

A WHOLE-OF-GOVERNMENT APPROACH TO GRAY ZONE WARFARE

Elizabeth G. Troeder



The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a “think factory” for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.



The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.



The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.



The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.



The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.



The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

**Strategic Studies Institute
and
U.S. Army War College Press**

**A WHOLE-OF-GOVERNMENT APPROACH TO
GRAY ZONE WARFARE**

Elizabeth G. Troeder

May 2019

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5238.

All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of certain reports may also be obtained through the U.S. Government Bookstore's website at <https://bookstore.gpo.gov>. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: <https://ssi.armywarcollege.edu/>.

The Strategic Studies Institute (SSI) is the U.S. Army's institute for geostrategic and national research and analysis. SSI supports the U.S. Army War College (USAWC) curricula, provides direct analysis for Army and Department of Defense leadership, and serves as a bridge to the wider strategic community. SSI studies are published by the USAWC Press and distributed to key strategic leaders in the Army and Department of Defense, the military educational system, Congress, the media, other think tanks and defense institutes, and major colleges and universities.

ISBN 1-58487-811-8

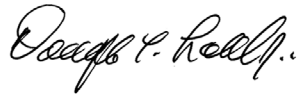
FOREWORD

Gray zone warfare has increasingly been the strategy selected by states that are determined to influence change without the risk of major escalation to outright military war. It is a significant concern today, threatening U.S. national security as well as the security of U.S. allies and partners. Although warfare is traditionally led by the Department of Defense (DoD), as the use of gray zone warfare increases and evolves, a whole-of-government approach that incorporates the unique capabilities of Federal departments and agencies for this fight is needed.

In this monograph, Ms. Elizabeth Troeder builds the case for convening a National Security Council/Deputies Committee (NSC/DC) meeting whenever any Federal agency deems a gray zone approach to an international issue is appropriate, ensuring that a whole-of-government solution is developed. She also advocates the establishment of a standing National Security Council/Policy Coordination Committee (NSC/PCC) for gray zone solutions, with sub-NSC/PCCs for each of the United States' most active adversaries so that subject matter experts from the DoD, Department of State, Department of Commerce, Department of Homeland Security, Department of Justice, Department of the Treasury, and the national intelligence community can be quickly assembled in times of crisis.

The appropriate size of the NSC has been debated for decades. Adversaries of a larger NSC argue that the bureaucratic process may take too long to develop solutions, with the potential risk of media leaks; advocates counter that a more solid product will emerge as the result of input from a wider range of expertise. In

the case of gray zone warfare, I believe it to be essential that we consider all instruments of national power as well as tools of national security policy, not just those that the DoD has available. As Ms. Troeder says, “the future of U.S. democracy depends on it.”

A handwritten signature in black ink, reading "Douglas C. Lovelace, Jr." in a cursive script.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHOR

ELIZABETH TROEDER joined the civil service as an Army Civilian in 2007. She is currently assigned to Headquarters, Army Materiel Command, in Huntsville, AL, where she is leading the Army's effort to develop and publish the Army's Organic Industrial Base Strategic Plan, which will include master planning, major equipment, energy, and funding requirements. Prior to studying at the U.S. Army War College (USAWC), she served at the Pentagon, executing special projects for the Army, supporting the preparations for the Army's Military and Construction 1-N initial project list for the fiscal year (FY) 2019-2023 Program Objective Memorandum, performing executive and operational oversight for the Army's real property accountability and audit readiness mission, and deploying twice as an Army Civilian to Afghanistan, once embedded as the basing strategist in the Combined Joint Future Plans Division of the 82d Airborne Division in Kandahar, and once to lead the Master Planning and Land Management Division in Bagram. Between deployments, she was detailed to the Army's European Infrastructure Consolidation Working Group, which was dedicated to identifying the strategy currently being executed to consolidate the U.S. Army's infrastructure in Europe. She has earned several awards including: the Non-Article 5 North Atlantic Treaty Organization Medal (2 awards), Global War on Terrorism Civilian Service Medal (2 awards), Certificate of Wartime Service in Support of Operations ENDURING FREEDOM and RESOLUTE SUPPORT, Certificate of Appreciation for Patriotic Civilian Service in Support of Operation FREEDOM'S SENTINEL, and the Commander's Award for Civilian Service (2 awards). Ms. Troeder

holds a Bachelor of Arts from Washington University, St. Louis, MO; a Master of Landscape Architecture from the University of Edinburgh; and a Master in strategic studies from the USAWC.

SUMMARY

Gray zone warfare, also known as irregular warfare, political warfare, hybrid warfare, asymmetric warfare, and unconventional warfare, is increasingly becoming the norm. It is a significant concern today, threatening U.S. national security as well as the security of U.S. allies and partners. Despite its population's immense capacity for creativity and innovation, the United States is losing this war. The Department of Defense (DoD) has historically led the gray zone war fight with assistance from other Federal agencies. However, it cannot require other agencies to engage, and it cannot be aware of all of the 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 monograph provides an assessment of the gray zone tactics used against the most active U.S. adversaries, and 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 that a standing National Security Council/Policy Coordination Committee (NSC/PCC) for gray zone solutions be developed, with sub-NSC/PCCs for each of the most active adversaries so that experts can be quickly assembled in times of crisis.

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 becoming the norm. Yet the United States is losing this war, despite its immense capacity for creativity and innovation. The February 2018 indictment of 13 Russian nationals and 3 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 the 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. However, the DoD cannot require other agencies to engage in this fight, nor can it be aware of all of the effective tools available across the whole-of-government. Most importantly, leadership at the DoD cannot know how or if its proposed solutions conflict with or potentially harm the approaches being used by other Federal agencies unless all of those agency approaches are considered from a whole-of-government perspective.

This monograph 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 the 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 (Russia, China, Iraq, North Korea, and violent extremist organizations) so that experts can be quickly assembled in times of crisis.¹ 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 been employed and are synchronized.

THE GRAY ZONE

The term “gray zone” was coined by the U.S. Army’s Special Operations Command “to describe activities, actions, or conflict in the space between peace and war.”² Commander of 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.”³ 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 Chinese military strategist Sun Tzu, the author wrote, “To subdue the enemy without fighting is the acme of skill.”⁴ In 400 B.C., Kautilya, who was an Indian advisor to the first king of the Maurya Empire and is credited with writing the political essay, *Arthashastra*, recommended the

use of secret agents, assassins, disinformation, deception, and the weakening of bonds between united adversaries to create an 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. During the Cold War, an information campaign was used both to harm the enemy and 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.⁵

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 that was commonly known as the "Children's Crusade against Communism," targeted American children in the 1950s and 1960s 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.⁶

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 on September 11, 2001, when the terrorist attacks 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.”⁷ It was a good start. Nevertheless, 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 that date 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.”⁸ The 2009 *Quadrennial Roles and Missions Review Report* stated that the DoD “supports institutionalizing whole-of-government approaches to addressing national security challenges.”⁹ 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, Director of Defense Capabilities and Management John Pendleton, in his testimony before the House Subcommittee on Oversight and Investigations, stated, “Agencies lack adequate coordination mechanisms to facilitate this collaboration during planning and execution of programs and activities.”¹⁰ 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.”¹¹ Former President Obama’s Executive Order 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 Qa’ida, and other violent extremists abroad.¹²

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.¹³

In January 2018, the 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.”¹⁴ 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.”¹⁵ The time to do so is now.

The February 2018 indictment of 13 Russian nationals and 3 Russian companies for interfering in the 2016 U.S. Presidential election provided the 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.”¹⁶ The task force also provides Trump the opportunity to heighten public awareness of outside influences engaging in gray zone warfare, undermining American democracy, and threatening 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’.”¹⁷ The term abbreviated “4+1” has endured, describing 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, U.S. Director of National Intelligence Daniel Coats 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.¹⁸

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,”¹⁹ which seeks to improve China’s economic condition throughout Asia, including the Middle East, Africa, and 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 cyber-attacks.”²⁰ Coats also added, “And North Korea will continue to use cyber operations to raise funds, launch attacks and gather intelligence against the United

States.”²¹ A deeper understanding of each is needed, as well as a call to action.

Russia

A resurgent Russia, demonstrating its aspirations 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.”²² Its “information confrontation” – or in the Russian language, “*informat-sionnoye protivoborstvo* (IPb)” – can be delineated into two forms of destabilizing informational 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.²³

The United States has no such organized campaign. As Commander, U.S. European Command General Curtis Scaparrotti said before the House Armed Services Committee in March 2017: “we are not as effective as we could be . . . particularly in the information domain.”²⁴ To mitigate this, the 2017 NSS (Pillar III) in 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.”²⁵ In addition, a Presidential Executive Order 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 the execution of the individual actions.²⁶ This issue will be discussed later in the suggested approach toward a solution.

Russian manipulation of the global information environment is rampant, causing an informational-technical effect in the cyber environment. The Fancy Bear reconnaissance program that, once downloaded, allows hackers access to an individual's computer has been linked to Russia's military intelligence agency. U.S. intelligence claims that the malware allowed hackers to breach the email account of John Podesta, the former chairman of Hillary Clinton's 2016 Presidential campaign. 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 personal equipment.²⁷ In 2016, Russian cyber-experts deliberately caused a significant power blackout in Kyiv, Ukraine, by attacking a transmission substation, which impacted electric grid operations and caused subsequent power outages throughout Ukraine; this blackout affected hospitals, banks, and transportation for more than 225,000 customers for approximately 6 hours.²⁸

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 CRASH-OVERRIDE, combined with numerous clauses found in the Military Doctrine of the Russian Federation (2014), reveal an escalation from Russian programs for reconnaissance to programs causing outright destruction. Confirmation of this concern is provided

in the Russian military doctrine known as Strategic Operations to Destroy Critical Infrastructure Targets, which “calls for escalating to deescalate” in an attempt to “un-level the playing field,” per retired General Martin Dempsey, former Chairman of the Joint Chiefs of Staff.²⁹ The doctrine refers to the use of gray zone capabilities, including the sabotage of adversaries’ energy grids as well as the 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 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.³⁰ The television network RT (formerly Russia Today) and the Russian Government-funded 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’.”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 displayed on the social media website 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.³² In February 2018,

prosecutors were able to indict 13 Russian nationals and 3 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

However, it is important to note that Deputy Attorney General Rod Rosenstein told reporters, "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 among European countries, a key objective of Russia. Moreover, "about 30 percent of the Twitter accounts that magnified the Catalan issue in Spain were registered in Venezuela but were Russian."³⁵ Again, a Catalonian 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 that minorities are being "mistreated," that there is "ethnic cleansing" of local Russian populations, and that "significant cities such as Klaipeda never belonged to Lithuania" are efforts to destabilize the European Union, the North Atlantic Treaty Organization (NATO), and the United States.³⁷ 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 obligates them 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.³⁸ 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 regarding China’s initiatives in the South China Sea—which are not necessarily consistent with international law—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.³⁹ As Prime Minister Narendra 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.”⁴⁰

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 the Permanent Court of Arbitration case number 2013-19 was brought to The Hague in The Netherlands. The findings of this landmark case refuted China's claim to sovereignty in the South China Sea; addressed Chinese interference in traditional fishing rights, which were violations of international law; and stated that China had failed to protect and preserve the marine environment, causing "irreparable damage . . . [in] the area."⁴¹ 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.⁴²

President Trump's "America First" doctrine, as well as his withdrawal of the United States from the Trans-Pacific Partnership trade deal almost immediately upon taking office in January 2017, caused further consternation among our Asian allies and partners. However, he acknowledged that freedom of navigation of the seas is imperative for the economic growth of both the United States and its Asian allies in the 2017 NSS when he stated that 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."⁴³ 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].⁴⁴

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 to protect its 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'."⁴⁵ A highlight 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.⁴⁶

The People's Liberation Army (PLA) General Staff Department, Third Department, Second Bureau (similar to the U.S. NSA) is responsible for cyberespionage 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.⁴⁷

In June 2015, *Politico* reported that Chinese hackers “breached a database containing a wealth of sensitive information from federal employees’ security background checks.”⁴⁸ 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, its allies, and its partners require unrelenting, focused attention.

Iran

Iran’s soft power strategy includes using the media, the 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.⁴⁹

In terms of cyberespionage, 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.⁵⁰

In 2016, one such invasion included an attack on 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 Iranian 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.⁵¹

During his reconfirmation as Vice Chairman of the Joint Chiefs of Staff, General Selva stated:

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.⁵²

Iran also fights a proxy war against Saudi Arabia in Yemen by supporting a Shi'ite opposition group there, provides support to President Bashar al-Assad in Syria in its fight against the Islamic State of Iraq and Syria (ISIS), and works to expand its influence in Iraq. Given its 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 Votel 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.⁵³

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.”⁵⁴

North Korea

North Korea’s state-sponsored criminal activity, which is lucrative and widespread, reaches beyond Asia into Europe and Africa. It has been characterized as money laundering, cyberwarfare, drug trafficking, and smuggling primarily to fund its weapons of mass destruction programs. A headline from a recent *Defense One* article read, “Kim’s nuclear arsenal is built to ‘deter and coerce’.”⁵⁵ 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.⁵⁶

As North Korea continued its practice, it was finally “designated a ‘primary money laundering concern’ under the Patriot Act” in 2016.⁵⁷

North Korea's cyber-activities have been ongoing 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 [italics in original].⁵⁸

Retaliatory attacks against the American film endeavor, which was considered embarrassing to Kim Jong-un, consisted of 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."⁵⁹

Since the 1970s, leadership in Pyongyang has been rewarding drug traffickers and smugglers, primarily of illegal rhino horn and ivory from Zimbabwe and Zambia, but also the traffickers and smugglers of 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.⁶⁰ 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.⁶¹

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.”⁶²

North Korea wields soft power in any way it can. Skeptics of North Korea believed that improved relations between North and South Korea, particularly in February 2018, were merely 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.⁶³

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.” However, 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.⁶⁴

The BBC described her as “North Korea’s secret weapon . . . the master of her brother’s image.”⁶⁵ It seems that not everyone was fooled by her smile after all.

Violent Extremist Organizations

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 their information campaigns have been extremely compelling, violent extremist organizations' (VEOs) gray zone operations have been limited mainly to one domain. Thus far, VEOs have only proven themselves proficient in using social media to disseminate propaganda, generate support, and broadcast violent interpretations of Islam.

The National Security Council

The NSC was created in the United States by the National Security Act of 1947 and appears in Title I, Section 101, "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.⁶⁶

NSC members are required per Title 50 U.S. Code § 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 action 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.⁶⁷ 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 the U.S. Agency for International Development. In addition, any "Deputy Assistant to the President for the specific regional and functional issue under consideration shall also be invited to attend."⁶⁸

Also pertinent are the NSC/PCCs, previously called Interagency Policy Committees, or NSC/IPC, 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." They are "the main day-to-day fora for interagency coordination of national security policies."⁶⁹

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.⁷⁰

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

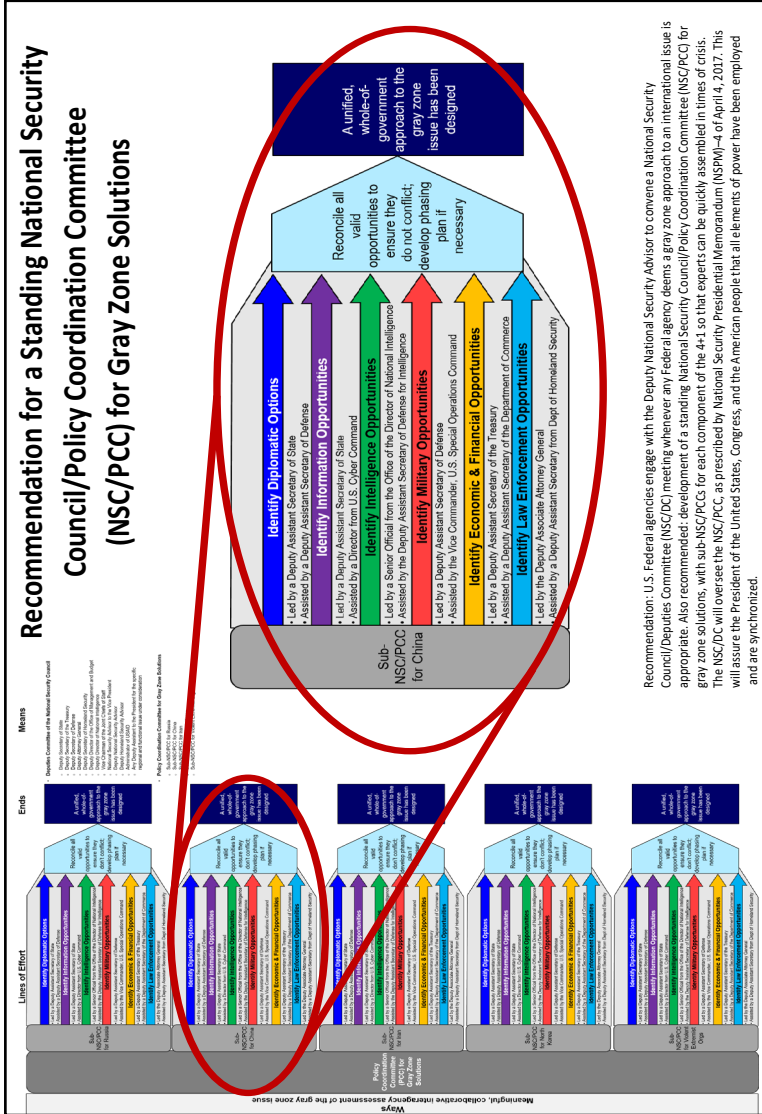
In this volatile, uncertain, complex, and ambiguous environment, where gray zone warfare is increasingly the norm, the U.S. Government must become better at defeating its adversaries using superior non-kinetic tactics. In addition, due to the accelerating speed at which technological and social changes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

Currently, the DoD develops gray zone strategies by engaging with other Federal agencies when it deems necessary. However, due to its circumscribed authorities, the DoD cannot require other agencies to engage in its processes. In addition, the DoD is more focused on conventional warfare. It, therefore, cannot also focus on all of the effective, non-kinetic tools available across the whole-of-government. Most importantly, leadership at the DoD cannot know how or if its proposed solutions conflict with approaches being used by other Federal agencies unless all of

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 an NSC/DC meeting to discuss the issue or event and propose a way forward. All NSC/DC members would be required to attend.

NSC/PCCs “provide policy analysis for consideration by the more senior committees of the national security system” and are primarily at the assistant secretary level.⁷¹ 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. These sub-NSC/PCCs would 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 would 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.)



Source: Elizabeth G. Troeder.

Figure 1. Proposed Whole-of-Government Approach to Gray Zone Warfare⁷²

Meetings of the NSC/DC are held on a regular basis. Meetings of the standing NSC/PCC for gray zone solutions would also be required on a regular basis, during which prescribed tasks undertaken by the sub-PCCs would be assessed. Upon approval by the NSC/PCC for gray zone solutions, courses of action would be provided to the NSC/DC for review. The sub-PCCs could 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’.”⁷³ The day prior to each NSC/DC meeting, all NSC/PCC for gray zone solutions products should be delivered to the NSC staff who would compile the products into one book to be reviewed and discussed by members of the NSC/DC. New tasks to the NSC/PCC could 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 would be developed.

The U.S. Army War College advocates for 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 a 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.

However, there are risks to this approach. The inherent risk is that some opponents to 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 would 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."⁷⁴ 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."⁷⁵ 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.⁷⁶

With additional committees within the NSC, there is a corresponding increased risk of leaks to the media. However, there will always be those who believe that 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 the DoD, which is accustomed to moving forward unilaterally, and the Central Intelligence Agency, which may become frustrated with having to disclose more information than it is comfortable providing. In addition, 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 the 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 DoD, with assistance from other Federal agencies, has historically led the gray zone war fight, the “conflict in the space between peace and war.”⁷⁷ However, history has shown that this unilateral approach is not sufficient. In fact, we have known for more than a decade that a unified, whole-of-government response to gray zone attacks is needed. We can no longer postpone implementing a solid response mechanism. As such, the author recommends that U.S. Federal agencies request the Deputy National Security Advisor to convene an 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, and North Korea, as well as for VEOs.

In previous crisis situations that required coordination of whole-of-government experts, the White House has issued Presidential Policy Directives 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 or agency available to assist, as described earlier and shown in figure 1. Through a meaningful, collaborative, interagency assessment of the gray zone issues, reconciliation of all valid opportunities developed by sub-NSC/PCCs to ensure that they do not conflict, and with the 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 NSS: “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.”⁷⁸ Through these actions, U.S. national security and American democracy will be preserved.

ENDNOTES

1. For a definition of the “4+1 Framework,” see Fred Dews, “Joint Chiefs Chairman Dunford on the ‘4+1 Framework’ and Meeting Transnational Threats,” *Brookings Now*, blog entry posted February 24, 2017, available from <https://www.brookings.edu/blog/brookings-now/2017/02/24/joint-chiefs-chairman-dunford-transnational-threats/>, accessed February 16, 2018.

2. “Special Forces Training: Gray Zone,” n.d., available from <http://www.specialforcestraining.info/topics/gray-zone.html>, accessed February 18, 2018.

3. Joseph L. Votel, Charles T. Cleveland, Charles T. Connett, and Will Irwin, “Unconventional Warfare in the Gray Zone,” *Joint Force Quarterly*, Vol. 80, No. 1, January 1, 2016, p. 102.

4. Sun Tzu, *The Art of War*, Samuel Griffith, trans., New York: Oxford University Press, 1963, p. 77.

5. Cecily Hilleary, "The CIA's Cultural War against Soviet Russia," *Voice of America*, April 13, 2014, available from <https://www.voanews.com/a/the-cias-cultural-war-against-soviet-russia/1890560.html>, accessed February 11, 2018.

6. Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Advancing Strategic Thought Series, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, December 2015, p. 1, available from <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303>, accessed January 24, 2018.

7. "Creation of the Department of Homeland Security," Washington, DC: Department of Homeland Security, last pub. September 24, 2015, available from <https://www.dhs.gov/creation-department-homeland-security>, accessed February 10, 2018.

8. Donald Rumsfeld, *Quadrennial Defense Review*, Washington, DC: U.S. Department of Defense, February 6, 2006, p. 85.

9. Robert M. Gates, *Quadrennial Roles and Missions Review Report*, Washington, DC: U.S. Department of Defense, January 2009, p. 31.

10. U.S. Government Accountability Office, *Testimony before the Subcommittee on Oversight and Investigations, Committee on Armed Services, House of Representatives, GAO-10-822T*, Washington, DC: U.S. Government Accountability Office, June 9, 2010, available from <https://www.gao.gov/new.items/d10822t.pdf>, accessed May 21, 2018.

11. Barack Obama, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Washington, DC: The White House, January 2012, p. 1.

12. Barack Obama, Executive Order 13721 of March 14, 2016, "Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584," Washington, DC: The White House, March 14, 2016, available from

<https://www.gpo.gov/fdsys/pkg/FR-2016-03-17/pdf/2016-06250.pdf>, accessed February 24, 2018.

13. Donald J. Trump, *National Security Strategy of the United States of America*, Washington, DC: The White House, December 2017, p. 28.

14. Mark Pomerleau, "DoD Quietly Reorganizes Cyber Command," *Fifth Domain*, January 9, 2018, available from <https://www.fifthdomain.com/dod/cybercom/2018/01/09/dod-quietly-reorganizes-cyber-command-to-shepherd-command-through-elevation/>, accessed February 3, 2018.

15. Senate Armed Services Committee, Advance Questions for General Paul Selva, USAF, Nominee for Reconfirmation as Vice Chairman of the Joint Chiefs of Staff, 115th Cong., 1st sess., July 18, 2017, available from https://www.armed-services.senate.gov/imo/media/doc/Selva_APQs_07-18-17.pdf, accessed December 21, 2017.

16. U.S. Department of Justice, *Attorney General Sessions Announces New Cybersecurity Task Force*, Washington, DC: U.S. Department of Justice, February 20, 2018.

17. Megan Eckstein, "CNO: Navy Needs More Agile Procurement to Keep Pace With '4-Plus-1' Threat Set," *USNI News*, December 7, 2015, available from <https://news.usni.org/2015/12/07/cno-navy-needs-more-agile-procurement-to-keep-pace-with-4-plus-1-threat-set>, accessed February 24, 2018.

18. Jim Garamone, "Cyber Tops List of Threats to U.S., Director of National Intelligence Says," Washington, DC: Department of Defense, February 13, 2018, available from <https://www.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligencesays/source/GovDelivery/>, accessed February 13, 2018.

19. *Ibid.*

20. *Ibid.*

21. *Ibid.*

22. U.S. Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, Washington, DC: U.S. Office of the Director of National Intelligence, January 6, 2017, p. 32.

23. Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations*, Defense Intelligence Agency, DIA-11-1704-161, Washington, DC: Defense Intelligence Agency, 2017, p. 38, available from <http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf>, accessed May 21, 2018.

24. General Curtis Scaparrotti, “EUCOM Commander Testifies before House Armed Services Committee,” linked from the U.S. European Command Public Affairs Office, March 28, 2017, available from <http://www.eucom.mil/doc/35615/eucom-commander-statements-as-delivered-to-house-armed-services-committee-mar-28-2017>, accessed January 12, 2018; “the often referred to ‘information’ domain . . . encompasses cyberspace, the electromagnetic spectrum, social media and everything in between.” Mark Pomerleau, “Information Domain Demands Major Force Structure Changes for Marines,” *Marine Corps Times*, September 22, 2017, available from <https://www.marinecorpstimes.com/c2-comms/2017/09/22/information-domain-demands-major-force-structure-changes-for-marines/>, accessed January 15, 2018.

25. Trump, *National Security Strategy of the United States of America*, p. 32.

26. The Secretary of Commerce and The Secretary of Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats—Draft for Public Comment*, Washington, DC: U.S. Department of Commerce and U.S. Department of Homeland Security, January 5, 2018, p. 4.

27. Dustin Volz and John Walcott, “Ex-U.S. NSA Employee Pleads Guilty to Taking Classified Documents,” Reuters, December 1, 2017, available from <https://www.reuters.com/article/us-usa-cyber-leaks/ex-u-s-nsa-employee-pleads-guilty-to-taking-classified-documents-idUSKBN1DV5YA>, accessed January 28, 2018.

28. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*, Hanover, MD: Dragos Incorporated, June 13, 2017, p. 3, available from <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>, accessed January 15, 2018.

29. General Martin Dempsey, interview by Peter Feaver, Durham, NC: Duke University, April 11, 2016, available from <http://livinghistory.sanford.duke.edu/interviews/martin-dempsey/>, accessed February 18, 2018.

30. Hunter Walker and Michael Isikoff, "Sputnik, the Russian News Agency, is Under Investigation by the FBI," *HuffPost*, September 11, 2017, available from https://www.huffingtonpost.com/entry/sputnik-the-russian-news-agency-is-under-investigation-by-the-fbi_us_59b6b453e4b036fd85cccc61, accessed January 14, 2018.

31. *Ibid.*

32. Nash Jenkins, "Investigators Say Russia Is Still Trying to Interfere in U.S. Politics," *Time*, October 4, 2017, available from <http://time.com/4969304/russia-election-interference-collusion-congress/>, accessed January 14, 2018.

33. David Voreacos and Steven T. Dennis, "Mueller Accuses Russians of Pro-Trump, Anti-Clinton Meddling," *Bloomberg*, February 16, 2018, available from <https://www.bloomberg.com/news/articles/2018-02-16/u-s-charges-13-russians-3-companies-for-hacking-election>, accessed February 18, 2018.

34. *Ibid.*

35. Stephen Blank, "We have no counterattack to Russia's information warfare," *The Hill*, November 27, 2017, available from <http://thehill.com/opinion/international/361897-we-have-no-counterattack-to-russias-information-warfare>, accessed January 15, 2018.

36. Christopher Woody, "Baltic States Think Russia Is Laying the Groundwork for Looming 'Kinetic Operations'," *Business Insider*, April 3, 2017, available from <http://www.businessinsider.com/russia-propaganda-in-lithuania-attack-on-the-baltics-2017-4>, accessed January 31, 2018.

37. Ibid.

38. "Statement to the House Foreign Affairs Committee on the FY 2018 Budget Request," June 14, 2017, Testimony by Rex Tillerson, Secretary of State, available from <http://docs.house.gov/meetings/FA/FA00/20170614/106115/HHRG-115-FA00-Wstate-TillersonR-20170614.pdf>, accessed November 15, 2017.

39. *The Asia-Pacific Maritime Security Strategy: Achieving U.S. National Security Objectives in a Changing Environment*, Washington, DC: Department of Defense, July 27, 2015, p. 6.

40. "Remarks by Secretary Mattis at Shangri-La Dialogue," News Transcript, Washington, DC: U.S. Department of Defense, June 3, 2017, available from <https://www.defense.gov/News/Transcripts/Transcript-View/Article/1201780/>, accessed November 15, 2017.

41. Thomas A. Mensah, *In the Matter of the South China Sea Arbitration*, July 12, 2016, pp. 319, 323, available from <http://www.pcacases.com/pcadocs/PH-CN%20-%2020160712%20-%20Award.pdf>, accessed March 20, 2018.

42. Jane Perlez, "Tribunal Rejects Beijing's Claims in South China Sea," *The New York Times*, July 12, 2016, available from <https://www.nytimes.com/2016/07/13/world/asia/south-china-sea-hague-ruling-philippines.html>, accessed March 20, 2018.

43. Trump, *National Security Strategy of the United States of America*, p. 46.

44. "Mike Pence Hints at Possible US Return to TPP in Talks with Japan DPM Aso: Kyodo," *The Straits Times*, February 8, 2018, available from <http://www.straitstimes.com/asia/east-asia/pence-hints-at-possible-us-return-to-tpp-in-talks-with-aso-kyodo>, accessed February 18, 2018.

45. "Hu Calls for Enhancing 'Soft Power' of Chinese Culture," *Xinhua News Agency*, October 15, 2007, available from <http://www.china.org.cn/english/congress/228142.htm>, accessed February 13, 2018.

46. Ibid.

47. Adam Segal, "How China is preparing for cyberwar," *The Christian Science Monitor*, March 20, 2017, available from <https://www.csmonitor.com/layout/set/print/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar>, accessed March 20, 2018.

48. David Perera and Joseph Marks, "Newly Disclosed Hack Got 'Crown Jewels'," *Politico*, updated June 17, 2015, available from <https://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954>, accessed March 20, 2018.

49. U.S. Department of Justice, "Acting Assistant Attorney General Mary B. McCord for National Security Delivers Keynote Remarks at Second Annual Billington International Cybersecurity Summit Dinner," Washington, DC, March 29, 2017, available from <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mary-b-mccord-national-security-delivers-keynote>, accessed March 3, 2018.

50. Dorothy Denning, "Iran's Cyber Warfare Program is Now a Major Threat to the United States," *Newsweek*, December 12, 2017, available from <http://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427>, accessed March 3, 2018.

51. Ahmad Majidiyar, "Iran's Soft Power: Islamic Azad University Opening Branches in Major Syrian and Iraqi Cities," January 17, 2018, available from <http://www.mei.edu/content/article/io/iran-s-soft-power-islamic-azad-university-opening-branches-major-syrian-and-iraqi-cities>, accessed February 18, 2018.

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

53. Joseph L. Votel, *The Posture of U.S. Central Command: Terrorism and Iran: Defense Challenges in the Middle East*, Posture Statement presented to the House Armed Services Committee, Washington, DC: U.S. House of Representatives, February 27, 2018, p. 27, available from <http://docs.house.gov/meetings/AS/AS00/20180227/106870/HHRG-115-AS00-Wstate-VotelJ-20180227.pdf>, accessed March 3, 2018.

54. Ibid.

55. Patrick McEachern, "Expect North Korea to Add Nuclear Coercion to Its Provocation Playbook," *Defense One*, March 5, 2018, available from http://www.defenseone.com/ideas/2018/03/expect-changes-pyongyangs-provocation-playbook/146411/?oref=driver&utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%203/6/18&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief, accessed March 6, 2018.

56. Laura Koran and Jose Pagliery, "US Treasury Cracks Down on North Korea's Money Laundering," *CNN*, June 6, 2016, available from <http://money.cnn.com/2016/06/01/news/north-korea-money-laundering/index.html>, accessed March 3, 2018.

57. Ibid.

58. Gabriel Sanchez, *Case Study: Critical Controls that Sony Should Have Implemented*, North Bethesda, MD: Sans Institute, SANS Institute Reading Room, June 1, 2015, p. 2, available from <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022>, accessed March 3, 2018.

59. U.S. Department of Justice, "Acting Assistant Attorney General Mary B. McCord for National Security Delivers Keynote Remarks at Second Annual Billington International Cybersecurity Summit Dinner."

60. *The Global Initiative against Transnational Organized Crime, Diplomats and Deceit: North Korea's Criminal Activities in Africa*, Commissioned Report, Geneva, Switzerland: The Global Initiative against Transnational Organized Crime, September 2017, p. 63, available from https://conservationaction.co.za/wp-content/uploads/2017/09/TGIATOC_Diplomats_and_Deceit_DPRK_Report_1868_web_pdf, accessed March 3, 2018.

61. "N. Korean Diplomats 'Sell Millions of Dollars Worth of Drugs'," *Chosun Ilbo*, March 20, 2013, available from http://english.chosun.com/site/data/html_dir/2013/03/20/2013032001084.html, accessed March 3, 2018.

62. Ibid.

63. Donald M. Bishop, "The Three Spectacles of Pyeong-Chang," *The Hill*, February 21, 2018, available from <http://thehill.com/opinion/international/374662-the-three-spectacles-of-pyeongchang>, accessed March 6, 2018.

64. Claudia Rosett, "Kim Yo Jong Is a Twisted Sister," *The Wall Street Journal*, February 13, 2018, available from <https://www.wsj.com/articles/kim-yo-jong-is-a-twisted-sister-1518564481>, accessed March 3, 2018.

65. Laura Bicker, "Kim Yo-jong and North Korea's Secret Weapon," BBC News, February 13, 2018, available from <http://www.bbc.com/news/world-asia-42984960>, accessed March 3, 2018.

66. National Security Act of 1947, Public Law 235, July 26, 1947, 61 STAT. 496, available from <https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947>, accessed May 21, 2018.

67. Donald J. Trump, "National Security Presidential Memorandum-4: Organization of the National Security Council, the Homeland Security Council, and the Subcommittees, April 4, 2017," Washington, DC: The Government Printing Office, April 4, 2017.

68. Ibid.

69. Ibid.

70. Richard A. Best, Jr., *National Security Council: An Organizational Assessment*, Washington, DC: Congressional Research Service Report for Congress, 2009, p. 26.

71. Trump, National Security Presidential Memorandum-4.

72. Image created by author.

73. Kori Schake and William F. Wechsler, "Process Makes Perfect: Best Practices in the Art of National Security Policymaking," Washington, DC: Center for American Progress, January 5, 2017, available from <https://www.americanprogress.org/issues/security/reports/2017/01/05/295673/process-makes-perfect/>, accessed March 5, 2018.

74. "Security, not bureaucracy," *The Ottawa Citizen*, June 8, 2002, p. B6.

75. Schake and Wechsler.

76. Kim Holmes, "Memo to a New President: How Best to Organize the National Security Council," *Backgrounder*, No. 3098, Washington, DC: The Heritage Foundation, April 14, 2016, p. 12, available from <https://www.heritage.org/defense/report/memo-new-president-how-best-organize-the-national-security-council>, accessed March 5, 2018.

77. "Special Forces Training: Gray Zone."

78. Trump, *National Security Strategy of the United States of America*, p. 32.

U.S. ARMY WAR COLLEGE

**Major General John S. Kem
Commandant**

**STRATEGIC STUDIES INSTITUTE
AND
U.S. ARMY WAR COLLEGE PRESS**

**Director
Professor Douglas C. Lovelace, Jr.**

**Director of Research
Dr. Steven K. Metz**

**Author
Ms. Elizabeth G. Troeder**

**Publications Assistant
Ms. Denise J. Kersting**

**Composition
Mrs. Jennifer E. Nevil**



U.S. ARMY



FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
<https://www.armywarcollege.edu/>

ISBN 1-58487-811-8



9 781584 878117

9 0000 >



This Publication



SSI Website



USAWC Website