to focus national attention in order to build domestic consensus for Putin’s policies.

In any long-run competition, Russia will be at a profound disadvantage to the U.S. unless the U.S. imposes costs on itself, imposes them inefficiently on Russia, or simply fails to respond. In short, this is not a policy of containment, but of constrainment. The U.S. approach should be to defend its allies and interests and to respond to destructive Russian actions with policies that raise Russian costs going forward and thus incentivize Russia to choose other, more desirable actions.197

Intellectual Preparation

Dr. Frank Hoffman asserts that “gray zone conflicts are aimed at a gap in our intellectual preparation of the battlespace and a seam in how we think about conflict.” Hoffman highlights that, unlike military organizations in Western democratic countries, other states function more autocratically and do not legalistically define peace and conflict in the same binary nature that we do. For Hoffman, this narrow categorization of the conditions of peace and war is outmoded and that we must “expand our definition and concepts beyond its history, cultural biases, and organizational preferences.” This would enable us to adapt to the forms of warfare that our adversaries are choosing.198 Steven Orkin advances the idea that our thinking, in International Relations theory, about the fundamental nature of warfare hamstrings our ability to properly analyze our adversaries’ actions and see them for what they are. He asserts that warfare in International Relations theory, “accepts, reinforces, and operates within the binary divide between war and peace.” Orkin opines that this is important because current
International Relations theory provides the baseline for a significant amount of the strategic education and thinking in the West. Thus, this binary framework may leave policymakers ill-equipped to recognize and operate within the gray zone.¹⁹⁹

Hal Brands expands on this idea that a lack of intellectual, organizational and bureaucratic preparation has created gaps and seams that allow our adversaries opportunities to operate effectively in the gray zone. In his opinion, aligning our bureaucratic and organizational structures with knowledge, understanding and experience in gray zone challenges is more important to achieving our objectives that having equipment or other material resources. For Brands, it is a paradox that “America is not poorly equipped for the gray zone—but it may not be fully prepared.”²⁰⁰

COL (R) David Maxwell concurs with Brands’ assessment but takes this idea a step farther by questioning whether we are prepared to “do strategy” in the gray zone. Maxwell asserts that we have tremendous capability and capacity and thus the ability to execute a campaign plan designed to counter our adversaries’ use of a hybrid strategy. For Maxwell, the questions are “whether we are prepared to orchestrate all these tools, organizations, and elements as part of a holistic strategy with balance and coherency among ends, ways, and means…and do we have national security structure capable of operating in the gray zone?”²⁰¹

Irregular Warfare

Outside of USSOCOM, we are organizationally and intellectually unprepared to conduct Irregular Warfare and must adapt our professional military education, thought processes, policy making and strategy development so that we are better prepared to conduct Irregular Warfare. Irregular Warfare is not only for Special Operations. In particular, our officers require doctrinal and theoretical grounding in the principles of
Irregular Warfare. This is critical to our ability to achieve success against our adversaries who pursue hybrid warfare strategies in the gray zone; in particular the Russians, whose hybrid warfare concept includes a military component heavily weighted towards UW.

In his Small Wars Journal Article, “Do We Really Understand Unconventional Warfare?” COL (R) David Maxwell states that “USSOCOM has been working over the past year to remedy the lack of joint and DOD doctrine and will soon publish the first ever joint doctrine for UW; however, that is unlikely to solve the problem of policy makers and strategists not appreciating and understanding unconventional warfare and all that operating in that realm of warfare entails. There seems to be an insufficient intellectual foundation in unconventional warfare.”

John Nagl asserts that we are not organized properly to conduct Irregular Warfare. His remedy for this is to establish an Advisory Corps dedicated to Irregular Warfare missions. Nagl takes this a step further and asserts that the US Army must man this Advisory Corps with skilled, experienced cadre that possess the requisite language and cultural understanding to successfully execute this mission. Additionally, he calls for skills collecting and analyzing intelligence information about our partners, the enemy and the operational environment. While Nagl is correct in his assessment that personnel assigned to the Advisory Corps will require language, cultural skills and experience beyond what we expect of Soldiers assigned to General Purpose Forces, our advisors will also require the ability to understand their operational environment. The importance of understanding, in the context of hybrid warfare, will be discussed in more detail. At this juncture, the fact that countering our adversaries in the gray zone
requires engagement in the human domain mitigates toward being able to have the right people, with the right skills and experience assigned to positions where they are needed; whether these positions are in cyber command, an interagency assignment, the intelligence community or an operational unit such as a Special Forces Detachment or the Advisory Corps.

Understanding as a Principle of War

Hal Brands asserts in his article “Paradoxes of the Gray Zone” that while we are well equipped to operate in the gray zone we are not fully prepared to do so. Brands calls for us to prepare ourselves intellectually as well as organizationally. This is especially important if the US plans to counter the Russians’ hybrid warfare strategy. The nature of the operational environment in this context is volatile, uncertain, complex and ambiguous. As was previously discussed, this complex operational environment requires personnel that possess cultural and language skills as well as military skill and experience. But beyond skills, the US requires personnel, from the strategic level down to the operational level that possess an understanding of their operational environment, the nature of the threats and the capability, capacity, will, motivations and limitations of the partners they will work with.

Renowned military theorist Frank Hoffman believes that understanding is so vitally important that it should become one of the immutable principles of war alongside the more traditional military principles of objective, offensive, mass, economy of forces, maneuver, unity of command, security, surprise and simplicity. For Hoffman, understanding is “craft, strategy and operations upon a detailed understanding of the nature of military conflict and the specific context (cultural, social, political and geographic) in which military force is to be introduced and applied.” This implies that
the nature of war is incredibly complex because it involves humans. Indeed, it is the human, cognitive domain in which hybrid warfare is waged. Succeeding in this complex environment requires more than language and cultural skills; it requires an ability to answer the fundamental question of ‘why.’ Why is something happening or not happening? Why is the enemy doing what he does? Why are the local people behaving the way they are? Why is the local partner that we are working with willing (or not) to do certain things? Having understanding not only enables people to answer these questions but to also turn these answers into plans of action that are suitable, feasible and acceptable given the totality of the circumstances.

Hoffman rightly contends that there are significant implications for professional military education, at every level, in order to achieve the level of understanding required to counter a hybrid strategy in the gray zone. He asserts that “we must therefore prepare a generation of future warriors with the general skill sets of working within foreign cultures, while learning how to access specific knowledge and understanding of crisis areas on short notice. Rather than focus on network-centric forms of war, there is great merit in calls for cultural-centric warfare, in which our soldiers and sailors are prepared with an acute degree of cultural awareness and the need for “global scouts to advance our interaction with foreign societies.”

Achieving Understanding - Culture and Language

Language, cultural understanding and operational experience are not developed overnight. They are time consuming skills and, once developed, must be maintained. Individuals with language capability, cultural expertise and experience in a particular region that are assigned to an Advisory Corps unit are tailor made for that particular mission and using them to fill gaps in other units that do not have the same mission
degrades readiness and fails to properly utilize our human capital. Each of these considerations has great impact on all of our mechanisms and policies for how we recruit, retain, assign and promote our people. Many of these personnel management policies have foundations in US law that require Congressional action to change.

In Frank Hoffman’s explanation of why understanding is vitally important and should therefore become a principle of war, he addresses the importance of having a deep understanding of a society’s culture, language, history and social patterns.²⁰⁸ Like Hoffman, Lieutenant General (R) Mike Flynn believes that this is vitally important as he wrote in his 2010 critique of the intelligence community when he was the senior intelligence officer for the International Security Assistance Force in Afghanistan. Flynn found that, despite having been in Afghanistan for nearly ten years, the US military and the rest of the Intelligence Community lacked a fundamental understanding of their operational environment. In Flynn’s assessment “the tendency to overemphasize detailed information about the enemy, at the expense of the political, economic, and cultural environment that supports it, becomes even more pronounced at the brigade and Regional Command levels.”²⁰⁹ Achieving an understanding of the operational environment is grounded in having knowledge about the local culture, language, religion and social norms. This has implications for our professional military education to which we will now turn.

Professional Military Education

Properly investing in our most precious resource, our people, is essential if we are to achieve the understanding necessary to successfully counter our adversaries use of a hybrid warfare strategy in the gray zone. Once we successfully recruit the people with the right potential, we must train them and then prepare them to succeed in the
operational environments we expect them to operate in. This is particularly true for our Special Operations Forces and personnel assigned to the Advisory Corps and Military Intelligence military occupational specialties. Language and cultural skills are part of this training as are lessons in the history, religion and societal norms. This type of skill development instruction starts individuals out in the right direction to help them achieve an understanding of their operational environment. However, our professional military education has significant gaps, at every level of instruction, regarding an understanding of the theory and practice of Irregular Warfare.

Frank Hoffman asserts that our professional military education must do more than just teach our doctrine and specific military skills. He believes that a fundamental shift in or culture is needed, starting with the way we train people. For Hoffman, it is vitally important that we train people to become adept at problem solving and to be agile and adaptive enough to adjust to one’s operating environment. These qualities are particularly important when conducting Irregular Warfare and operating against a hybrid threat in the gray zone.

In August 2011, the Joint Special Operations University hosted a SOF-Power Workshop that was designed to bring together a group of subject matter experts to explore the future need for an understanding of Special Operations theory and strategic art. They concluded that succeeding in the future will require “a SOF strategic culture that constantly advances strategic thinking and education in a SOF strategic art. Such a culture must rest on the foundations of a unified theory of Special Operations and a body of knowledge to support the demands of educating a strategic force.” This panel of experts made a number of recommendations at the conclusion of the workshop
that are specific to the professional military education of SOF professionals as well as members of the conventional military. Their recommendations include:

- “Encourage the enhancement of strategic art-level Special Operations classes at the various PME institutions and particularly in SOF Electives
- Establish a SOF pre-War College course of 2–3 weeks, focused on SOF strategic-level subjects to prepare SOF students for better advocacy during their class year
- Adapt SOF strategic curriculum courses for integration into Senior Service College’s (SSC) core courses, vice into SOF electives.
- Consider development of a School for Advanced Special Operations Warfare Studies (SASOWS), similar to the School of Advanced Military Studies (SAMS) or the School of Advanced Air and Space Studies (SAAS)
- Incorporate Special Operations strategic art and warfighting into the service’s advanced course curriculums.”

The findings and recommendations of the SOF-Power Workshop regarding Professional Military Education are a start point for including much-needed SOF theory, SOF strategic art and Irregular Warfare-related curriculum into our military educational institutions.

**Winning at the Strategic Level – The Human Domain**

Given the effects of globalization in the information age and the increasing velocity of human interaction, combined with the inter-connected nature of the world
economy and global commons, we will prevail in future conflicts if the US military possesses Strategic Landpower capable of winning at the strategic level by deterring, denying and defeating threats by employing combat power and people capable of operating effectively in the human domain. Tomorrow's strategic environment will likely become even more volatile, uncertain, complex and ambiguous and the military must possess people capable of leadership and engagement that are able to succeed in the human domain by integrating joint, interagency, intergovernmental and multinational capabilities amongst all the domains the Joint Force must operate in. Technology alone will not achieve the overmatch required to win because superior technology can be nullified or pilfered and exceptional concepts of operation outmaneuvered. Our future margin of victory will likely be decided by whether we have the keenest, most competent, most committed people our country has to offer.

Strategic Landpower is the essential military force for winning at the strategic level. War is an incredibly complex human endeavor and this is particularly true when facing an adversary employing a hybrid warfare strategy in the gray zone. The Russian approach to implementing a hybrid warfare strategy that is underpinned by unconventional warfare, cyber and information operations, makes the use of Strategic Landpower's ability to engage in the human domain even more relevant. Hybrid conflicts are inherently political and are fought amongst the people using host nation security forces or proxy forces. Key components of countering the Russians’ hybrid warfare strategy are Counter-Unconventional Warfare supported by information operations, intelligence and cyber operations. Each of the domains in which hybrid warfare is fought in greatly impacted by what we will term the human domain despite
the fact that current US Joint Doctrine does not specifically categorize the human domain. As we will see, our human capital is the key component to successful engagement in the human domain and therefore we must invest in our most precious resource; our people.

The Role of Strategic Landpower

The US Joint Staff’s Capstone Concept for Joint Operations describes a concept for globally integrated operations for how the Joint Force should prepare for the future strategic environment we will soon face. The concept calls for a Joint Force capable of quickly combining its capabilities with mission partners “across domains, echelons, geographic boundaries, and organizational affiliations.” Further, the capstone concept emphasizes the importance of partnering and “integrat[ing] effectively with U.S. governmental agencies, partner militaries, and indigenous and regional stakeholders to leverage expertise and resources existing outside the U.S. military to achieve unity of effort in applying all elements of national power.” The ability to effectively integrate and achieve cross-domain synergy enables exploitation of advantages in one domain, thus potentially creating advantage in other domains. Critical to the concept of a globally integrated force is our ability to develop deep regional expertise while integrating knowledge of political and cultural considerations; particularly during security cooperation, counter-insurgency and irregular warfare operations. Thus, one can see how Strategic Landpower is an essential capability for the Joint Force to successfully operate in the land and human domains while influencing the other domains through human interaction. Adding the human domain to US Joint Doctrine is an essential first step toward codifying the nature of the operational environment, the face of future
conflict and how we will operate as a Joint Force as articulated in our Capstone Concept for Joint Operations.

The overarching concepts outlining the importance of an ability to successfully operate and engage in the human domain, as it relates to Strategic Landpower’s contribution to the Joint Force is described in the Strategic Landpower Task Force’s May 2013 White Paper, "Strategic Landpower: Winning the Clash of Wills." ²¹⁷

The Army Operating Concept

The Army has recognized that Strategic Landpower’s ability to engage in the human domain is a critical capability required in the future joint force. Towards this end, the Army developed its current Army Operating Concept which describes how future Army forces will prevent conflict, shape security environments, and win wars while operating as part of our Joint Force; working with multiple partners. The Army Operating Concept’s title, “Win in a Complex World”, emphasizes the importance of ready land forces’ defending the nation and achieving our vital interests across the spectrum of conflict. The Army Operating Concept focuses at the tactical, operational, and strategic levels of war and describes how Strategic Landpower enables winning at the strategic level by operating in the human domain and employing more than just firepower.²¹⁸

The Engagement Warfighting Function

The Army’s initiatives for preparing to operate in the human domain go beyond just studying the problem and defining conceptually how the Army will operate as part of the Joint Force while developing its personnel to accomplish the mission. Towards these ends, the Army Training and Doctrine Command published the “U.S. Army Functional Concept for Engagement” and designated ‘Engagement’ as a new Army warfighting function. Engagement is defined as “the related tasks and systems that
influence the behaviors of a people, security forces, and governments” and designating it as a warfighting function was intended to utilize recent wartime experiences for development of the future force and institutionalization of required capabilities, The Army Functional Concept for Engagement describes how the Army effectively operates in the land domain to win at the strategic level, considering the human dimension of warfare, by engaging to “assess, shape, deter, and influence the decisions and behaviors of a people, security forces, and governments.”

In their article, “Toward Strategic Landpower,” LTG Charles T. Cleveland and LTC Stuart L. Farris argue that future military success requires a continuously increasing interdependence among military, interagency, intergovernmental and multinational partners. Critical to Landpower achieving this success is its ability to know the populace in the framework of the operational environment. This knowledge enables successfully influencing behavior in the human domain to achieve the desired outcome. Cleveland and Farris call for a dedicated effort to “organize, educate, train, equip and provide forces for operating in the human domain as we already do in the land, air, maritime, space and cyber domains.” The development of the capability to successfully engage in the human domain enables Strategic Landpower to prevent, shape and win across the spectrum of conflict to achieve the desired [political] outcomes. But we must do more than just train the people that we have to successfully operate in the human domain. We must also succeed at recruiting and retaining the best talent available. Succeeding in the human domain requires skilled, experienced people and we cannot surge to gain experience in times of conflict. A deep bench of people with
experience and cultural expertise is required. Special Operations Forces have long recognized this fact and all of the “SOF Truths” speak to this.\(^\text{221}\)

The Human Domain

The United States Special Operations Command has devoted considerable effort to understanding the complexities of the gray zone and the hybrid threats we may face there in the future. In a recent interview with the Tampa Tribune, the Commanding General of USSOCOM, General Votel stated that “a key part of success in the gray zone is understanding how and why societies work, knowing the key players and cultures and motivations. It’s all part of what the military and academics like to call the human domain.\(^\text{222}\) Whether the United States and its partners and allies face hybrid threats operating in the gray zone, near-peer adversaries employing conventional military force in decisive combat operations or simply US forces engaging our partners overseas to build their capacity during theater security cooperation exercises, a deep understanding of the human domain will be required in order win at the strategic level. It is a fundamental premise that people are the center of all national engagements and it is equally self-evident that war, or more broadly, conflict, is also an inherently human endeavor. "War remains a clash between hostile, independent, and irreconcilable wills each trying to dominate the other through violence. Enemies will continue to search for, find, and exploit U.S. vulnerabilities. Even when waged with increasingly sophisticated technologies, the conduct of military operations remains a fundamentally human enterprise."\(^\text{223}\) The means required to assure that we achieve the ends desired – that we win in a complex environment – are people. So is there are human domain and, if so, how is it described?
A definition of the human domain developed by the Army Special Operations Capabilities Integration Center is “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 population-centric conflicts.”

The human domain, as described by former commander of US Special Operations Command, Admiral William McRaven, is “unlike other domains that are easily defined by geospatial boundaries such as land, sea, air and space. It is a domain that encompasses the social, cultural and physical elements that influence human behavior.”

The military element of national power is employed in all of the domains in what is referred to in US joint doctrine as the ‘operational environment.’ Accordingly, the US joint doctrinal manual, Joint Operations Planning, describes the operational environment as “the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors of the air, land, maritime, and space domains and the information environment (which includes cyberspace). Included within these areas are the adversary, friendly, and neutral actors that are relevant to a specific joint operation.”

A unifying characteristic of all aspects and domains included in the operational environment is that humans operate in them, or affect them to varying degrees.

Investing in our Human Capital

In February 2015, newly appointed Defense Secretary Ash Carter assumed his new position and the topic he selected for his first speech was about people. He spoke about how to identify, recruit and retain the best military and civilian talent in the
Department of Defense and not about the expected topics of reorganization of the force, the defense budget, sequestration, research and development, technology or modernization. Carter’s explanation for prioritizing the human resources aspect of the Department of Defense was that winning the unknowable future war would be less about technology and instead won by out-smarting the enemy, using a total force comprised of intelligent, capable, adaptive leaders. For the Secretary of Defense, prevailing in future wars is dependent on talent in the ranks and he clearly articulated this as a top priority in his first presentation as Secretary of Defense.\textsuperscript{227} 

Congress must reform / repeal the Defense Officer Personnel Management Act (DOPMA) and support the Secretary of Defense’s ‘force of the future’ initiatives by supporting similar legislation restricting grade plate authorizations and up-or-out policies for Enlisted Soldiers. Congress must also approve funding costs associated with recruiting, retention, critical skills training, and quality of life programs so that we can have the skilled, experienced personnel the Army requires to conduct Irregular Warfare and succeed against our adversaries that conduct hybrid warfare in the gray zone. Our Soldiers are the critical capability that makes Strategic Landpower the essential military element of national power for winning in the volatile, uncertain, complex and adaptive strategic environment we face in the future.\textsuperscript{228} 

Conclusions 

The nature of warfare has significantly changed over the past 13 years of conflict. The National Intelligence Council assesses it is highly likely that the future adversaries we will face will employ irregular and hybrid warfare in the gray zone in order to achieve their political objectives. Going forward, a bright line separating the conditions of peace and war is unlikely to exist and the threats we face will likely seek to operate in that
seam between peace and war in order to avoid inviting Western intervention or interference by international organizations. Thus, we must have a strategy for countering our adversaries’ use of hybrid strategies in the gray zones of tomorrow. The strategy we adopt must address the fundamental fact that, in the end, warfare is about achieving political objectives and winning a better peace.  

We must adapt our organizational structure, policies, strategic approach and the ways and means available to successfully counter future hybrid threats. This paper has outlined the Russian approach to hybrid warfare and revealed the vulnerabilities associated with their strategy, operational design and associated tactics. With this understanding, the paper recommends some specific actions with the potential to exploit the vulnerabilities associated with the Russian approach to hybrid warfare. The recommendations made here address our need to change personnel policies to better enable us to make long-term investments in human capital that position us more favorably to successfully engage in the human domain and win at the strategic level. Additionally, this analysis offers organizational and policy changes to better organize the US Army, Cyber Command and our information operations enterprise across the Interagency to counter hybrid threats. These recommendations propose changing our intellectual culture and the professional military educational structure that underpins it to better prepare the Army and its people to face hybrid threats operating in the gray zone. Finally, it is recommended that the US and its allies modify their strategies to conform to the framework offered by Political Warfare. Adopting these recommendations will enable us to successfully counter future Russian use of a hybrid warfare strategy thus achieving our strategic objectives.
U.S. policy makers should consider political warfare as a strategy for countering Russia’s hybrid warfare strategy it is employing in the gray zone. Political Warfare would satisfy both Sun Tzu and Clausewitz because it uses the indirect approach to attack the enemy’s strategy and center of gravity by shaping the enemy and synchronizing the employment of all elements of national power before hostilities. Supported by Irregular Warfare, a Political Warfare strategy balances Clausewitz’ trinity and adheres to Sun Tzu’s teachings by employing moral authority to connect the people to their government while separating the insurgents from the people. A political warfare strategy addresses our ability to counter hybrid threats in the gray zone and fills the critical policy gap General Votel cautioned us about. Political Warfare seeks the path to victory with the least bloodshed, least risk and least amount of resources while attempting to achieve the acme of skill described by Sun Tzu as subduing the enemy without fighting.

Endnotes


9 “Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP--the Marshall Plan), and ‘white’ propaganda to such covert operations as clandestine support of ‘friendly’ foreign elements, ‘black’ psychological warfare and even encouragement of underground resistance in hostile states.” George Kennan, “Policy Planning Staff Memo,” National Archives and Records Administration, RG 273, Records of the National Security Council, NSC 10/2, May 4, 1948. http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm (accessed September 27, 2015).


13 Votel, Cleveland, Connett, and Irwin, “Unconventional Warfare In,” 106.


16 Ibid., 96, 102 and 106.
17 Ibid., 66 and 106.
18 Ibid., 144-149.
19 Ibid., 77.


22 Baumann, “From Droid Armies,” 12.


26 Ibid., 177-186.

27 Raska, “China And The ‘Three Warfares’,” 1.


30 Ibid., 6-7.

31 Ibid.


Ibid., 17-18 and 28.

Ibid., 14-15.


Leonhard and Phillips, “‘Little Green Men’: A Primer,” 2 and 5.


51 Herzog, “Revisiting The Estonian Cyber Attacks,” 56.


60 Ibid., 21.

61 Ibid., 42.

62 Ibid.
“Russia’s Reliance on Landpower. The war demonstrated Russia’s willingness and ability to fight conventional wars. It also revealed a reliance on landpower as the primary means of Russian warfare. Russia’s success, however, was relative to the force ratios, which heavily favored them.

Command and Control. Another observation from the war—Russian C2 systems did not have modern satellite or GPS capabilities. Therefore, tactical units communicated primarily by low quality radio or mobile phones. This slowed the pace of communications needed in modern warfare and reduced the level of security. At the direction of the President, they have accelerated the purchase of improved systems such as the GLONASS, and senior leaders appear to recognize the need to improve communications.

Intelligence. Russian intelligence was ineffective. For instance, the Russian military was unaware that Georgia had purchased the SA-11 anti-aircraft system from Ukraine and the Spyder anti-aircraft system from Israel before the war. These systems were responsible for many of the Russian aircraft shot down by Georgia once the war began. The lack of satellite reconnaissance capabilities resulted in incomplete information on the Georgian forces’ preparations and activities, including lack of knowledge of where the major Georgian military garrisons were located. At the operational and tactical levels the lack of modern reconnaissance systems also hampered Russian intelligence efforts. This nearly had disastrous results for the Russian Army when the Russian 58th Army command group drove into a Georgian ambush that destroyed 25 of its 30 vehicles, killing a large number of officers and soldiers and wounding the 58th Army Commander. Lack of funding, lack of modernization and lack of training took its toll on the once-strong Russian warfighting intelligence function. Russia has begun to correct those deficiencies by fielding a modern intelligence system, complete with satellite and UAV intelligence capabilities.

Maneuver. The Russian Army had problems using helicopters to deploy soldiers in Georgia. This resulted from insufficient helicopter training in mountainous terrain. Russian mechanized maneuver in this war reflected the Soviet tactics, with units “moving in column formation, fighting from the lead elements and continuing to press forward after making contact. They generally made no attempt to stop, establish support by fire positions, and maneuver to the flanks of the Georgian units they encountered.”

Fire Support. There were several observations concerning fire support. The first is that the Russians lacked sufficient GPS, satellite communications and UAVs for target acquisition and designation. This precluded the effective use of Russia’s relatively modern precision-guided munitions. Counter-battery radars were also lacking, resulting in an inability to find and engage Georgian artillery units. These shortcomings increased the need for large volumes of artillery fire. Russian reports indicate that they are addressing this concern by purchasing UAVs from Israel. They also recognized the need to train artillery observers, Special Forces, and recon unit...
personnel to operate with artillery and aviation to employ precision weapons. The Russian hybrid warfare in the Eastern Ukraine, or proxy war, depicts how Russia’s doctrine has changed since 2008.

**Combined & Joint Operations.** Combined arms operations involving the infantry and artillery generally worked well, but joint operations between the Army and Air Force were less effective. There were clear indications of inadequate inter-service cooperation. The high losses of aircraft, despite being piloted by experienced pilots, indicate deficiencies in pilot training and aircraft capabilities. Most notably, the Air Force did not have air controllers with ground units. In addition, ground units and pilots could not communicate effectively because radios were often not compatible.

**Sustainment Operations.** Reports indicate severe logistical problems because of a bureaucratic supply system. For example, a Russian tank platoon was surrounded and destroyed by Georgian rocket-propelled grenades (RPGs) after the platoon ran out of ammunition. Maintenance and logistical problems also hampered the Russian advance even after effective Georgian resistance had ended.

**Protection.** Russian Air Forces were not able to suppress Georgian air defenses. At least seven Russian Su-25 and Su-24 aircraft and one Tu-22 bomber were destroyed by Georgian air defenses. Furthermore, Su-25s were old and not well equipped to fly in bad weather or at night. The Russians are replacing the aging Su-25s, and revising doctrine to improve air-to-ground and air-to-air coordination to suppress enemy air defenses. They are also improving pilot training by increasing annual flying hours from 40 to 200, and improving electronic warfare capabilities.

**Manpower.** The war against Georgia exposed several weaknesses in the Russian personnel system. First, the war demonstrated that the cadre system was ineffective. Under this system, only key command and staff positions are filled in peacetime, and the unit is supposed to be capable of rapidly expanding in wartime with the addition of new recruits. Next, the war exposed a lack of professional (or “contract”) soldiers, forcing the Russian Army to deploy conscripts to the fight, despite official policy forbidding the use of conscripts in wars. As part of its reform efforts, Russia is eliminating cadre units and expanding the number of professional soldiers in its Army.

Finally, Russia has changed the way it generates manpower, by formalizing the use of paramilitaries and proxy groups (long a force multiplier used by Russia in its wars). Russian President Vladimir Putin signed a decree, which allows foreign citizens to serve in the Russian army as contractors. The decree reads: Military men, who are foreign citizens, can participate in carrying out the tasks during military situations, and also during armed conflicts, in accordance with admitted principles and norms of international law, international treaties of the Russian Federation, and the Russian legislation.”


---


72 Ibid., 54.


74 Ibid., 48.


86 Kofman and McDermott, “No Return to Cold War,” 7.


89 Ibid., 31.


91 Ibid., 51.

92 Ibid., 50.
Ibid., 64-65.

Ibid., 31.

Ibid., 32.

Ibid., 33.

Ibid.


Ibid., 65.

Ibid., 52.

Leonhard and Phillips, “‘Little Green Men’: A Primer,” 43.

Ibid., 43-44.

Ibid.


Wilson, Ukraine Crisis: What It Means For The West, Kindle Locations 2561.


Leonhard and Phillips, “‘Little Green Men’: A Primer,” 43-44.
112 Ibid., 46.
113 Ibid., 45.
120 Ibid., 48.
121 Ibid., 49.
122 Ibid., 6.
126 Ibid., 61.
131 Ibid., 7.


135 Ibid., 34.


137 Ibid., 3.


139 Leonhard and Phillips, “‘Little Green Men’: A Primer,” 44.


147 Wilson, Ukraine Crisis: What It Means For The West, Kindle Locations 4174-4213.

148 Ibid., Kindle Locations 4166-4171.


151 “The U.S. and its partners can indeed overmatch adversaries practicing hybrid warfare and achieve escalation dominance against future adversaries—but only through a thoroughly whole of-government approach informed by unity of effort and purpose expressed through integrated strategy and cohesive policy options. This all amounts to Political Warfare, a supple, synergistic, and evolving use of “both overt and covert” tools at America’s disposal, with an emphasis on coercive diplomatic and economic engagement, Security Sector Assistance (SSA), information and influence activities (IIA), and diverse forms of unconventional warfare (UW). A thoroughly whole-of-government endeavor, Political Warfare is by no means the preserve of SOF. Given its diplomatic and economic content and its focus on achieving political ends, Political Warfare is likely best led by agencies beyond DoD. Indeed, Political Warfare can only succeed if it is conducted in a way to elevate civilian power alongside military power as equal pillars of U.S. foreign policy.”

152 “SSA, UW, C-UW and IIA hinge on skill sets cultivated by SOF, the latter are uniquely positioned to support both the joint force and America’s agencies beyond DOD leading Political Warfare strategies. Furthermore, SOF are unique in the Department of Defense, suited to integrate Political Warfare’s activities across the JIIM spectrum. Army Special Operators have a proven track record of bridging indigenous forces, local populations, Joint Force components, U.S. agencies, and coalition partners needed for an effective Political Warfare response to hybrid warfare. SOF must be the expert practitioners of this form of warfare to lead DOD’s contribution.”
Ibid., 10.

153 “Unconventional warfare at its core is about revolution, resistance, and insurgency (RRI) combined with the external support provided to a revolution, resistance, or insurgency by either the US or others (who may or may not have interests aligned with the US and may in fact be opposed to the US and our friends, partners, and allies). This is a type of warfare...is both political in nature and at times violent. For some years in Syria we have been focusing on training and equipping the “armed component” (and until recently provided only limited non-lethal assistance). Yet it is the underground that provides the key to understanding the motivation, objectives, interests, methods, and strategy of the leadership of a revolution, resistance, or insurgency (RRI).”


159 Ibid., 4.


165 Ibid., 7.


Using the SOCOM model, USCYBERCOM would be organized is a “unified combatant command that performs Service-like functions and has Military Department-like responsibilities and authorities. These unique functions, responsibilities, and authorities include programming, budgeting, acquisition, organizing, training, equipping, and providing combat-ready [Cyber] mission forces for employment by the CCOs and developing strategy, doctrine, tactics, and procedures for [Cyber].”


“SOF units based in the US are generally assigned to and under COCOM of CDRUSSOCOM, with OPCON exercised through the USSOCOM Service component commands. SecDef assigns the TSOCs to USSOCOM under CDRUSSOCOM’s COCOM, and assigns OPCON of the TSOCs to the GCCs. SecDef also authorizes CDRUSSOCOM/GCCs to establish support relationships when SOF commanders are required to simultaneously support multiple operations or commanders…As established in Title 10, United States Code (USC), Section 162, and discussed in Joint Publication 1, Doctrine for the Armed Forces of the United States, all forces shall be assigned or attached to and under command of a CCO, except as otherwise directed by Secretary of Defense.”

US Joint Chiefs of Staff, Special Operations, III-4.


178 “The DoD Manual … declares that it is “likely” that if a cyber operation produces “effects that, if caused by traditional physical means, [it] would be regarded as a use of force.” It goes on to provide examples that include a meltdown of a nuclear plant, opening a dam so as to cause physical destruction, or disabling an air traffic control system so as to cause a plane crash. The physicality of those illustrations would easily fit within the concept of “armed attack” as traditionally understood, and does not especially illustrate what kinds of lesser cyber incidents DoD would consider as sufficient to sanction a self-defense response.” Charlie Dunlap, “Cyber Operations and the New Defense Department Law Of War Manual: Initial Impressions,” Lawfare, blog entry posted on 15 June, 2015. https://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions (accessed February 20, 2016).


181 “Irregular Warfare (IW) is conducted independently of, or in combination with, traditional warfare. IW can include any relevant DoD activity and operation such as counterterrorism; unconventional warfare; foreign internal defense; counterinsurgency; and stability operations that, in the context of IW, involve establishing or re-establishing order in a fragile state or territory.” US Department of Defense, Irregular Warfare (IW), DoD Directive 3000.07 (Washington, DC: US Department of Defense, August 28, 2014). http://www.dtic.mil/whs/directives/corres/pdf/300007p.pdf (accessed February 29, 2016).


184 “Department of Defense Directive 3000.07 (Irregular Warfare) establishes five primary activities of Irregular Warfare: Foreign Internal Defense (FID), Counter Insurgency (COIN), Counter Terrorism (CT), Stability, Security, Transition and Reconstruction (SSTR) Operations, and Unconventional Warfare (UW). The first four of these activities (FID, COIN, CT, and SSTR) are ways that the U.S. can enable a HN to counter an existing or potential threat of insurgency. These activities seek to maintain a low U.S. troop signature, which protects or enhances the
legitimacy of the HN. UW is the only activity that does not seek to protect or enhance the legitimacy of the existing government within the HN. It is conducted in order to coerce, disrupt or overthrow a government or occupying power.”


192 Ibid., 4.


195 Ibid., 19-20.


200 Brands, “Paradoxes,” 5.


202 Maxwell, “Do We Really Understand,” 2.


204 Brands, “Paradoxes,” 5.


207 Ibid., 4.

208 Ibid., 3-4.


212 Ibid., 31-34.

214 Ibid. 6.

215 Ibid., 7.

216 Ibid., 11.

217 “Strategic Landpower,” 5.


223 *Capstone Concept for Joint Operations*, 2.


