A Whole-of-Government Approach to Gray Zone Warfare

by

Ms. Elizabeth G. Troeder
Department of the Army Civilian

Under the Direction of:
Professor Tamara K. Fitzgerald

United States Army War College
Class of 2018

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.
14. ABSTRACT
Gray zone warfare, also known as irregular warfare, political warfare, hybrid warfare, asymmetric warfare, and unconventional warfare, is increasingly the norm. Yet the United States is losing this war as will be demonstrated in this Strategy Research Project. The Department of Defense (DOD) has historically led the gray zone war effort with assistance from other federal agencies. But DOD cannot require other agencies to engage; it cannot be aware of all effective tools available across the whole-of-government; nor can it know how its proposed way forward may conflict with approaches made by other agencies. This paper builds the case for requiring U.S. federal agencies to request that the Deputy National Security Advisor convene a National Security Council Deputies Committee meeting whenever any federal agency deems a gray zone approach to an international issue is appropriate. It also recommends development of a standing National Security Council Policy Coordination Committee (NSC/PCC) for Gray Zone Solutions, with sub-NSC/PCCs for each component of the 4+1 so that experts can be quickly assembled in times of crisis. This will assure the President of the United States, Congress, and the American people that all elements of power have duly been employed and are synchronized.
A Whole-of-Government Approach to Gray Zone Warfare

(6618 words)

Abstract

Gray zone warfare, also known as irregular warfare, political warfare, hybrid warfare, asymmetric warfare, and unconventional warfare, is increasingly the norm. Yet the United States is losing this war as will be demonstrated in this Strategy Research Project. The Department of Defense (DOD) has historically led the gray zone war fight with assistance from other federal agencies. But DOD cannot require other agencies to engage; it cannot be aware of all effective tools available across the whole-of-government; nor can it know how its proposed way forward may conflict with approaches made by other agencies. This paper builds the case for requiring U.S. federal agencies to request that the Deputy National Security Advisor convene a National Security Council Deputies Committee meeting whenever any federal agency deems a gray zone approach to an international issue is appropriate. It also recommends development of a standing National Security Council Policy Coordination Committee (NSC/PCC) for Gray Zone Solutions, with sub-NSC/PCCs for each component of the 4+1 so that experts can be quickly assembled in times of crisis. This will assure the President of the United States, Congress, and the American people that all elements of power have duly been employed and are synchronized.
A Whole-of-Government Approach to Gray Zone Warfare

Gray zone warfare, also known as irregular warfare, political warfare, hybrid warfare, asymmetric warfare, and unconventional warfare, is increasingly the norm. Yet the United States (U.S.) is losing this war, despite its immense capacity for creativity and innovation. The February 2018 indictment of the thirteen Russians and three Russian companies for interfering in the 2016 U.S. presidential election using what was described as “information warfare,” a form of gray zone warfare, is the most vivid example of gray zone tactics used against the United States. The U.S. Government and American people were ill-prepared for this type of warfare.

The Department of Defense (DOD) has historically led the gray zone war fight with assistance from other federal agencies. But DOD cannot require other agencies to engage, nor can it be aware of all effective tools available across the whole-of-government. Most importantly, leadership at DOD cannot know how or if its proposed solution conflicts with or potentially harms approaches being used by other federal agencies unless all those agency approaches are considered from a whole-of-government perspective.

This paper builds the case for requiring U.S. federal agencies to request that the Deputy National Security Advisor convene a National Security Council Deputies Committee (NSC/DC) meeting whenever any federal agency deems a gray zone approach to an international issue is appropriate. It also recommends development of a standing National Security Council Policy Coordination Committee (NSC/PCC) for Gray Zone Solutions, with sub-NSC/PCCs for each component of the 4+1 so that experts can be quickly assembled in times of crisis. The NSC/DC will oversee the NSC/PCC as prescribed by National Security Presidential Memorandum (NSPM)–4 of April 4, 2017.
This will assure the President of the United States, Congress, and the American people that all elements of power have duly been employed and are synchronized.

The Gray Zone

The term “gray zone” was coined by the U.S. Army’s Special Operations Command in order “to describe activities, actions, or conflict in the space between peace and war.”¹ U.S. Central Command General Joseph L. Votel further describes that space between peace and war as “characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war.”² The types of campaigns waged within the gray zone are numerous; all are considered elements of soft power and are differentiated as Instruments of National Power (Diplomatic, Information, Military, and Economic) and Tools of National Security Policy (Finance, Intelligence and Law Enforcement).

Gray zone strategies are not new. In The Art of War, written in 500 B.C. and credited to the Chinese military strategist Sun Tzu, the author wrote, “To subdue the enemy without fighting is the acme of skill.”³ In 400 B.C., Kautilya, the Indian advisor to the first king of the Maurya Empire and credited for writing the political essay Arthashastra, recommended the use of secret agents, assassins, disinformation, deception, and weakening the bonds between united adversaries to create opportunity for his king. In the 20th century, the United States used gray zone tactics in Vietnam and during the Cold War. For example, the U.S. Army’s 7th Psychological Operations Group used propaganda to misinform the enemy during the Vietnam War. And during the Cold War, an information campaign was used both against the enemy as well as to gain U.S. public support against communism. “In 1950, the Central Intelligence Agency created the Congress for Cultural Freedom with the goal of undermining the Soviet Government
and winning over the hearts and minds of Europe’s left-leaning intellectuals.”

For example, books such as *Dr. Zhivago* by Boris Pasternak, music such as *The Rites of Spring* by Igor Stravinsky, and the film version of *Animal Farm* by George Orwell were given to unsuspecting Soviet patrons of the arts in Europe who thought they were acquiring decadent, exciting material. Not cognizant of the underlying message, they then distributed it to other patrons of the arts throughout the Soviet Union, thus unknowingly propagating the U.S. message in the Soviet Union. In the United States, the organization known as the “Children’s Crusade Against Communism” targeted American children in the 1950’s and 1960’s through the use of comic books, cards tucked into bubblegum wrappers, and school textbooks to generate U.S. support against communism. In addition, American television, movies, music, and art conveyed messages promoting the advantages of democracy.

The U.S. Army War College describes gray zone strategies as activities undertaken by “states dissatisfied with the status quo and determined to change important aspects of the global distribution of power and influence in their favor. Unwilling to risk major escalation with outright military adventurism, these actors are employing sequences of gradual steps to secure strategic leverage. The efforts remain below thresholds that would generate a powerful … response, but nonetheless are forceful and deliberate, calculated to gain measurable traction over time.”

Gray zone warfare is a significant concern today, threatening U.S. national security as well as the security of our allies and partners.

Strategic Guidance

The need to improve interagency collaboration in the United States has been deliberated ever since that horrendous day in 2001 when the terrorist attacks of
September 11th took place in New York, Pennsylvania, and Washington, DC. Eleven days following the attack, the U.S. Department of Homeland Security was created to oversee and coordinate “a comprehensive national strategy to safeguard the country against terrorism and respond to any future attacks.” It was a good start. But as the use of irregular warfare increases and evolves, a whole-of-government approach that incorporates the unique capabilities of federal departments and agencies for this fight is also needed.

The authors of the U.S. National Security Strategy (NSS) and National Defense Strategy reports dating back more than a decade have stated that the best method for achieving national security is using a whole-of-government approach. The 2006 Quadrennial Defense Review Report recommended “the creation of National Security Planning Guidance to direct the development of both military and non-military plans and institutional capabilities.” The 2009 Quadrennial Roles and Missions Review Report stated that DOD “supports institutionalizing whole-of-government approaches to addressing national security challenges.” In the May 2010 NSS, President Barack Obama devoted almost three pages to outlining a whole-of-government approach to strengthening U.S. national security. In June 2010, John Pendleton, Director, Defense Capabilities and Management, in his testimony before the Subcommittee on Oversight and Investigations stated, “Agencies lack adequate coordination mechanisms to facilitate this collaboration during planning and execution of programs and activities.”

Still, no changes were made and a lack of inclusive collaboration between agencies persisted.
The 2012 Defense Strategic Guidance states, “The global security environment presents an increasingly complex set of challenges and opportunities to which all elements of U.S. national power must be applied.” Former President Obama’s Executive Order (EXORD) 13721 of March 14, 2016 established the Global Engagement Center within the U.S. Department of State with the mission to “lead the coordination, integration, and synchronization of Government-wide communications activities directed at foreign audiences abroad in order to counter the messaging and diminish the influence of international terrorist organizations, including the Islamic State of Iraq and the Levant, al Qaeda, and other violent extremists abroad.” In his 2017 NSS, President Donald Trump stated, “Our diplomatic, intelligence, military, and economic agencies have not kept pace with the changes in the character of competition…. To meet these challenges we must … upgrade our political and economic instruments to operate across these environments.” In January 2018, DOD announced a reorganization within U.S. Cyber Command: “…President Donald Trump, in accordance with congressional mandate, directed Cyber Command to elevate to a full unified combatant command out from under Strategic Command.” As General Paul J. Selva said during his Senate Armed Services Committee reconfirmation as Vice Chairman of the Joint Chiefs of Staff in July 2017, “Responding to hybrid warfare is an inherently whole-of-government proposition.” The time to do so is now.

The February 2018 indictment of the thirteen Russians and three Russian companies for interfering in the 2016 U.S. presidential election provided impetus for Attorney General Jeff Sessions to stand up the Justice Department’s Cyber-Digital Task Force to “advise [him] on the most effective ways that this Department can confront …
threats [from criminals, terrorists, and enemy governments] and keep the American
people safe.” It also provides President Trump the opportunity to heighten public
awareness of outside influences or what is called gray zone warfare, which is
undermining American democracy and poses a significant threat to U.S. national
security.

Understanding the Environment

In December 2015, Chief of Naval Operations Admiral John Richardson
described the current threat as “four-plus-one,” where the goal was to “balance two
‘great powers’ of Russia and China, two ‘very influential’ regional powers in Iran and
North Korea, and the ‘persistent global counterterrorism challenge.’” The term “4+1”
has endured to describe the countries that are most active in the gray zone today.
Recent actions undertaken by the 4+1 indicate a profound need for a comprehensive,
measured approach in order to deny future effects of gray zone warfare. Speaking to
the Senate Select Committee on Intelligence in February 2018, Daniel Coats, U.S.
Director of National Intelligence, said, “Russia is using a variety of capabilities short of
war to assert its presence. President [Vladimir] Putin will continue to rely on assertive
foreign policies to shape outcomes beyond Russia’s borders…. Russia uses these
tools—including the cyber weapon—because it’s relatively cheap, it’s low risk, it offers
what they perceive as plausible deniability and it’s proven to be effective at sowing
division.” Furthermore, China “will take a firm stance on its claims to the East … and
South China Sea[s], its relations with Taiwan and its regional economic engagement” in
addition to its “One Belt, One Road initiative,” which seeks to improve China’s
economic condition from China throughout Asia to the Middle East and Africa, as
well as Europe. With respect to Iran, Coats said, “Iran will try to penetrate U.S. and
allied networks for espionage and lay the groundwork for future cyberattacks.”

“And North Korea will continue to use cyber operations to raise funds, launch attacks and gather intelligence against the United States.” A deeper understanding of each is needed, as well as a call to action.

Russia

A resurgent Russia, demonstrating aspiration to regain its status as a world power, has launched an extremely effective information campaign using “electronic warfare and other information warfare capabilities, including denial and deception as part of its approach to all aspects of warfare….“ Its “information confrontation”—or in the Russian language, “informatsionnoye protivoborstvo” (IPb)—can be delineated into two forms of informational destabilizing tactics. The “informational-technical effect is roughly analogous to computer network operations, including computer-network defense, attack and exploitation…. [The] informational-psychological effect refers to attempts to change people’s behavior or beliefs in favor of Russian governmental objectives.”

The United States has no such organized campaign. As General Scaparrotti, Commander, U.S. European Command, said before the House Armed Services Committee in March 2017, “we are not as effective as we could be … particularly in the information domain.” To mitigate this, the 2017 NSS (Pillar III) with reference to cyberspace states, “We will improve the integration of authorities and procedures across the U.S. Government so that cyber operations against adversaries can be conducted as required.” In addition, a Presidential EXORD on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure was issued to the U.S. Department of Commerce and the U.S. Department of Homeland Security on May 11, 2017. The draft report for public comment from the study identifies the risks and
proposes numerous actions to be taken by different agencies, but does not identify a specific lead for execution of the individual actions. This issue will be addressed below in the suggested approach towards a solution.

Russian manipulation of the global information environment having an informational-technical effect is rampant. The Fancy Bear reconnaissance program that, once downloaded, allows hackers access to any individual's computer, has been linked to Russia's military intelligence agency. U.S. intelligence claims the malware allowed hackers to breach the email account of the former chairman of Hillary Clinton's 2016 presidential campaign, John Podesta, during the 2016 elections. In 2015, hackers stole National Security Agency (NSA) classified information from a former NSA employee's home computer after he illegally removed the data from the Agency and loaded it onto his own equipment. And in 2016, Russian cyber experts effected a significant power blackout in Kyiv, Ukraine by attacking a transmission substation, resulting in electric grid operations impact and subsequent power outages throughout Ukraine, affecting hospitals, banks, and transportation, for more than 225,000 customers for approximately six hours.

Each of these events and many more can be instigated again if action is not taken. The malware used to cause the Kyiv power outage known as CRASHOVERRIDE, combined with numerous clauses found in the Military Doctrine of the Russian Federation (2014), reveals an escalation from Russian reconnaissance programs to programs causing outright destruction. Confirmation of this concern is provided in the Russian military doctrine known as SODCIT, or Strategic Operations to Destroy Critical Infrastructure Targets, which “calls for escalating to deescalate” in an
attempt to “un-level the playing field”\textsuperscript{29}, per retired General Martin Dempsey, former Chairman of the Joint Chiefs of Staff. The doctrine refers to the use of gray zone capabilities, including sabotage of adversaries’ energy grids as well as deployment of nuclear weapons.

The Russian drive to change people’s behavior in favor of Russian objectives—the informational-psychological effect—has also been extremely successful. This strategy, which embraces social media, has proliferated exponentially in the last decade. Russia’s “state-run propaganda machine”\textsuperscript{30} uses a variety of platforms such as television and radio to amplify pro-Russian themes, influence decision-making, and destabilize both the United States and countries in Europe. The television network RT—formerly Russia Today—and the Russian-funded government news agency Sputnik, have both been identified in a U.S. intelligence report “as being arms of Russia’s ‘state-run propaganda machine’ that served as a ‘platform for Kremlin messaging to … international audiences.’”\textsuperscript{31} Social media is also employed, where both bots and people are used to perpetuate the Russian agenda. Russia is known to have meddled in the U.S., German, and French presidential elections of 2016, 2017, and 2017, respectively. U.S. Congressional investigators were able to ascertain that more than 3,000 political advertisements that were displayed on the social media website called “Facebook” during the U.S. presidential election came from Russia. The advertisements targeted “every group in America” and they “…were indiscriminate,” but they created chaos at every level.\textsuperscript{32} In February 2018, prosecutors were able to indict thirteen Russians and three Russian companies with evidence that included a “detailed picture of how Russians used social media, fake rallies, and secretive operatives in the U.S. to create
political intensity by backing radical groups, opposition social movements, and disaffected voters.... [The Russian campaign] included direct contact with over 100 Americans...."³³ It is important to note however, that Deputy Attorney General Rod Rosenstein told reporters that, "This ‘information warfare’ by the Russians didn’t affect the outcome of the presidential election."³⁴

In the United Kingdom (UK), election officials suspect that Russia financed the political advertisements surrounding Brexit that were displayed on social media, since a UK vote to leave the European Union weakens the bonds between European countries, a key objective of Russia. And, “about 30 percent of the Twitter accounts that magnified the Catalan issue in Spain were registered in Venezuela but were Russian.”³⁵ Again, a Catalanian secession from Spain would be another division within democratic Europe and another win for Russia. Also significant are examples of Russia’s information campaign aimed at ethnic Russians and Russian-speaking minorities living in the Baltic States, which are “similar to … [the] disinformation efforts in Ukraine that led to Russia's annexation of the Crimean peninsula.”³⁶ Assertions such as these minorities are being “mistreated,” there is “ethnic cleansing” of local Russian populations, and “significant cities such as Klaipeda never belonged to Lithuania”³⁷ are efforts to destabilize the European Union, the North Atlantic Treaty Organization (NATO), and the United States. The concern that what is now a non-kinetic conflict will lead to a kinetic conflict and invocation of Article 5 of the NATO Treaty, the principle of collective defense, is significant. Per Article 5, “an attack against one Ally is considered as an attack against all Allies,” and thus obligates all Allies to defend any NATO member country from attack by a non-member country.
China

Examples of China’s gray zone tactics are its “One Belt, One Road” initiative as well as its “artificial island construction and militarization of facilities on features in international waters,” especially in the South China Sea. Both strategies expand China’s control in the Asian region and threaten national security, trade, and economic growth, particularly for those who require navigation through the South China Sea. The three primary issues in the South China Sea are multiple claims to land masses, multiple claims to Exclusive Economic Zones, and restrictions of varying activities enforced by claimants within their Exclusive Economic Zones, which are not necessarily consistent with international law. As Prime Minister Modi of India stated, “Respecting freedom of navigation and adhering to international norms [are] essential for peace and economic growth in the inter-linked geography of the Indo-Pacific.”

Former President Obama attempted to reassure our Asian allies and partners by making Asia a top priority for U.S. foreign policy. This “rebalancing” was not successful as China continued to engage in land reclamation activities in the South China Sea in addition to annexing the Spratly Islands. Finally in 2016, the Chinese government was challenged by the Philippines in an international court when Permanent Court of Arbitration Case Number 2013-19 was brought to The Hague. The findings of this landmark case refuted China’s claim to sovereignty in the South China Sea, addressed China’s international law violations of interference in traditional fishing rights, and stated that Chinese activities failed to protect and preserve the marine environment causing “irreparable damage … [in] the area.” In response, “a former senior Chinese official … said that the findings would amount to no more than ‘waste paper’ and that China would
not back down from its activities in the South China Sea even in the face of a fleet of American aircraft carriers.”

President Trump’s doctrine “America First,” combined with withdrawing from the Trans-Pacific Partnership trade deal almost immediately upon taking office in January 2017, caused further consternation amongst our Asian allies and partners. However, he acknowledged that freedom of navigation of the seas is imperative for economic growth of both the United States and Asian allies in the 2017 NSS when he stated, China’s “efforts to build and militarize outposts in the South China Sea endanger the free flow of trade, threaten the sovereignty of other nations, and undermine regional stability.” And on February 7, 2018, “U.S. Vice President Mike Pence referred to the possibility of the United States returning to the Trans-Pacific Partnership free trade deal when he met Deputy Prime Minister Taro Aso [of Japan]….”

Increased trade in the region will improve the economies of U.S. allies and partners, increase stability in the region, and slow the rise of China. Currently, the United States is using a conventional military approach for protection of ships sailing in the South China Sea. Although somewhat effective, there is the risk that an enduring U.S. presence may aggravate China, although it is unlikely to provoke the Chinese into military escalation. Nevertheless, freedom of navigation in the South China Sea must remain an important element of American policy.

Soft power was explicitly referenced in China’s national government policy for the first time at the 17th National Congress of the Chinese Communist Party in 2007 when President Hu Jintao said, “We must enhance culture as part of the soft power of our country to better guarantee the people’s basic cultural rights and interests.” Highlights
of his proposed methods included the need to improve Chinese media in order to “give correct guidance to the public and foster healthy social trends,” “to strengthen efforts to develop and manage Internet culture and foster a good cyber environment,” and “create a thriving cultural market and enhance the industry's international competitiveness….”

The People’s Liberation Army (PLA) General Staff Department Third Department Second Bureau, similar to the U.S. NSA, is responsible for cyber-espionage operations. “…Two PLA groups, Units 61938 and 61486, have reportedly stolen information from over two dozen Defense Department weapons programs, including the Patriot missile system and the U.S. Navy’s new littoral combat ship.” In June 2015, Politico reported that Chinese hackers “breached a database containing a wealth of sensitive information from federal employees’ security background checks.” It is believed that the Chinese Government is not only targeting the U.S. Government, but also U.S. defense contractors and think tanks. China’s gray zone tactics used against the United States, her allies, and partners require unrelenting, focused attention.

Iran

Iran’s soft power strategy includes using the media, distribution of money under the guise of charity, as well as brazen bribery. Iran has also been charged with denial-of-service attacks against 46 major financial institutions. “These attacks cut customers off from online access to their bank accounts and cost the victim companies tens of millions of dollars…. One of the hackers was also charged with obtaining unauthorized access into the industrial control systems of the Bowman Dam, located in Rye, New York [in 2013]. Had the dam not been disconnected from the system for maintenance, the intrusion could have given the hacker control of the dam’s water levels and flow rates.” In terms of cyber espionage, one Iranian cyber team “has
invaded computers around the world, with targets in the petrochemical, defense, and aviation industries. The group uses code linked to Iran’s wiper malware, possibly in preparation for more destructive attacks. Another group … has been active since at least 2014, targeting companies in the financial, energy, telecom, and chemical industries.”

In 2016, this included the New York Stock Exchange and AT&T.

Recently, Iran expanded its Islamic Azad University to Syria, Iraq, and Lebanon with the goal of promoting Iran’s ideological and political goals in an educational environment. During his speech in January 2018, Ali Akbar Velayati, foreign policy advisor to Supreme Leader Ali Khamenei, “stressed that Iran’s soft power influence is helping the ‘expansion of Islam’ in different parts of the world, including in China, India, and the Arab world – particularly focusing on Shiite Islam.” Per General Paul Selva during his reconfirmation as Vice Chairman of the Joint Chiefs of Staff, “Iran seeks to achieve regional power and influence in the Middle East through a variety of means. To advance its strategic interests, it is pursuing more advanced missile systems and a more capable naval presence that could be used to threaten the Arabian Gulf region and Strait of Hormuz in the event of conflict. It is also developing proxy forces, supporting Shi’a movements, and promoting other pro-regime elements throughout the region,” such as fighting a proxy war against Saudi Arabia in Yemen through its support for a Shi’ite opposition group there, its support provided to President Bashar al-Assad in Syria in its fight against the Islamic State of Iraq and Syria (ISIS), and its expanding influence in Iraq. Given Iran’s close ties to Hezbollah in Lebanon, Iran now has direct access through Iraq and Syria across Israel’s northern border to the Mediterranean Sea. Accordingly, General Joseph L. Votel, Commander of U.S. Central
Command, said before the House Armed Services Committee in February 2018, “Leaders in the Islamic Revolutionary Guard Corps–Quds Force have taken advantage of surrogates, businesses, and logistics entities to execute direct action, intelligence, influence building, terrorism, and cyber operations against the U.S. and our partner nations.”\(^5^4\) It is anticipated that “Iran will continue to pursue policies that threaten U.S. strategic interests and goals throughout the Middle East while seeking to expand diplomatic and economic relations with a wide range of nations.”\(^5^5\)

**North Korea**

North Korea’s state-sponsored criminal activity is lucrative and widespread, ranging from Asia to Europe as well as Africa. It has been characterized as money laundering, cyber warfare, drug trafficking, and smuggling primarily to fund its weapons of mass destruction programs. A headline from a recent article from *Defense One* reads, “Kim’s nuclear arsenal is built to ‘deter and coerce.’”\(^5^6\) And it has been found that North Korean diplomats, as well as those posing as North Korean diplomats, repeatedly abuse their privileges of diplomatic immunity in order to commit these crimes.

North Korea has been accused of money laundering for over a decade. In 2006, it was found to be “producing ‘superdollar’ counterfeit $100 bills. The Benjamins were so accurate, they were practically indistinguishable from the real thing. The United States was forced to redesign the bill in 2013, adding a ‘3D security ribbon,’ tiny text, and color shifting images.”\(^5^7\) As North Korea continued its practice, it was finally “designated a ‘primary money laundering concern’ under the Patriot Act”\(^5^8\) in 2016.
North Korea’s cyber activities have been on-going and disruptive for some time, but they are best-known for the attack on Sony Pictures Entertainment in 2013 when Sony embarked on creating the movie *The Interview*, a comedy about assassinating the leader of North Korea, Kim Jong-un. “The original release date of *The Interview* was targeted for the end of 2014; however, before the movie could be released an incident occurred that put hackers in complete control of Sony Pictures Entertainment's network.” Retaliation against the American film endeavor considered embarrassing to Kim Jong-un was characterized by stolen intellectual property, extortion, the release of personally identifiable information, and a destroyed computer system. Despite actions taken by North Korea and at former President Obama’s urging, Sony released the film and “the U.S. Government added new sanctions against North Korea.”

Since the 1970’s, leadership in Pyongyang has been rewarding drug traffickers and smugglers primarily of illegal rhino horn and ivory from Zimbabwe and Zambia as well as gold from Bangladesh, pharmaceuticals, tobacco, and cigarettes. Although “North Koreans have been implicated in 18 of at least 29 detected rhino horn and ivory smuggling cases involving diplomats in Africa since 1986,” the practice continues. In 2013, “North Korea sent a large amount of illegal drugs to its embassy in an East European Country…. [Apparently, Pyongyang had] ordered each diplomat to raise US$300,000 to prove their loyalty and mark the birthday of the nation’s founder Kim Il-sung…. At approximately the same time, methamphetamines were smuggled into the United States and Australia. According to “a North Korean police officer who defected to
South Korea, methamphetamine manufacturing is frequently a joint operation of the Chinese and North Korean underworld.”

North Korea wields soft power however it can. Skeptics of North Korea believed that “improved relations” between North and South Korea, particularly in February 2018, were really opportunistic propaganda staged to avoid additional sanctions due to the North Korean nuclear weapon and missile programs. “A few athletes, some winsome cheerleaders and Kim Yo-jong, the younger sister of North Korea’s dictator, spread a shimmery mix of celebrity, hope, and Korean fraternity over the Games — with the world’s media as enablers.” Kim Yo-jong flirted with the crowd at the opening ceremony of the 2018 Olympics in PyeongChang and was celebrated in the media as “a beguiling emissary” and “self-aware pageant star.” But shortly thereafter, she was described as “a twisted sister” by The Wall Street Journal, where it was reported that Kim Yo-jong is “a deputy director of the powerful and omnipresent Propaganda and Agitation Department… [where its] mission is to control not only the media but minds — to indoctrinate all North Koreans, at all levels, in the absolute supremacy of Kim Jong-un and his Workers’ Party.” And the BBC described her as “North Korea’s secret weapon … the master of her brother’s image.…" It seems that not everyone was fooled by her smile after all.

Violent Extremist Organizations (VEOs)

China and Russia have proven themselves to be quite skilled in gray zone warfare; Iran and North Korea, although becoming more skilled, have not been quite as deleterious as China and Russia have been, yet. Although its information campaign has been extremely compelling, VEOs’ gray zone operations have been limited mainly to one domain. Thus far, they have only proven themselves proficient using social media
to disseminate propaganda, generate support, and broadcast violent interpretations of Islam.

The National Security Council (NSC)

The NSC was created in the United States by the National Security Act in 1947 and appears in Section 101 of Title I, Coordination for National Security. The original role of the NSC was to promote interagency cooperation on emerging policy issues. It has evolved to “advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security.” Some Council members are required per Title 50 U.S.C §3021, others are added at the President’s discretion. On January 28, 2017, President Trump released NSPM-2, which reorganized the NSC to reflect his needs; this was superseded on April 4, 2017 by NSPM-4, which is used today.

Although there are many changes from the way former President Obama organized his NSC, the NSC/DC under President Trump remains the same as former President Obama’s and “shall continue to serve as the senior sub-Cabinet interagency forum” for national security issues. The NSC/DC is convened and chaired by the Deputy National Security Advisor. The attendees to the NSC/DC are the Deputy Secretary of State, Deputy Secretary of the Treasury, Deputy Secretary of Defense, Deputy Attorney General, Deputy Secretary of Homeland Security, Deputy Director of the Office of Management and Budget, Deputy Director of National Intelligence, Vice Chairman of the Joint Chiefs of Staff, National Security Advisor to the Vice President, Deputy National Security Advisor, Deputy Homeland Security Advisor, and
Administrator of USAID. In addition, any “Deputy Assistant to the President for the specific regional and functional issue under consideration shall also be invited to attend.”

Also pertinent are the NSC/PCCs, previously called Interagency Policy Committees, or NSC/IPCs, under former President Obama. The mission of NSC/PCCs continues to be “management of the development and implementation of national security policies by multiple executive departments and agencies” and are “the main day-to-day fora for interagency coordination of national security policies.”

Staff on the NSC typically focus on foreign and defense policy issues, crisis management, and urgent matters requiring well-considered solutions. They are not generally focused on long-term strategy. Effective national security policy is based on a measured assessment of these matters; as “international economic, banking, environmental, and health issues… [become] increasingly important to… [U.S.] national security”; however, the need for interagency coordination with NSC oversight and direction is equally imperative.

**Problem Statement**

A whole-of-government approach is needed to deny the effects of gray zone warfare undertaken by U.S. adversaries and to secure American gray zone superiority. This approach is vital in order to protect U.S. national security and to preserve American democracy.

**Developing the Approach**

In this volatile, uncertain, complex, and ambiguous environment where gray zone warfare is increasingly the norm, the United States Government must become better at defeating her adversaries using superior non-kinetic tactics. In addition, due to the
accelerating speed at which technological and social changes are occurring, it is more essential than ever that bureaucratic processes become more efficient so as to meet these rapidly emerging challenges. The United States no longer has the luxury to work in stovepipes; it is imperative that it works more collaboratively.

Currently, DOD develops gray zone strategies, engaging with other federal agencies when it deems necessary. But due to its circumscribed authorities, DOD cannot require other agencies to engage in its processes. In addition, DOD is most focused on conventional warfare. It therefore cannot also focus on all effective, non-kinetic tools available across the whole-of-government. Most importantly, leadership at DOD cannot know how or if its proposed solution conflicts with approaches being used by other federal agencies unless all those agency approaches are considered from a whole-of-government perspective. Therefore, it is recommended that whenever a U.S. federal agency believes that a U.S. Government gray zone approach is the best approach to take in response to an issue or event, it should formally request the Deputy National Security Advisor to convene a NSC/DC meeting to discuss the issue or event and propose a way forward. All NSC/DC committee members would be required to attend.

NSC/PCCs “provide policy analysis for consideration by the more senior committees of the national security system”73 and are primarily at the Assistant Secretary level. A standing NSC/PCC for Gray Zone Solutions should be developed with sub-NSC/PCCs for each component of the 4+1. Specifically, the following sub-NSC/PCCs should be developed: a sub-NSC/PCC for Russia; a sub-NSC/PCC for China; a sub-NSC/PCC for Iran; a sub-NSC/PCC for North Korea; and a sub-NSC/PCC
for VEOs. This will ensure that the appropriate subject matter experts are included in the development of gray zone solutions. The lines of effort for each sub-NSC/PCC for Gray Zone Solutions will be to identify diplomatic options, led by a Deputy Assistant Secretary of State and assisted by a Deputy Assistant Secretary of Defense; identify information opportunities, also led by a Deputy Assistant Secretary of State but assisted by a Director from U.S. Cyber Command; identify intelligence opportunities, led by the appropriate senior official from the Office of the Director of National Intelligence and assisted by a Deputy Assistant Secretary of Defense for Intelligence; identify military opportunities, led by a Deputy Assistant Secretary of Defense and assisted by the Vice Commander, U.S. Special Operations Command; identify economic and financial opportunities, led by a Deputy Assistant Secretary of the Treasury and assisted by a Deputy Assistant Secretary of the Department of Commerce; and identify law enforcement opportunities, led by the Deputy Associate Attorney General and assisted by a Deputy Assistant Secretary from the Department of Homeland Security. (See Figure 1: Proposed Whole-of-Government Approach to Gray Zone Warfare.)

Meetings of the NSC/DC are held on a regular basis. Meetings of the standing NSC/PCC for Gray Zone Solutions also will be required on a regular basis, during which prescribed tasks undertaken by the sub-PCC(s) will be assessed. Upon approval by the NSC/PCC for Gray Zone Solutions, courses of actions will be provided to the NSC/DC for review. The sub-PCC(s) may meet as often as required while developing the products that will be sent to the next NSC/PCC for Gray Zone Solutions meeting.

“The most important part of the deputies meeting is the pre-reads. This gives people the chance to prepare.”74 The day prior to each NSC/DC meeting, all NSC/PCC
for Gray Zone Solutions products must be delivered to the NSC Staff, who will compile the products into one combined book to be reviewed and discussed by members of the NSC/DC. New tasks to the NSC/PCC may be disseminated at the conclusion of each NSC/DC meeting; ultimately, a unified, whole-of-government approach to deny an adversary’s attack or a unified approach to confronting an issue will be developed.

The U.S. Army War College advocates an ends, ways, and means approach to devising strategy. In this case, the “ends” is a unified, whole-of-government approach to a gray zone issue. The “ways” is through meaningful, collaborative interagency assessment of the gray zone issue. The “means” are members of the NSC/DC, the recommended standing NSC/PCC for Gray Zone Solutions, and the recommended sub-NSC/PCCs.

There are risks to this approach, however. The intrinsic risk is that some adversaries of a large NSC worry that the bureaucratic process may take too long to develop a unified, whole-of-government approach to the problem. Advocates of a more structured, inclusive approach argue that a more solid product will emerge as the result of input from those with such diverse expertise. “One of the few ways of counteracting such homogenization is to hear from competing government agencies. There is more likelihood one will see the other's blind spots.”75 Advocates have also said, “The NSC staff’s job is to make sure that ultimately the President gets all the options, all the information, and all sides of the issue. That’s the important job that I think only the NSC can do.”76 In support of interagency meetings at the NSC/PCC level, “NSC staff should monitor progress but should never be put in actual charge of operational task forces;
placing them in charge of operations can cause the NSC staff to become treated as an ‘agency’ for various purposes, resulting in legal difficulties.”

The external risk of additional committees within the NSC is a corresponding increased risk of leaks to the media. However, there will always be those who believe the public has a right to know everything, such as Edward Snowden, the former intelligence contractor who leaked classified information to the public. The external risk of a U.S. response to a gray zone attack leaked to the public could be significant; the U.S. Government risks repercussions from both adversaries and the American public.

The risks to implementation are primarily cultural. Examples include DOD, which is accustomed to moving forward unilaterally, the CIA, which may become frustrated with having to disclose more information than it is comfortable providing, and it may seem to NSC/PCC member agencies that the Department of Justice takes an inordinate amount of time to develop a proposed solution. Nevertheless, input from a whole-of-government must be considered in order to develop the best approach to gray zone warfare. The future of U.S. democracy depends on it.

Conclusion

The Department of Defense, with assistance from other federal agencies, has historically led the gray zone war fight, the “conflict in the space between peace and war.” But history has shown that this unilateral approach is not sufficient. In fact, we have known for more than a decade that the need for a unified, whole-of-government response to gray zone attacks is needed. We can no longer ignore implementing a solid response mechanism. As such, the author recommends that U.S. federal agencies request the Deputy National Security Advisor convene a NSC/DC meeting whenever any agency deems a gray zone approach to an international issue is appropriate, and
that a standing NSC/PCC for Gray Zone Solutions be stood up, with sub-NSC/PCCs for each of our greatest adversaries, Russia, China, Iran, North Korea and VEOs, inserted underneath.

In previous crisis situations requiring coordination of whole-of-government experts, the White House has issued a Presidential Policy Directive that included the scope of the response required, the lead federal agency, guiding principles, lines of effort, and required coordination efforts. In a crisis situation requiring a gray zone response, a similar directive should be issued. In this case, all instruments of national power (diplomatic, information, military, and economic) and tools of national security policy (finance, intelligence and law enforcement) must be considered; the appropriate Deputy Assistant Secretary (or equivalent) responsible for each instrument of national power or tool of national security should be designated the lead of that line of effort with a Deputy Assistant Secretary (or equivalent) from an appropriate fellow department/agency available to assist, as described above and shown in Figure 1 of this document. Through a meaningful, collaborative interagency assessment of the gray zone issues, reconciliation of all valid opportunities developed by member sub-NSC/PCCs to ensure they do not conflict, and development of phased courses of action, the United States will defeat the adversary in gray zone warfare. As President Trump stated in the December 2017 National Security Strategy of the United States of America, “The United States will fuse our analysis of information derived from the diplomatic, information, military, and economic domains to compete more effectively on the geopolitical stage.” Through these actions, U.S. national security and American democracy will be preserved.
Figure 1: Proposed Whole-of-Government Approach to Gray Zone Warfare
Endnotes


18 Ibid.

19 Ibid.

20 Ibid.


29 Ibid.


31 Walker and Isikoff, “Sputnik, the Russian News Agency, is Under Investigation by the FBI.”


34 Ibid.


37 Ibid.


Ibid., 323.


Ibid.


Senate Armed Services Committee, Advance Questions for General Paul Selva, USAF, Nominee for Reconfirmation as Vice Chairman of the Joint Chiefs of Staff.

55 Ibid.


58 Ibid.


63 Ibid.


68 Donald J. Trump, “National Security Presidential Memorandum – 4,” memorandum for the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Agriculture, the Secretary of Health and Human Services, the Secretary of Transportation, the Secretary of Commerce, the Secretary of Energy, the Secretary of Homeland Security, the Assistant to the President and Chief of Staff, the Director of the Office of Management and Budget, the Representative of the United States to the United Nations, the United States Trade Representative, the Chairman of the Council of Economic Advisers, the Chairman of the Board of Governors of the Federal Reserve System, the Director of National Intelligence, the Director of the Central Intelligence Agency, the Chairman of the Joint Chiefs of Staff, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security and Counterterrorism the Assistant to the President for Economic Policy, the Assistant to the President for Trade and Manufacturing Policy, the Assistant to the President for Intragovernmental and Technology Initiatives, the Counsel to the President, the Deputy Assistant to the President and National Security Advisor to the Vice President, the Administrator of the United States Agency for International Development, the Administrator of the National Aeronautics and Space Administration, the Chairman of the Nuclear Regulatory Commission, the Director of the Federal Bureau of Investigation, the Director of the Office of Science and Technology Policy, the Director of National Drug Control Policy, the Chairman of the President’s Intelligence Advisory Board, the Administrator of the Federal Emergency Management Agency[, and] the Archivist of the United States, Washington, DC, April 4, 2017.

69 Ibid.

70 Ibid.

71 Ibid.


79 Donald J. Trump, National Security Strategy of the United States of America, 32.