SUMMER STUDY ON

CAPABILITIES FOR CONSTRAINED MILITARY OPERATIONS

DECEMBER 2016

This page intentionally blank

REPORT OF THE DEFENSE SCIENCE BOARD

SUMMER STUDY ON
Capabilities for
Constrained Military Operations

December 2016

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE BOARD

December 28, 2016

MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS

SUBJECT: Final Report of the Defense Science Board (DSB) Summer Study on Capabilities for Constrained Military Operations

I am pleased to forward the final report of the DSB Summer Study on Capabilities for Constrained Military Operations. This report offers important recommendations on how the Department can respond to regional conflicts that remain below the threshold of full-scale warfare, called constrained military operations.

This study is unique in not only describing the character and implications of so-called gray zone conflicts but also offering a comprehensive agenda of actionable recommendations for the U.S. to address such conflicts. This report proposes whole-of-government concepts and Department of Defense information systems and physical capabilities that have the potential to provide responses to constrained military operations. The recommendations do not require significant investments, but do require a shift in mindset within The DoD to successfully confront constrained military operations. As the report explains, The DoD may not always have the lead role in responding, but the Department does have significant capabilities to support whole-of-government approaches.

The good news is that The DoD can prevail with inexpensive capabilities that have low technology risk and accomplish all of this on a short timeline.

I fully endorse all of the recommendations contained in this report and urge their careful consideration and soonest adoption.

Chairman

December 28, 2016

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board Summer Study on Capabilities for
Constrained Military Operations

The final report of the Defense Science Board Summer Study on Capabilities for Constrained
Military Operations is attached. In accordance with its charter, the Study focused on regional
conflicts that remain below the threshold of full-scale warfare, called constrained military
operations. This study is unique in not only describing the character and implications of so-
called gray zone conflicts but also offering a comprehensive agenda of actionable
recommendations for the U.S. to address such conflicts. The good news is that The DoD can
prevail with inexpensive capabilities that have low technology risk and on a short timeline. The
Study analyzed planning and assessment processes; information, intelligence, and cyber
capabilities; physical capabilities; and interagency capabilities where The DoD provides a
supporting role. While the Study reviewed technologies, capabilities, operating concepts, and
processes to provide responses to constrained military operations, they also reviewed the need
for a strategic framework to provide guidance for any future actions.

The Study took a three-pronged approach to countering potential adversaries' strategies for
waging long-term campaigns for constrained military operations and Gray Zone conflicts:

1. Create a long-term strategic framework and threat-oriented campaigns.
2. Exploit the new and evolving information landscape.
3. Continue to add to the available set of tools applicable to operations addressing less than
full-scale conventional warfare.

The Study concluded that much of the Department's actions for constrained military operations
and Gray Zone conflicts were reactive and episodic. The creation of a long-term strategy to
counter adversaries' activities and to proactively advance national interests should be a first and
important priority for department leadership. The Study recommends that the Secretary of
Defense charter and staff a DoD Strategic Options Task Force with the objective of creating a
strategic framework, campaigns, and playbooks aimed at providing both reactive and proactive
actions to deter and counter adversaries' potential constrained military operations. Important to
be considered by the DoD Strategic Options Task Force is the role and integration of allied
actions into interagency and DoD strategy and campaigns. The roles of allies in military,
diplomatic, economic, and societal activities must be considered to create an enduring U.S.
strategy.

A new and critical element of Gray Zone operations is the importance of the information landscape in both understanding adversaries' actions and prosecuting U.S. and allied campaigns. New sources of information derived from social media, the Internet of Things (IoT) and advanced data analytical methods must be integrated with conventional intelligence to effectively prosecute Gray Zone information operations. The information needs to prosecute an information campaign are different than those required for conventional military operations.

The Study emphasizes the need to accelerate the collection and exploitation of open source information and apply this information to cyber information campaigns for supporting and waging constrained military operations.

The Study also found that The DoD needs to determine the enabling capabilities, or toolbox, necessary to prosecute constrained military campaigns. The ability to control escalation is an important consideration. The toolbox will need to include tools that are flexible and reversible. As has been done in the past, clandestine, covert, and deniable tools are important in the Gray Zone as the U.S. and its partners often bring differing societal policy restrictions to such operations. Therefore, building partner capacity should be emphasized since working in concert with partners has proven to be more effective than the U.S. operating alone. The Study found that many capabilities exist and are ready for procurement. Achieving coordinated interagency and allied effects is a difficult and important determinant of success and the creation of playbooks by the DoD Strategic Options Task Force that shape this activity will assist in achieving this required coordination.

The Study believes that all the recommendations contained in this report are important for ensuring the Department is capable of effectively responding to constrained military operations.

Mr. Vincent Vitto
Study Co-Chair

General Michael Carns, USAF, Retired
Study Co-Chair

Executive Summary

Today, the United States is engaged in a global competition with emerging and resurgent global powers, aspiring regional hegemons, and non-state actors seeking to undermine aspects of the post-World War II international order. The challenges of this era seem more pressing than those of the recent past, due to the global scope of American interests, the proliferation of disruptive capabilities, and the increasing access to information, both real and false, of an interconnected world. By traditional measurements the world is more stable today than ever before, but those metrics obscure a trend of increasing belligerence among actors vying for position in a zero-sum competition for influence. The political activities of strategic competitors like China and Russia, regional powers like Iran and North Korea, and non-state actors like the Islamic State of Iraq and the Levant (ISIL) and Hezbollah garner coverage in news outlets across the world, but rarely do their actions warrant full-scale military responses or elicit any sense of urgency or alarm. These actions are unlike headlines from the 20th century that conveyed the pursuit of national interests through armed conflict. Nonetheless, today's actors engage in well-conceived and highly deliberate campaigns to advance their core interests, often at the expense of American influence and to the detriment of long-term U.S. and Department of Defense (DoD) interests.

In November 2015, the Under Secretary for Acquisition, Technology, and Logistics (USD(AT&L)) requested that the Defense Science Board (DSB) explore U.S. capabilities to protect its interests early before hostilities begin and to deter aggression with the objective of minimum loss of life and infrastructure using shaping techniques, massive information collection and assessment, autonomous, and non-lethal capabilities. These actions, defined in this study as Constrained Military Operations (CMO), are military activities that address threats to U.S. interests abroad and stability in critical regions of the world that are not existential challenges to the United States and do not rise to the level of full-scale military operations. With this charter, the Study assessed DoD capabilities for planning, shaping, and carrying out operational activities in constrained military operations; identified information needed to determine threat capabilities; identified the required capabilities to collect that information; identified the tools currently held by the DoD; identified the tools that the DoD needs to develop or acquire to provide strategic warning and threat analysis, and to respond to CMO; and examined the existing government and commercial capabilities that the DoD can repurpose for CMO.

The Study found that the U.S. already has significant competitive advantages that can be exploited for constrained military operations. To effectively leverage its competitive advantages, though, the U.S. requires a global strategic framework, rapid access to information, a proactive information campaign, upgraded tools, and a whole-of-government perspective. Failure to compete effectively in constrained military operations will have consequences, such as the erosion of national interests and influence, undesired escalation of conflicts, and the loss of allied support.

This study is unique in not only describing the character and implications of so-called gray zone conflicts but also offering a comprehensive agenda of actionable recommendations for the U.S. to address such conflicts. This report proposes whole-of-government concepts and Department of Defense information systems and physical capabilities that have the potential to provide responses to constrained military operations. The recommendations do not require significant investments, but do require a shift in mindset within the DoD to successfully confront constrained military operations. As the report explains, the DoD may not always have the lead role in responding, but the Department does have significant capabilities to support whole-of-government approaches. The recommendations in this report will allow the U.S. to address and respond to these conflicts with inexpensive capabilities that have low technology risk and accomplish all of this on a short timeline.

Introduction

Touching virtually every corner of the globe, America's global interests intersect, to varying degrees, with those of every state and non-state actor. These interactions sometimes align to foster collaboration, but diverge in others to underscore long-term competitions that characterize today's strategic environment. America's competitors, for example, perceive America as encroaching upon their historic spheres of influence and threatening the security of their core interests. Likewise, regional powers, long subject to the political will of various imperial powers and more recently the reach of American influence, seek to exploit any opportunity to advance their own national interests. Unable to compete with the conventional military and economic might of the United States, many of America's competitors and potential adversaries are forced to compete using combinations of alternative and asymmetric ways and means. These competitors apply age-old techniques, enabled by modern technology, and underwritten by unique, non-Western strategic cultures to pursue their national interests. These strategic campaigns do not directly threaten American or allied lives and property, or the wealth of their citizens, thus avoiding thresholds that trigger an immediate response and often lead to the unwitting acceptance of the United States. Yet, America's competitors position themselves to secure their long-term, core interests, oftentimes at the expense of American interests and the international order that the U.S. has upheld for more than seven decades. Most U.S. allies, particularly Western allies, are equally sanguine about the ultimate objectives of U.S. competitors' strategic campaigns. It is only when the U.S. and its partners and allies are faced with conventional military effects—masses of tanks or operating radii of destroyers and aircraft, for example—that the deliberate strategic campaigns of these competitors are identified as efforts to project the application of national power in non-traditional domains.

Growing Chinese assertiveness in East and Central Asia and the western Pacific, a resurgent Russia seeking to restore influence in its near abroad, and increasing belligerence of Iran and North Korea highlight the expanding scope and capabilities of U.S. competitors. The United States must not, however, lose sight of its existing sources of competitive advantage. They are significant and should underpin a long-term competitive strategy to protect and advance American interests. America

retains a qualitative edge by leveraging the talent of its citizens to drive innovation and technology in an open society. Also, the ethnic and religious diversity of the United States represents a society unique to the world that appeals to universal aspirations.

In the quarter-century of U.S. primacy following the end of the Cold War, the U.S. faced no "existential" threat on par with that it had faced for more than four decades. Absent a peer competitor, the United States enjoyed its "unipolar moment" and pursued interpretations of its national interests that led to the commitment of large amounts of resources for non-vital interests. Without serious challenges to its role as global hegemon, there was little need to prioritize resources in a long-term competitive strategy. Instead, the United States wielded its national power in various conflicts and engagements, generally acting with constraint due to weak adversaries and limited political will. Regardless of the political ends for each of these engagements, a psychological effect on the American people, of the U.S.'s unipolar power, has been a myopia that prevents a broader view of world events that indicate the enduring nature of competition among states. Throughout history, periods of unipolar power are rare exceptions that are always short-lived. The pace of China's rise and the resurgence of Russia over the past five years took the United States by surprise, not because of the success enjoyed by both Beijing and Moscow in their deliberate campaigns for influence, but because of the methods for achieving their campaigns. What many in the U.S. read as individual episodes of belligerence has, in fact, been components of long-term competitive strategies that fall far below any threshold for a unified, resolute American response. Swarms of Chinese fishing fleets overwhelming Vietnamese coast guard vessels in the South China Sea or companies of "little green men" seizing key pieces of terrain in Ukraine do not conform to American conceptions of military power. Further, state-planned misinformation campaigns and economic subversion are not considered acts of war by a large percentage of the American public, even if these actions have allowed China and Russia to advance their national interests at the expense of the United States. These kinetic and non-kinetic actions represent a new model of conflict, not yet war, but not quite peace. The term of art among government officials and defense analysts today is "Gray Zone conflict," but is also termed constrained military operations in this report.

Strategic Framework and Interagency Coordination

Today, U.S. policies are ill-suited to address its competitors and potential adversaries' current approach to achieving their strategic goals. Competitors of the U.S. have identified their long-term strategic interests, and have made a careful study of the U.S. These competitors have developed a deep understanding of the U.S.'s approach to warfare and the current boundaries governing American actions. Competitors of the U.S. understand that, to date, the U.S. has limited its responses and, by testing the waters, competitors to the U.S. have concluded they can push their objectives, even when violating international norms, by staying just below the threshold that triggers armed conflict. America's competitors and potential adversaries have identified, and are remaining within, a Gray Zone.

In many ways, the approaches pursued by competitors and potential adversaries are a tribute to the U.S.' success at conventional deterrence. The capabilities developed by the U.S. to counter conventional aggression has sent a message to all potential adversaries that going against the United States in armed conflict is a risky proposition. So, in a sense, the U.S. has driven its competitors into a Gray Zone for pursuing their objectives. America's challenge, now, is to extend its effectiveness in conventional deterrence into the Gray Zone. This will require a reevaluation of policies and planning processes to support developing new capabilities that will be effective for constrained military operations.

The Gray Zone is a challenging place for the DoD, since the U.S. tends to treat each incursion as a discrete event and then ask if that event is a threat to American strategic national interests. The answer so far has consistently been "no" and that is no coincidence. America's competitors and potential adversaries are making a calculation that the U.S. will not be willing to make a significant response to their actions. Even more so, these competitors are designing their actions to ensure that the U.S. will not respond in a significant way. The question to be asked is: What is the cumulative effect of these actions and what should the U.S. do about it?

Even more challenging for the DoD is the fact that many of the tools needed to engage in the Gray Zone are not tools that can be exclusively wielded by the DoD. Success in the Gray Zone requires a whole-of-government approach, leveraging all the tools available to the nation vice just the military.

The DoD needs a strategic framework that provides the U.S. with the same kind of overarching perspective that the U.S. perceives its competitors have developed. Ideally, this would be a national framework based on an understanding of competitor goals and objectives and that organizes all elements of government into a coordinated response. The DoD would then develop global campaign plans, in partnership with other agencies, to meet the objectives of the strategic framework.

However, today's events make it increasingly clear that the DoD cannot afford to sit and wait for a national strategic framework. In the absence of such a framework, the DoD must draft one for higher level consideration and then, based on that draft, push forward in concert with interagency partners to develop global campaign plans for responding to Gray Zone conflicts.

A Strategic Framework

One of the foundational documents of the U.S. response to the Cold War, National Security Council (NSC) Report 68, was also one of the most the important examples of interagency coordination under the National Security Act of 1947. NSC 68 set forth the U.S. core policy assumptions and objectives that formed the underpinnings of bi-partisan management of the U.S. policy response to Soviet-American Cold War competition over four decades and nine presidential administrations.

After considering a number of courses of action and desired outcomes, NSC 68 recommended a rapid build-up of the political, economic, and military strength of the Free World. This recommendation reflected a deep understanding of the historical and ideological roots of the Soviet Union's foreign

policy that permitted the U.S. national security leadership to anticipate rather than respond to Soviet initiatives that challenged the security interests of the U.S. and its allies.

In today's strategic environment, the United States needs a strategic framework to guide whole-of-government actions for constrained military operations. As in the past, the development of a strategic framework will be initiated by postulating the U.S.'s desired outcomes, and the alternative sets of outcomes to be considered. By specifying the desired outcomes, the U.S. can identify the courses of action to produce those results, as well as identify the pros and cons of each option.

A strategic framework will guide the whole-of-government actions for all government agencies. The important challenges the United States faces are not exclusively military in their character, and often not best addressed by military actions. Military actions may be critical, but only provide necessary, but not sufficient, conditions for success. A strategic framework can identify whole-of-government actions—the implicit or explicit authorities to act—to drive action. A strategic framework will help the Nation to develop the incentives to produce necessary actions by the U.S. Government. A strategic framework will also help drive collaboration with allied governments and non-government organizations. A key role of strategic frameworks is to identify capabilities and adjust resources accordingly. Current capabilities that fail to contribute will be identified, and those resources can then be devoted to the newly identified capabilities or higher priority needs.

Perhaps most important, a strategic framework provides the context within which to gauge the effectiveness of the chosen course of actions towards the desired outcomes. Questions to be asked include:

- Is the U.S., in fact, making progress against those goals, not just progress in implementing selected policies?
- Is the U.S. losing ground in such a way that selected courses of action should re-evaluated?
- Is a debate on a new set of goals in order, either because the original agenda has been achieved, or because a fresh set of different challenges now confronts the nation?

A strategic framework, preferably developed at the National Security Council as NSC XX, is required to drive a whole-of-government response to Gray Zone challenges. With a framework in place, each component of government has a clear directive for developing campaign plans. As the framework evolves to address unanticipated adversaries or new information about previously identified adversaries, individual agency plans can also evolve.

The process to develop a strategic framework begins by defining U.S. national interests and strategic objectives. Importantly, the process is based on an assessment of U.S. competitors' and potential adversaries' intentions. The strategic framework then outlines actions to defeat threats and achieve desired outcomes. This understanding will allow U.S. policymakers to anticipate developments and threats to national interests and preclude them. Leveraging the capabilities and tools available to the entire government to implement the strategic framework is critical to achieving national interests.

Based on the tools available, a strategic framework will identify desired outcomes, potential courses of action, and the strengths and weaknesses of each option in order to determine future actions.

Recommendation 1: Develop a strategic framework and campaign plan

The United States needs a global strategic framework to counter competitors who operate in a long-term campaign mode. The Secretary of Defense (SECDEF), with his Cabinet colleagues, should recommend that such a framework (NSC XX) be developed. The goal should be an enduring, effective, and adaptable framework that can guide government agencies, and interactions with allies, for decades to come.

Although prompted in significant part by competitor Gray Zone activities, the strategic framework should not focus on Gray Zone conflicts in isolation. A wider strategic context is essential.

The DoD and its interagency partners should not wait for NSC XX to start this essential work. The Department should immediately draft a candidate strategic framework in conjunction with its interagency partners.

Recommendation 2: Create a DoD Strategic Options Task Force

To develop the above framework and associated campaign plans, the SECDEF should assemble a small group of the "best minds" broadly representative of the interagency community. This group could be a DoD Strategic Options Task Force, reporting directly to the SECDEF. The DoD Strategic Options Task Force should consist of a small number of senior officials drawn from the Department of Defense, including the Joint Chiefs of Staff (JCS), Office of the Secretary of Defense (OSD), and Combatant Commands (CCMDs); the Intelligence Community (IC); and other federal departments responsible for non-military instruments of national power and influence, such as the Department of State, Department of Treasury, and the United States Trade Representative (USTR).

The Task Force's priorities will evolve over time in response to the SECDEF's authority and direction but should begin with the development of a candidate strategic plan. The Task Force, in coordination with CCMDs and JCS, would then help the DoD develop campaign plans, Operational Plans (OPLANs), and associated playbooks to proactively deal with competitors operating in, but not limited to, Gray Zone conflicts. Similarly, interagency partners and allies would be encouraged to develop campaign plans with the strategic framework as guidance. The DoD Strategic Options Task Force would assist interagency partners as appropriate. The emphasis should be on developing a full suite of integrated steps that different parts of the U.S. Government should consider to shape and constrain these competitors wherever and whenever they contemplate or take aggressive actions against U.S. interests.

Task Force members would serve at the SECDEF's pleasure and must have a demonstrated track record analyzing geopolitical, international economic, and/or military trends, as well as experience in developing coherent strategies of action. They must be able to think strategically and creatively. It is likely that the Task Force will not include all the required expertise and thus must have the flexibility to tap outside subject matter experts (SMEs), when needed.

Interagency and IC reps will be critical for understanding the background and context of the topics and issues that are considered.

The strategies and general guidance recommended by the DoD Strategic Options Task Force would lead to SECDEF decisions, with specific tasks by the CCMDs as directed by the President and the Secretary.

Recommendation 3:   New assessment tools are required

Developing and implementing the strategic framework, campaign plans, OPLANs, and associated playbooks will depend on effective analytic support. Fortunately, the DoD enjoys access to a robust set of analytical and assessment capabilities. Nonetheless, some new approaches will be required to adapt to the problems posed by Gray Zone conflicts and constrained military operations. Current DoD analysis in support of planning and capability development predominantly focuses on traditional military conflict.

While some of these approaches will remain relevant to Gray Zone conflicts and constrained military operations planning, assessments will also need to:

- ♦ Incorporate non-military factors;
- ♦ Evaluate the effectiveness of non-military tools;
- ♦ Address competitive behavior short of conflict in political, economic, and information realms; and
- ♦ Address longer-term trends and effects of U.S., allied and competitor actions.

Leveraging Information and Intelligence

The information sphere has two distinct characteristics as a supporting functional domain and is also a battlespace. As a "functional" domain that provides essential support for the other levers of power, information provides indications and warning (I&W), situational awareness (SA), targeting, and battle damage assessment (BDA). On the other hand, information is also a direct lever of power and, in this sense, information is a battlespace. In the information battlespace, proactive messaging is carried out, with the goal of shaping the opinions, beliefs, and, ultimately, actions of individuals, organizations, and governments. Such messaging is used in systematic propaganda campaigns, mixing fact and fiction to further their desired goals. The information battlespace also includes cyber actions that

target information sources; and, in overlap with the physical sphere, cyber actions can target material objects to result in physical effects.

Information is an especially important sphere for Gray Zone operations for several reasons. As described earlier, Gray Zone operations are enduring, so there is ample time to observe their effects. Many near- and long-term results are overt, rather than covert (although deception and denial are often in play). Gray Zone operations often impact populations or individuals, who may speak openly about their experiences and observations. Thus, Gray Zone campaigns leave a long trail of easily observable footprints. This makes open-source information especially important in Gray Zone operations.

In addition, the information battlespace is critical to the U.S. as it seeks to counter Gray Zone operations of competitors and potential adversaries. These potential adversaries choose to operate in the Gray Zone to achieve their objectives without triggering a major military confrontation with the U.S. Competitors and potential adversaries understand that the U.S. has a very high threshold for the use of physical force because of American cultural values, domestic politics, legal constraints, and, increasingly, a national weariness with overseas conflict. So, potential adversaries tailor their Gray Zone actions with the goal of diminishing the value of American physical levers of power. As the physical sphere is diminished in Gray Zone conflicts, compared to major combat operations, the information sphere becomes more important. This is not simply because of the large information footprint described above. It is also because the reluctance to engage in physical actions need not apply in the information battlespace. Indeed, potential adversaries are already actively engaged in this battlespace. While the U.S. does not want to mirror their methods, which include tactics at odds with U.S. values, there is untapped opportunity for a proactive U.S. engagement in this information domain, in which the cultural, policy, and legal barriers to entry are much lower.

The types of information important in Gray Zone campaigns are different from those needed for combat operations and include whether to understand an adversary's campaign, or to conduct a proactive U.S. campaign. Defeating nation-state adversaries in head-to-head combat requires a focus on traditional military power, such as order of battle, military strategies and plans, doctrine, tactics, training, exercises, changes in military posture, etc. Thus, the intelligence community's apparatus and expertise during the Cold War was tuned to understanding adversarial military forces. Subsequently, the attention of the national security community shifted to defeating global terrorism, and in response, the intelligence community developed the tools and expertise for a more robust understanding of non-military entities, specifically, for understanding terrorists, their networks, and their exploitation of non-military, civilian, infrastructure. This expertise provides a foundation to meet the information needs for Gray Zone campaigns, but it requires further evolution including special attention to the exploitation of open source information.

In Gray Zone campaigns, necessary interest falls into three distinct categories beyond traditional military entities that include: individuals, society, and an adversary's campaign as executed outside of traditional military means. The same categories of information are required regardless of whether the

U.S. needs to understand and thwart a Gray Zone campaign against an ally, or to understand the most effective means to wage a U.S. campaign against an adversary.

Open Source Information

The world-wide proliferation of the smart phone has provided a low-cost network appliance for accessing social media sites, collecting and sharing pictures, and enabling peer-to-peer gaming across the globe. This exponential growth in the adoption of hand-held, multi-function computing and communication devices has also helped the growth of social sites like Facebook, YouTube, and Twitter, to name a few. Today, the number of mobile social media users has reached just under two billion globally, or about twenty-seven percent of the global population. The mobile social media adoption rate by country presented in Exhibit 1 shows a high of fifty-two percent for North America and a low of four percent for Central Asia. The annual growth for social media users is expected to continue to grow at ten percent per year.

ACTIVE ACCOUNTS ON THE TOP SOCIAL NETWORK IN EACH COUNTRY ACCESS VIA MOBILE, COMPARED TO POPULATION (JAN 2016)
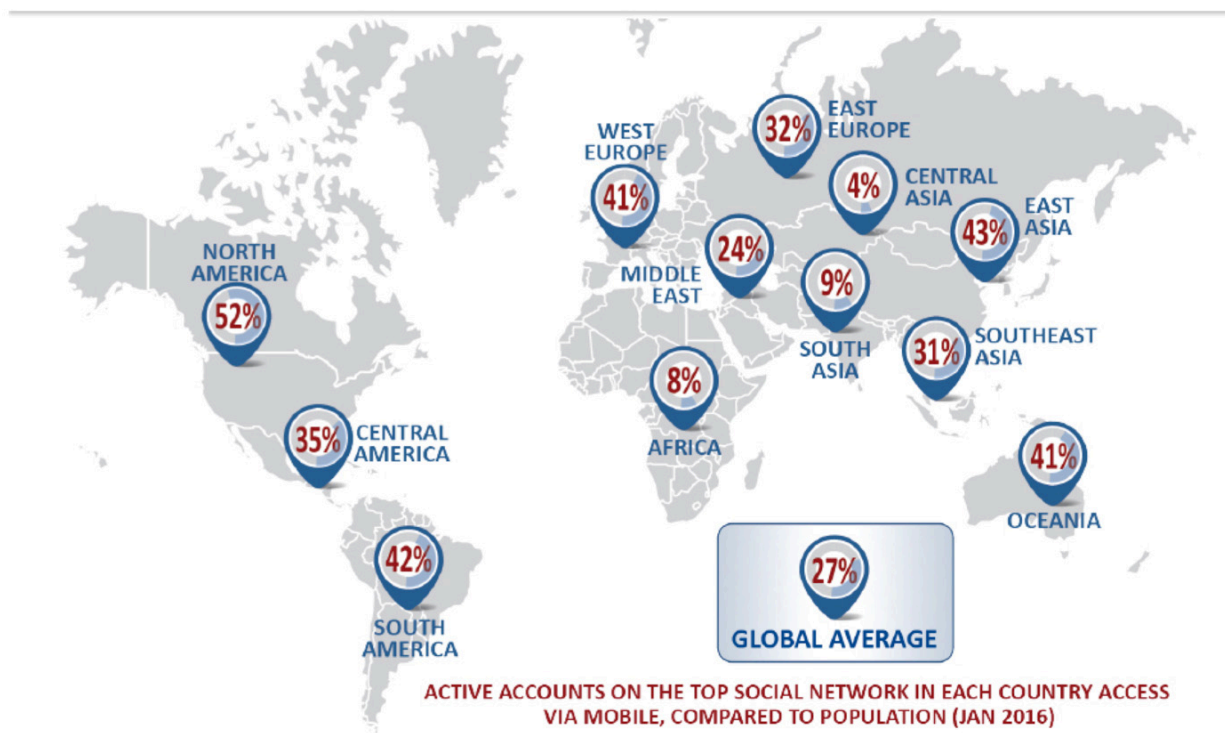
Exhibit 1: Worldwide Mobile Social Media Use

Today, the internet provides an open network environment enabling connectivity between users, computer systems, smart phone devices, and the emerging Internet of Things (*i.e.*, sensors, devices,

and actuators). One can imagine a future where every functional device and every person is connected to the global internet. This vast network offers ever-increasing opportunities for intelligence collection, but will also present many challenges. These challenges include focusing and enhancing the signal-to-noise ratio of desired information, assessing the validity of desired information, and assuring the reliability of desired information. The concept of active tasking of the internet offers one approach to help address these challenges.

With current technology, information can be extracted from a vast array of open information sources by combing through selected material, filtering for relevance, correlating with other information sources, and rejecting unrelated information. This passive process does not allow analysts to use the data to develop specific questions and then task various internet sources for additional information, clarification, or refinement of the original hypothesis.

Opportunities

Due to their "below threshold" nature, CMO campaigns can be difficult to recognize and understand. The open source information (OSI) environment is both the "playing field" and the primary source of information for the DoD, the IC, and others spurred by the massive growth in the information "fabric" contributed to by all connected assets (*i.e.*, people, platforms, and transactions). OSI is an especially important source of knowledge for recognizing CMO campaigns because most activities are carried out in the open and reported by either, or both, the open press and private citizens.

The amount of OSI is increasing at an exponential rate. Countries not already invested in legacy infrastructure such as land lines (*e.g.,* Africa, Indonesia, Malaysia) are the fastest growing new users of the internet, creating content in what was historically low-priority, national intelligence priority framework (NIPF) collection areas. Consider that the global Internet of Things (IoT) market, by 2019, is forecast to be valued at more than 1.7 trillion U.S. dollars, with the number of connected devices worldwide forecast to reach 42.1 billion the same year. In autonomous systems, the commercial market for fully autonomous vehicles will grow to some six billion U.S. dollars by 2025. This does not include unmanned aerial vehicles (UAVs) or unmanned underwater vehicles (UUVs). Smart homes are expected to have an installed base of connected things reaching 1.1 billion things by 2018, such as video streaming door bells, smart refrigerators, and internet-connected security and monitoring systems. At the same time, the installed base of connected things within smart cities is expected to reach 3.33 billion things, including toll roads, traffic cameras, street surveillance cameras, and power and water sensors.[1] By 2025, it may not be possible to purchase an automobile without multiple connection points to the internet.

---

[1] "Size of the global Internet of Things (IoT) market from 2009 to 2019 (in billion U.S. dollars)," Statista: The Statistics Portal, https://www.statista.com/statistics/485136/global-internet-of-things-market-size/

Challenges

The world is changing around us at a scale and volume that's unprecedented. As an indicator, consider that:

♦ "The cell phone is the most quickly adopted consumer technology in the history of the world".[2]

♦ 70+ million photos are uploaded to Instagram every day.

♦ Half a billion tweets are posted every day.

♦ Social media is being used for near real-time command and control to prevent incidents at sporting events (*e.g.*, riot prevention) and special security events (*e.g.*, meetings of the International Monetary Fund and U.S. political conventions).

♦ Two-thirds of law enforcement believe that social media helps them solve crimes more quickly.[3]

These changes are opportunities as well as vulnerabilities. To leverage this opportunity, OSI must be viewed culturally in the DoD/IC as a critical asset to be exploited and not ignored or overcome by the volume, velocity, variety, and veracity of the data and associated issues. Big data systems can help, but they are not useful if there are no investments made in better decision-making from such systems.

Success in recognizing, interpreting, and predicting CMO campaigns will depend on our ability to effectively and efficiently integrate and cross-cue, bi-directionally, enormous volumes of OSI and classified data for discovery of unknown campaigns or intent. This presents a challenge regarding where the data should reside and how much should reasonably move to the high- or low-side of classification barriers. Cross-cueing requires iterative, interactive workflow across all data streams. Simply classifying all relevant open source intelligence (OSINT) will be difficult to sustain as it continues to outgrow classified sources. Commercial analogs (finance and health sectors) deal with this type of divide with both scale and time urgency (*e.g.*, fraud detection, financial trading) but this will require the DoD and the IC to replace its various classified-centric data and workflow architectures, sometimes augmented with OSINT, with one that seamlessly integrates across the OSINT and classified INT divide.

Recommendation 4: DNI should establish a National Intelligence Manager (NIM) for constrained military operations

Within the IC, *"NIMs serve as the principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional areas. NIMs provide a single voice to policymakers to orient and guide collection and analytic activities to satisfy customers' information*

---

[2] Lee Rainie, "Cell phone ownership hits 91% of adults," *Pew Research Center*, June 6, 2013.
[3] Shea Bennet, "How Social Media Is Changing The World [INFOGRAPHIC]," *Social Times*, July 25, 2013.

needs."[4] The DNI and the Under Secretary of Defense for Intelligence (USD(I)) should appoint a National Intelligence Manager for Constrained Military Operations (NIM/CMO). At the same time the DNI and USD(I) should create a National Intelligence Program (NIP)/Military Intelligence Program (MIP) funding line for OSI collection and analysis that will be overseen by the NIM/CMO. The appointment of a NIM/CMO provides the DoD Strategic Options Task Force a counterpart responsible for marshalling IC resources in support of its charter. This newly created NIM/CMO must work in collaboration with other NIMs when interests overlap, but will be the primary interface to the DoD Strategic Options Task Force as well as CCMDs and U.S. Special Operations Command (USSOCOM) to support CMO activities.

Recommendation 5:   DNI should establish an Open Source Analysis Cell

The DNI should establish an Open Source Analysis Cell for Constrained Military Operations that is tasked by the NIM/CMO. The organization will place operators, analysts, and technologists together for mission unity and operate at scale and speed with current capabilities. The organization will improve existing approaches to detect deception, derive intelligence value, and drive tasking for OSI. One mission for the Open Source Analysis Cell is to develop ways to thwart adversaries using OSI deception. The Open Source Analysis Cell will be responsible for integrating real-time modeling and forecasting that relies on both OSI and classified sources.

This Open Source Analysis Cell for CMO could improve delivery of near-term value through a more robust application of existing tools to available data feeds. By linking the Open Source Analysis Cell to the DoD Strategic Options Task Force, however, a broader array of consumer expectations will emerge as indicated in the recommendation above. A shift from event-focused detection to campaign-focused detection, analysis and projection is essential for effective support to CMO.

Recommendation 6:   DARPA should establish a proving ground for open source analytics that is external to the Intelligence Community

The Defense Advanced Research Projects Agency (DARPA) should establish a proving ground for advanced analytics of open source information that is external to the IC and is managed by a Federally Funded Research and Development Center (FFRDC) or commercial entity. The primary reason for establishing the proving ground external to the IC is to enable operation in an open ecosystem with incentives (*e.g.*, challenge problems), tangible value (*e.g.*, curated data), and a frictionless interface to the private sector and academic communities that are driving innovation in big data analytics. Activities of the proving ground should include:

---

[4]   Office of the Director of National Intelligence, "Intelligence Integration: Who We Are"
(https://www.dni.gov/index.php/about/organization/intelligence-integration-who-we-are)

♦ Benchmarking of existing and emerging analytic tools with curated data sets provided by the Open Source Analysis Cell to assess relative value in addressing IC-relevant challenge problems

♦ Rapid transition of benchmarked tools into the IC Open Source Analysis Cell while maintaining a feedback loop to assess operational value and identify areas needing improvement

♦ Identification of shortfalls and gaps in current capabilities, and motivating or incentivizing ongoing innovation across external communities

♦ Creation of a publicly available, easily accessible corpus of machine learning tools with the goal of making the use of such tools as easy as formulating a search query and providing access to these tools as building blocks to speed innovation

♦ Evolving the system architecture in alignment with industry best practices, while facilitating synchronization Open Source Analysis Cell's system architecture
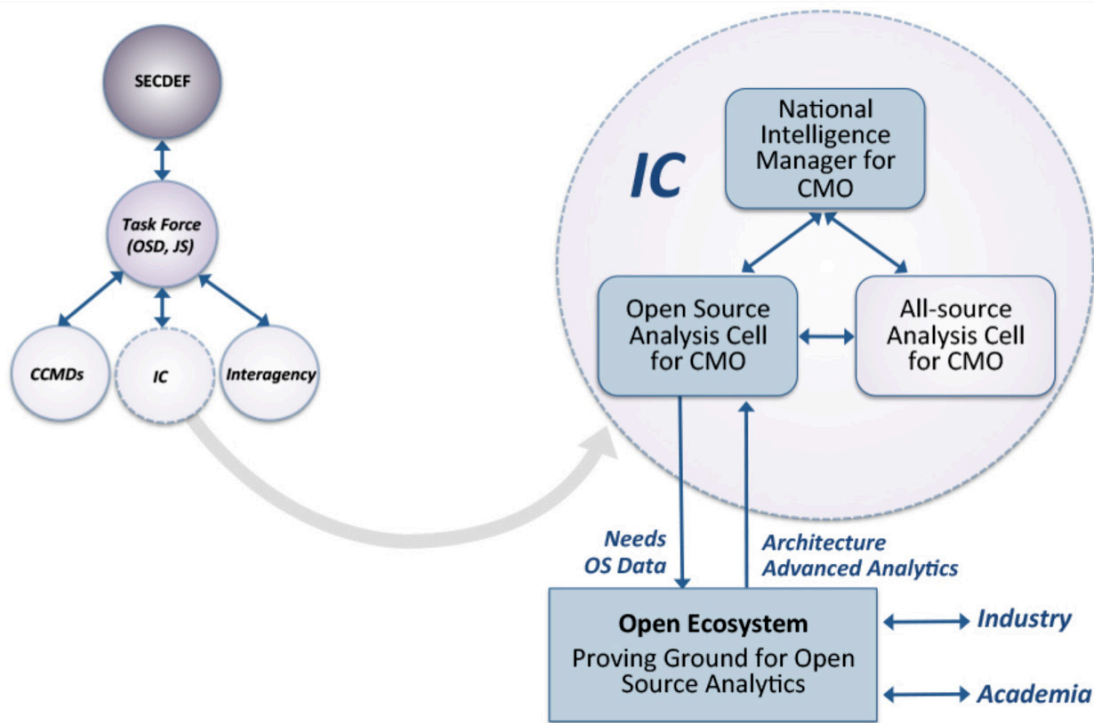

Exhibit 2: Framework for Accelerating and Exploiting Open Source Information

A two-pronged approach, as illustrated in Exhibit 2, is required to implement the above recommendations. In this construct, the internal Open Source Analysis Cell for CMO and the external

proving ground share a common system architecture to enable the IC to rapidly operationalize advanced analytic tools emerging from external entities. This architecture must adopt commercial best practices, provide a standard DevOps environment to speed innovation, and transition to operations inside the IC.

Advanced Analytics

The application of new analytic methods is necessary to extract useful information from tremendous volume and variety of open source data. The specific tools and methods depend on both the nature of the source data and the type of analysis. In general, however, analytic tools must transform the raw data into useful information, combine the information to address the intelligence questions, and present the results in ways that are useful to analysts. Particular tools and data sources can address different elements of the intelligence process, some of which are explained below. Specific examples of the utilization of advanced analytical techniques are included in the Leveraging Information and Intelligence chapter of this report.

Enhanced Situational Awareness:

Open source data, including published writings, opinion surveys, social media, commercial imagery, and geospatial reference data, can provide foundational and contextual information for analyzing and interpreting transient activities and behaviors. Analysts are beginning to apply human geography tools to these unclassified sources to develop deeper understanding of societies and nations.[5]

Rapid Detection:

Early detection of new campaigns affords decision-makers time to formulate effective responses. However, CMO and Gray Zone activities are intentionally kept below certain thresholds, making them more difficult to detect. There is a need for analytic tools that will automatically ingest streaming data from open sources, process the data quickly, and generate alerts in near real-time. Ideally, these tools should flag the key evidence that caused the alert, and provide analysts with methods for exploring the data.

Anticipatory Analysis:

Decision-makers attempt to calculate outcomes to inform their actions. A variety of forecasting methods exist for anticipating political change, economic trends, and other important events. The two general classes of methods are those based on expert judgment, and others based on automated, data-driven methods. Combining expert judgment with automated, model-based forecasts is an area of current research. The model-based methods often exhibit good short-term performance, but are unable to adapt to changes in the underlying mechanisms that govern the process.

---

[5] See Greg Slabodkin, "GEOINT Tradecraft: 'Human Geography,'" *Defense Systems*, October 29, 2013.

Opportunities for Advanced Analytics

The Department has an opportunity to leverage newly available data sources and significant research from academia and the private sector that will have a long-term impact on the nation's ability to prevail in constrained military operations.

Social media, economic indicators, political indicators, and financial disclosures have become globally available and provide new signatures for sentiment analysis, collaboration detection, and recognition of intent. Over the past several years, commerce, marketing, finance, insurance, and other industries have adopted these data types to understand and personalize their customer offerings.

Private sector companies have developed data curation, machine learning, and decision support services to solve some of the world's most challenging problems. The race is on to provide these insights in real-time, with real-time data.

With the continued and accelerating pace of information collection and availability in the public sector (free or for purchase), OSI has changed and continues to change the landscape of social understanding, tracking, and projection. The future information landscape includes game-changing elements such as the currently embryonic IoT. The IoT promises to add an exponential source of highly networked data and metadata replete with key insights into constrained military operational plans and their execution if the DoD knows where, when, and how to look.

Recommendation 7: Align the skills of IC analysts with the Big Data environment

The Office of the Director of National Intelligence (ODNI)/Chief Human Capital Officer, together with their Defense Intelligence Agency (DIA) counterpart, should develop and implement a strategy to attract, develop, and retain analysts with expertise in Big Data analytics that includes:

♦ Requisite skills include data science, cognitive modeling, visual analytics, computer science, machine learning, and graph analytics;

♦ Assignments, compensation, and incentives must be attractive in the supply-constrained competitive environment;

♦ Developmental opportunities should include ongoing training, sabbaticals in industry and academia, and rotational assignments to the proving ground; and

♦ Overall strategy should include appropriate use of Intergovernmental Personnel Act (IPA) assignments, term employees, and other approaches to access scarce skills.

Information Campaigns

Capabilities to inform, influence, and persuade employ primarily message-based products to communicate tailored information to selected audiences either to maintain awareness of and support

for U.S. operations and policies, or to change audience attitudes and behaviors. They can also be used to counter the effects of adversary messaging and propaganda.

CMO strategies work when a population, or collective, views the attributed actor's activities as legitimate. In CMO, inform, influence, and persuade capabilities can make it more difficult, costly, or risky for the adversary to pursue a successful operation. This includes capabilities that delegitimize the adversary's effects on influential audiences, reduce vulnerabilities in adversary targets, or change, redirect, or expose who the adversary action is attributed to. Access to more information can make it harder to insert false beliefs, and thereby increases transparency and reduces vulnerabilities in adversary targets. However, this is most effective when there are diverse sources to combat entrenched (and targeted) biases already present. Capabilities used to promote more and diverse connections (in physical and virtual space) among key audiences will reduce their susceptibility to false beliefs. Confirmation bias makes it easier to reinforce an existing belief than to create an entirely new one. These aspects can work in our favor.

Adversary tactics are often carried out at the local or city level and attempt to make incremental gains. The U.S. Government tends to favor larger-scale, one-size-fits-all approaches over localized and incremental approaches. To promote stability and reduce vulnerability, is it essential to apply steady pressure over time. From a strategic level, this means having sustained, focused attention and building a coalition of partners outside the U.S. Government. The U.S. needs to equip them to act by providing tools, strategies, and resources.

Anticipate an Information Campaign

The U.S. needs to identify and take advantage of weaknesses in the adversary's ability to shape the narrative and its perceived legitimacy. Adversary actions are often aimed at exploiting a target's vulnerability. For example, this might include ethnic or tribal divisions, corruption, the inability of local leadership to deliver services, or fears and prejudices. Building stability and trust in local organizations reduces the weaknesses the adversary can exploit. If people have institutions they trust, they are less prone to instability. The key is increasing the number of these positive, stabilizing, trusting connections. The more of them there are, the harder it is for the severing of any one of them to foster instability. Positive activities, such as humanitarian assistance, development programs, and public diplomacy exchanges are particularly helpful at addressing partner vulnerabilities over time. The critical point is targeting the right individuals, communities, and organizations.

Respond to an Information Campaign

Constrained military operations and Gray Zone strategies are more likely to be effective when a population views the attributed actor's activities as legitimate. Two strategies to combat these views are to change the perception of legitimacy or to change who the action is attributed to. The narrower that space, the harder it is to pursue a successful operation in the Gray Zone. Finding ways to reveal an adversary's role and duplicities undermines their legitimacy and creates greater risk of

international (or public) outcry.[6] Again, it is important to have diverse sources dispelling false information.

Asymmetries in the Information Fight

Because of cultural norms and American values, there are asymmetries between the tools the United States Government is willing to apply and those that can be applied against us. For example, the U.S. is extremely reluctant to release information that may be inaccurate for either domestic or foreign audiences. Adversaries have no such reluctance as shown in Exhibit 3.

	Adversary	U.S.
Campaign Model	• No commitment to truth • No commitment to consistency • High volume, multi-channel • Rapid, continuous, and repetitive	• Strict adherence to truth • International laws and norms • Partners to work "by, with, and through" • Nation states, influences, and grass-roots truth-tellers

Strengths	• Leadership commitment and focus
	• Integrated with other elements of power
	• Persistence of messaging
		• Cultural attractiveness
		  • Entertainment and gaming industries
		• Deep information skills
		  • Understanding and shaping sentiment (marketing, politics, etc.)

Vulnerabilities	• Truth • Economic outlook	• Info fight in CMO is not a priority • Past experience with info campaigns

Exhibit 3: U.S. and Adversary Asymmetries in Information Campaigns

However, the U.S. has some advantages. First, the openness of American society is widely admired in the world. Second, the reluctance to engage in deception and pluralistic nature of U.S. society makes it far less vulnerable to a balanced reporting of actual events and actions of the government when they are discovered. Often, adversaries must carry out expensive and ultimately disproven campaigns to motivate or distract their own populations as well as others. The U.S. also enjoys support from a wide group of allies who share many of our values, while adversaries are often isolated and unfriended.

Recommendation 8:   Strengthen DoD messaging capabilities

The Deputy Secretary of Defense should task the Assistant Secretary of Defense for Public Affairs (ASD(PA)), the Joint Staff, and the DoD Strategic Options Task Force to strengthen DoD messaging

---

[6] Although, it is not universally effective. Consider the success of sources that are seen as reasonably likely to disseminate misleading information like "Russia Today" in the United States. This has been a particular concern when foreign powers or corporations seek to motivate entrenched population segments with pre-existing, strongly held misconceptions even in a pluralistic population with excellent access to "truthful" content like the United States. Deceptive messaging without robust counter-messaging is alarmingly effective.

capabilities. This includes expanding the DoD's capabilities to access the full suite of open source information and mechanisms to disseminate and assess information designed to reach target audiences. The private sector should be leveraged for communication expertise such as public relations, social media, and marketing. Strengthening the DoD's messaging capabilities should be focused on increasing the flow of true information from credible voices to dampen the effect of propaganda and enhance the role of strategic communication in military education and training.

Cyber Operations

Cyber operations can be a cornerstone for Gray Zone activities. Operations can range from covert to overt, be executed quickly if appropriate capabilities are already in place, provide a wide spectrum of effects, scale at very low cost, and have controllable reversible effects. Unfortunately, these advantages come with some notable shortcomings. In particular, cyber operations can be perceived as highly threatening and the relatively small investments needed to have major impact on targets with high importance. Additionally, persistence can be an issue with cyber operations, since once exploited and vulnerabilities are discovered, they can be mitigated, although it may take months to develop and test the mitigations and then propagate them throughout the enterprise.

Recommendation 9:   Building out and operationalizing the cyber toolbox

There are several steps that can be taken that will enhance the DoD's ability to conduct cyber operations in the Gray Zone. To enable broader use and more rapid response, the Department should establish a tiered cyber authorities structure to empower operational commanders. This would entail providing different levels of commands with predetermined levels of access to have the authority to employ cyber tools. This prearranged delegation of authority would be a function of intended level of operational impact, scale, and scope of operation; ability to contain effects to the intended target; likelihood and nature of target response, including blowback and escalation concerns; likelihood of unintended consequences; and consequences of tool and operation compromise. U.S. Cyber Command (USCYBERCOM) combat mission teams could be used to ensure appropriate utilization of the tools. It also could be beneficial to establish a USCYBERCOM outreach program that orients operational planners, fosters understanding of national cyber capabilities and limitations, and provides a reach-back resource. Finally, it is important to ensure appropriate levels of protection are provided both to defend against incoming attacks and to protect potentially ephemeral and sensitive capabilities.

Effects and Capabilities

The major levers of power available to the U.S. Government are information, physical, diplomatic and economic as depicted in **Error! Reference source not found.**.[7] These levers overlap somewhat and are used by a variety of government agencies. The Department's primary focus is in the information and physical domains although, as discussed later, the DoD also plays important supporting roles in the diplomatic and economic spheres. This section is devoted to the physical, diplomatic, and economic domains.
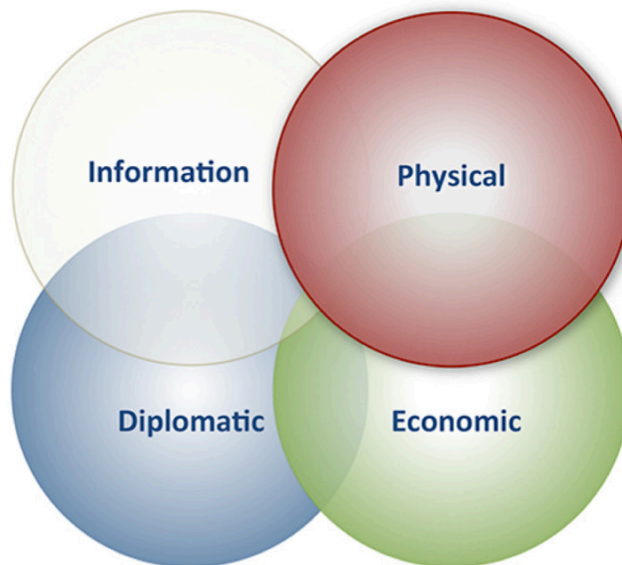

Exhibit 4: Major Levers of U.S. Power

Physical Effects

Gray Zone conflicts may not predominantly, or even heavily, rely on the military's application of physical effects. However, the availability of such physical capabilities and the ability to apply them when appropriate is important as a contributor to deterrence, controlling escalation, providing proportionate response, and assuring and strengthening allies and partners in the region of concern. The nature of these capabilities should be such that their use, whether threatened or applied, is sufficient to cast doubt in the adversary's calculus regarding the outcome, cost, and ability to accomplish their tactical or strategic objectives.

---

[7] These interacting circles in the figure are similar to the traditional "DIME" categorization of the elements of national power. The figure is intended to emphasize the military's role as an element of national policy highlighting the differing aspects of physical and information "levers."

The Study used four scenario case studies to analyze the potential use of physical capabilities. These scenarios include:

♦ China and the South China Sea – China's efforts to claim sovereignty over the majority of the South China Sea

♦ Russia in the Baltics – Russia's efforts to destabilize the region and stop the erosion of their "near abroad"

♦ Saudi-Iran Competition – traditional nation-state rivalry combined with religious and ethnic rivalries

♦ Short-Term Countering of ISIL- U.S. efforts to promote stability and counter violent extremism

In each scenario, physical capabilities were analyzed based on their usefulness in casting adversary doubt, reinforcing the strength and cohesion of regional relationships, and controlling escalation. Achieving these objectives with physical effects is dependent upon each effect being characterized by one or more of four important characteristics: scalability, deniability, reversibility, and shareability. Shareability may be the most important characteristic and is the ability of the U.S. to transition some of these physical effects to our partners, what has become known as building partnership capacity. Working "by, with, and through" our partners is often more important and effective than U.S. working alone for a variety of reasons. These reasons include a partner's use of capabilities that ensures long-term ownership of the response and often provides a vehicle for carrying out certain actions that the U.S. cannot do because of policy restrictions. Partner use, however, requires, among other things, the sharing of U.S. capabilities, a non-trivial requirement.

Based on the scenario case studies, four general categories of physical effects or capabilities are found to be the most useful in constrained military operations:

♦ Intelligence, Surveillance, and Reconnaissance (ISR) capabilities, including visible radio frequency (RF) and optical monitoring in proximity of national borders; acoustic and optical unmanned ground sensors; persistent remote taggants; unmanned underwater vehicles for monitoring harbors; and small unmanned aerial sensors for surveillance beyond the natural horizon

♦ Electronic Warfare (EW) capabilities, including measures to provide electronic resilience to radars, communications, and precision, navigation, and targeting (PNT) in all domains when operating near adversary regions; scalable and selective attack capabilities against adversary sensors; communications and PNT in all domains; and spoofing capabilities to create confusion, misdirect targeting, and stimulating action to expose and exploit adversary signatures

♦ Distributed Unmanned Technology capabilities, including smart undersea mines; undersea acoustic jammers; swarming UAVs launched from a variety of underwater and surface

vehicles; non-lethal UAV payloads to harass adversary military operations; smart land mines; local hot spots for tactical communications; and civilian internet access in denied areas

♦ Non-Lethal Effects in mechanical, electro-magnetic, chemical, acoustic, and biological domains with the ability to deliver immediate scalable (annoying to incapacitating) effects while minimizing lasting damage to both people and materiel. While potentially very useful, many of these non-lethal effects have major issues associated with use policy and operational effectiveness.

A fifth, conventional kinetic effects, also played a role but the panel did not focus on traditional kinetic effects since U.S. forces and many of our allies possess these in great numbers and in a wide variety. The existence of these play an important role in adversary deterrence and dissuasion. Many have "niche" applications in ongoing Gray Zone situations, but are generally not the effects of choice in constrained military operations.

After examining the use of many of the potential physical effects outlined above in the four scenarios, several high-level observations clearly emerged. First and foremost, it became clear that a rich set of potential military Gray Zone physical capabilities exist. Most require no development, and nearly all are broadly applicable to a wide variety of situations. When mapped into two of the most important attributes for using physical effects in the Gray Zone—reversibility and attributability—one finds that nearly 90% of available capabilities are reversible and/or non-attributable. Only 10% fall into the category that is most likely to lead to escalation. Exhibit 5 displays the mapping of physical effects.

	Unattributable	**Attributable**
Irreversible	• Persistent taggants • Cameras to fishing fleets • Anti-tamper technology • Disable land transport • Disable land vehicles and ships • Smart sea mines	• Airfield harassment • Foul airfields and ports • ISR platforms to partners • Smart land mines
Reversible	• Unattended ground sensors • ISR data to others • Undersea decoys and deception • Undersea surveillance • UAV sensors • Electronic attack • Electronic spoofing	• Enhanced regional surveillance • Optical border monitoring • Artificial "islands" • Persistent Close Air Support (PCAS) – Remote Advise & Assist (RAA) • Local hot spots • Micro-UAVs to clog airspace

Exhibit 5: Physical Capability Gray Zone Attributes

Significant benefits accrue by building partnership capacity and working "by, with, and through" partners in the application of these capabilities. Fortunately, many of them lend themselves to sharing with partners, given that necessary protective measures are applied to those capabilities for which there is special concern. Multiple approaches exist for the U.S. to enable and encourage partner acquisition of U.S. equipment and, despite the variety of approaches available, all require USSOCOM and the relevant geographic CCMD involvement in operational planning, training, and coordination. This involvement should be looked upon as an opportunity, rather than a burden, since such U.S. joint activity will go a long way in strengthening relationships, building confidence and, through joint training and exercising, send strong strategic messages to those on the other side of the Gray Zone competitions.

Joint exercises, either between U.S. forces or with partners, can have multiple benefits. Exercises provide experience with novel capabilities, build confidence in the ability of these capabilities to do what is needed, and provide an opportunity to refine and build trust in new concepts of operations (CONOPS). Depending upon specific capabilities involved and whether regional partners are involved; exercises can have powerful strategic messaging that has a significant impact on future events. Exercises can also occupy adversary attention and resources as they shadow U.S. activities.

The Study determined that the physical effects most impactful in constrained military operations are primarily available off the shelf and do not require much, if any, research and development. Also, these capabilities have a greater impact if they are shared with regional partners. In fact, how these capabilities are used and who uses them are often more important in responding to constrained military operations than the capability that is used. The recommendations for physical effects are detailed below.

> ## Recommendation 10: Acquire the appropriate equipment for constrained military operations

USD(AT&L) should create a $50M budget line item for rapid acquisition of non-development equipment for the Gray Zone as requested by the combatant commanders and USSOCOM. Much of the equipment that the U.S. military will need for physical actions in constrained military operations is already in the inventory. However, some items readily available, including unattended ground sensors (UGS), micro-UAVs, non-lethal equipment used by law enforcement, and the smartphone application for PCAS developed in a recently completed DARPA program. As the need is identified in response to specific challenges, the DoD should position itself to rapidly acquire items without a long administrative lead time.

The key to successful employment of the recommended equipment is providing adequate priority to ensure that these programs are not pushed to the side by the demands of existing programs of record with established advocacy within the Services. If necessary, USD(AT&L) should provide leadership and funding for the necessary equipment. However, the Services should create a budget line to rapidly

develop and procure sufficient quantities of equipment for experimentation, training, and exercises to refine and validate constrained military operations' CONOPS. The capabilities that the Services should focus on include:

- Treaty-compliant sea and land mines (10s)
- Low-cost UUV payloads (decoys, surveillance sensors, etc.) for commercial platforms (100s)
- Micro-jammers (100s)
- UAV swarm delivery system (10s)

Recommendation 11: Build partnership capacity by providing equipment to partners

The scenario analysis demonstrated that in many situations it is beneficial for the U.S. to operate by, with, and through partners. In many cases, partners have greater freedom of action since the threat or challenge is in their backyard and actions they initiate will be defensive, while U.S. efforts may be viewed as offensive and aggressive. Further, if partners take an active role in addressing their problems, they have long-term ownership of the results that may reduce the need for future U.S. involvement. Partner action also supports strategic messaging by building a coalition of nations that may be more effective in influencing adversaries than the U.S. acting alone.

To facilitate partner action, it is important that partners have access to U.S. equipment and training that will expand their inventory and capabilities. The Study identified three recommended actions for the DoD to actively support building partnership capacity through the acquisition of equipment:

- USSOCOM acquire and provide equipment with the appropriate training and support;
- CCMDs encourage regional partners to request purchase of U.S. equipment through the Foreign Military Sales (FMS) program; and
- USD(Policy) and USD(AT&L) encourage the U.S. Defense Industrial Base to pursue direct commercial sales with regional partners of appropriate products to build partnership capacity.

Recommendation 12: Implement a more strategic use of exercises

The Study concludes that exercises, both alone and with partners, can be important activities in the Gray Zone to improve performance and influence adversaries. The CCMDs, primarily U.S. Pacific Command (USPACOM) and U.S. European Command (USEUCOM), should use their training and exercise programs more strategically to:

- Gain experience, highlight policy and preparation issues, and establish value;
- Experiment with novel uses of current equipment;
- Actively engage partners and publicize maximum strategic messaging impact; and
- Provide a vehicle to distract adversary attention and consume physical activities.

DoD Contributions to Interagency Capabilities

The United States can only be successful in constrained military operations if there is an integrated whole-of-government effort. These operations require greater degrees of non-military actions than more common conventional or special military operations. In constrained military operations, the importance of diplomatic, informational, and economic instruments of power are often equal to, or greater than, military efforts. The DoD, however, has significant capabilities and programs across all these domains and can provide significant support to the interagency process.

Adversaries often seek opportunities to exploit seams within the U.S. Government. For example, an adversary can purposely present a diplomatic opportunity to the U.S. to gain a military advantage elsewhere and, thereby, create friction between the DoD and Department of State (DOS) efforts. A long-term, whole-of-government effort will help to eliminate potential interagency seams by focusing on broader strategic outcomes. In some cases, this will require one agency to withhold action to support the actions of another because it better supports the long-term strategic outcome. Done correctly, the actions of one agency will reinforce the action of others. This creates a much more complex problem for U.S. adversaries and forces them to compete simultaneously with multiple instruments of U.S. power

Security Cooperation

Security cooperation is the umbrella term for DoD efforts to build partnership capacity and work "by, with, and through" partner nations in pursuit of national security objectives. It includes efforts to build defense ministerial capacity, provide security force assistance, execute multinational exercises, and deliver training and materials. Security cooperation can be covert or overt, but usually has lengthy timescales, both because it can take years to sufficiently develop needed relationships with, and understanding of, partners, and it can take years to be effective. Security cooperation is not reversible, though security cooperation can be stopped, and the threat or actual suspension of security cooperation can be a persuasive lever to get partners to make changes in other policy areas.

Capabilities to Inform, Influence, and Persuade

Influencing foreign audiences is an essential tool in the Gray Zone. Capabilities to inform, influence, and persuade employ primarily message-based products to communicate tailored information to selected audiences either to maintain awareness of and support for U.S. operations and policies, or to change audience attitudes and behaviors. Capability components include listening, advocacy, cultural diplomacy, international broadcasting, exchanges, and psychological operations. [8] Of course other tools, such as military actions like show of force and coalition exercises, as well as other interagency tools, like financial sanctions, have complementary signaling or influential effects. The coordination and integration of these different kinds of efforts across the interagency has been described as

---

[8] Nicholas J. Cull, "Public Diplomacy: Taxonomies and Histories," *The ANNALS of the American Academy of Political and Social Science*, 616(1), 2008.

strategic communication,[9] a term of art that has fallen out of fashion within the DoD, but is a concept that needs to be revived and revitalized.

Diplomatic and Legal Tools

The U.S. government depends heavily on diplomatic and legal means to shape and sustain a peaceful, just, and prosperous world community, and applies the necessary tools in this domain to maintain international norms of behavior and influence adversary behavior. It goes without saying that the use of diplomacy and legal means to influence other nations is the preferred route over military conflict, but the path is rarely straightforward and the results likely unknown for many years. The currency of diplomacy is relationships, which are complicated and often difficult to assess.

Financial Tools for Constrained Military Operations

The Department of Defense is in a critical position among U.S. Government departments and agencies to take a lead role relative to the use of financial tools for defensive and offensive actions to counter financial threats. With direct access to, and dependence on, thousands of contractors in the Defense Industrial Base (DIB), the DoD must work closely with the DIB to protect supply chains and, where appropriate, protect companies that help the Department maintain its strategic advantage across the globe. In parallel, the DoD can use a variety of tools to confuse and delay adversary supply chains and the corresponding industrial base to directly impact the acquisition and assembly of weapons.

The global financial infrastructure allows for businesses to operate efficiently and effectively in real-time. Transactions are tracked down to the split-second and move trillions of dollars around the globe daily. For years, the financial sector has employed analytics and metrics that have resulted in a set of financial norms at the global, industry, company, and local levels. In order to leverage the available financial tools effectively, the DoD will need to adopt and use these financial analytical capabilities to enhance decision-making and protect interests relative to maintaining strategic advantage.

Foreign Humanitarian and Development Assistance

Foreign assistance refers to assistance to foreign nations ranging from the sale of military equipment to donations of food and medical supplies in aid of survivors of natural and manmade disasters. Humanitarian assistance programs are those activities conducted to specifically relieve or reduce human suffering, disease, hunger, or privation; whereas, development assistance programs are carried out to improve the lives of citizens of developing countries while furthering U.S. foreign policy interests in expanding democracy and promoting free market economic growth.

Foreign humanitarian and development assistance offers the opportunity to build more robust civil societies, combat corruption, and otherwise address the internal weaknesses upon which Gray Zone conflicts often prey. Gray Zone conflicts are designed to exploit the weaknesses of a given target; thus

---

[9] See Reports of the DSB Task Force on Strategic Communication, 2004 and 2008

mending those weaknesses, whether through security, humanitarian, or development assistance. These capabilities remain essential to effective defense or deterrence.

Recommendation 13: Effective interagency coordination

To ensure that the DoD has the appropriate plan for interagency coordination, the Secretary of Defense should ensure there are effective plans for the Department's use of integrated interagency capabilities for constrained military operations. Also, the recommended DoD Strategic Options Task Force, in coordination with the USD(P), the JCS, the IC, and CCMDs, should develop focused campaign-level approaches that integrate whole-of-government actions.

The development of a strategic framework focused on constrained military operations would transform the interagency landscape. First, it would provide a long-term focus for the NSC and the rest of the U.S. Government. Instead of reacting to continuous short-term policy challenges, a long-term strategic plan would guide the interagency. A strategic framework could integrate U.S. actions in a way that short-term policy decisions cannot. It would appropriately balance military and non-military activities in a way that presents complex problems sets to U.S. adversaries. Finally, it represents the best path to counter the long-term objectives of potential adversaries.

Despite the need for a strategic framework, each agency will need to develop their own campaign plans nested within the overarching strategic framework. Without equal participation by the other agencies of the U.S. Government, the DoD may dominate the interagency process due to its capacity for planning and conducting operations. This risk must be mitigated by ensuring that other government agencies have sufficient capacity for developing and implementing long-term campaign plans. In some cases, other government agencies may have to develop that capacity over time and the DoD should be prepared to assist with their effort.

These approaches should be supported by playbooks and guidance for shaping the environment and constraining an adversary, as well as provide processes for focusing, developing, and coordinating interagency capabilities for security cooperation; inform, influence, and persuade operations; diplomacy and legal actions; the use of financial tools; and foreign humanitarian and development assistance.

Summary

The Study took a three-pronged approach to countering potential adversaries' strategies for waging long-term campaigns for constrained military operations and Gray Zone conflicts:

 ♦ Create a long-term strategic framework and threat-oriented campaigns;
 ♦ Exploit the new and evolving information landscape; and

♦ Continue to add to the available set of tools applicable to operations addressing less than in full-scale conventional warfare.

The Study concluded that much of the Department's actions for constrained military operations and Gray Zone conflicts were reactive and episodic. The creation of a long-term (tens of years) strategy to counter adversaries' activities and to proactively advance national interests should be a first and important priority for Department leadership. The Study recommends that the Secretary of Defense charter and staff a DoD Strategic Options Task Force with the objective of creating a strategic framework, and assist in the development of campaigns, OPLANs, and associated playbooks aimed at providing both reactive and proactive actions to deter and counter adversaries' potential activities in the Gray Zone. The DoD Strategic Options Task Force should be populated with senior interagency, IC, Joint Staff, and CCMD representatives that can prepare, coordinate, and mobilize all instruments of national power to dominate in the Gray Zone. The Study outlined historical precedents for such an approach to serve as a model for the creation of such a framework and campaign process. Precedents from the Truman, Eisenhower, and Reagan years assist in guiding the development of strategy and campaigns. The DoD Strategic Options Task Force must consider the role and integration of allied actions into interagency and DoD strategy and campaigns, and the roles of allies in military, diplomatic, economic, and societal activities in order to create an enduring U.S. strategy.

A new and critical element of Gray Zone operations is the importance of the information landscape in understanding adversaries' actions and prosecuting friendly (U.S. and allied) campaigns. New sources of information derived from social media, the IoT, and advanced data analytical methods must be integrated with conventional intelligence to effectively prosecute Gray Zone information operations. Data analytical tools are rapidly being developed within the government and commercial sector and must be applied to the preparation and execution of campaigns. The information needs to prosecute an information campaign are different than those required for conventional military operations. The investigation of topics such as adversary tactics and order of battle, important in conventional warfare, must be augmented by the investigation of diplomatic, societal, and economic actions undertaken by potential adversaries. The Study emphasizes the need to accelerate the collection and exploitation of open source information and apply this information to campaigns for supporting and waging constrained military operations.

Having investigated strategic objectives and supporting information operations, it is finally important to determine the enabling capabilities, or toolbox, necessary to prosecute constrained military campaigns. In creating the toolkit, it is important to determine how and by whom these capabilities are to be applied. Building partner capacity should be emphasized since working in concert with partners has proven to be more effective than the U.S. operating alone. As has been done in the past, clandestine, covert, and deniable tools are important in the Gray Zone as the U.S. and its partners often bring differing societal policy restrictions to such operations. The control of escalation is an important consideration. Tools that are flexible and reversible are essential to assure that the U.S. and its allies, instead of the adversary, determine the level of escalation necessary to accomplish

objectives. The Study found that many of these capabilities exist and are ready for procurement. Achieving coordinated interagency and allied effects is a difficult and important determinant of success and the creation of playbooks by the DoD Strategic Options Task Force that shape this activity will assist in achieving this required coordination.

Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

NOV 3 2015

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board 2016 Summer Study on Capabilities for Constrained Military Operations

Over the last two decades the U.S. has sustained the credibility of its nuclear deterrent and maintained sufficient conventional forces to deter major aggression by a peer or near-peer competitor. More recently we have honed our capabilities for combatting global terrorism. For the last 20 years, however, we have seen a third category of conflict that occurs again and again. These conflicts are regional, may be represented by an insurgency against a standing government, military and political activities within a sovereign nation conducted by a neighbor, disputes over territory between neighboring nations, or terrorist or criminal activities within ungoverned territories or within failing states.

In these conflicts it has been very difficult to assess the situation and to determine what U.S. interests are at stake. Additional challenges include determining what actions should the U.S. take to protect those interests, who our allies and adversaries are in the particular situation, and what end-state would be best to protect our interests and result in the most favorable outcome. These actions and plans are usually constrained by: cost considerations, the need for coalitions of supporting nations, the desire to use minimal physical force, a strong desire to minimize U.S. military and civilian casualties, the need to minimize damage to critical infrastructure, and an awareness that public opinion - internationally, in the region, and at home - plays a highly influential shaping role.
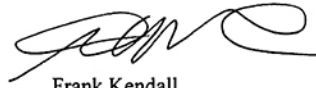
Overarching goals of the USG are to protect its interests early before hostilities begin and to deter aggression with the objective of minimum loss of life and infrastructure through the use of shaping techniques, massive information collection and assessment and autonomous and non-lethal capabilities.

The objective of the 2016 Summer Study on Capabilities for Constrained Military Operations is to assess the military planning, shaping, and operational activities that address potential threats to U.S. interests and strive to establish stability in critical regions of the world that do not rise to the level of full scale military operations. Areas of consideration will include an assessment of current planning processes within DoD Policy, the Joint Chiefs of Staff, Combatant Commands, and the Intelligence Community with a focus on the period before significant hostilities begin. What information is required - provided by traditional ISR, emerging commercial sources, and social media - to assess which threats to U.S. interests are in play, who is responsible for the threat, what are their objectives, and what can be done to deter their activities? What physical and cyber based capabilities does the DoD currently have to bring to bear on the situation, what commercial capabilities can be employed, and what technologies must be developed?

TERMS OF REFERENCE

I will sponsor the study. Mr. Vincent Vitto and General Michael Carns, USAF (retired) will serve as Co-chairs of the study. LTC Keith R. Walters, USA, (OSD ODNA) will serve as Executive Secretary. Lt Col Victor Osweiler, USAF, will serve as the DSB Secretariat Representative.

The study will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act" and DoD Directive 5105.04, the DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

Frank Kendall

Study Membership

Study Chairs

Gen. Michael Carns (RET)   Private Consultant
Mr. Vincent Vitto   Private Consultant

Executive Secretary

LTC Keith Walters   Office of the Secretary of Defense, Office of Net Assessment

DSB Board Chair

Dr. Craig Fields   Private Consultant

DSB Board Vice-Chair

Dr. Eric Evans   MIT Lincoln Laboratory

Members

Mr. Brandon Ahrens	Ernst & Young, LLP
Dr. Amy Alving	Private Consultant
Dr. Michael Anastasio	Los Alamos National Laboratory (LANL)
Dr. Wanda Austin	Aerospace Corporation
Mr. Michael Bayer	Private Consultant
Dr. Kerry Buckley	MITRE Corporation
Mr. Frank Cappuccio	Private Consultant
Mr. James Carlini	Private Consultant
Dr. David Chu	Institute for Defense Analysis (IDA)
Dr. Victoria Coleman	Technicolor
Mr. Andrew Coon	Autogration, LLC
Dr. Lisa Costa	MITRE Corporation
Dr. Ruth David	Private Consultant
Mr. Christopher Day	Packet Forensics
ADM William Fallon (RET)	Private Consultant
Dr. Michael Fitzsimmons	Institute for Defense Analysis (IDA)
Ms. Christine Fox	Johns Hopkins University Applied Physics Laboratory (JHU/APL)
Dr. Timothy Gibson	Parasang Solutions, LLC
Dr. Theodore Gold	Private Consultant
Mr. James Gosler	Johns Hopkins University Applied Physics Laboratory (JHU/APL)

Mr. Al Grasso	MITRE Corporation
Mr. Page Hoeper	Private Consultant
Mr. Mark Hoffman	Lockheed Martin Advanced Technology Laboratory
Brig. Gen. Christopher Inglis (RET)	U.S. Naval Academy
Dr. John Irvine	Draper Laboratory
Dr. Miriam John	Private Consultant
Dr. David Johnson	RAND Corporation
Dr. Anita Jones	University of Virginia
Dr. Paul Kaminski	Technovation, Inc
Dr. Ronald Kerber	Private Consultant
GEN. Paul Kern (RET)	The Cohen Group
Mr. Zachary Lemnios	IBM
Dr. John Manferdelli	Google
Dr. Joe Markowitz	Private Consultant
Dr. Mark Maybury	MITRE Corporation
Dr. James Miller	Johns Hopkins University Applied Physics Laboratory (JHU/APL)
Dr. Judith Miller	Private Consultant
Mr. Robert Nesbit	Private Consultant
Dr. Paul Nielsen	Carnegie Mellon University Software Engineering Institute (SEI)
Dr. Christopher Paul	RAND Corporation
Mr. Michael Rich	RAND Corporation
Mr. Benjamin Riley	Georgia Tech Research Institute (GTRI)
Mr. Paul Rosenstrach	Draper Laboratory
Mr. Mark Russell	Raytheon
Dr. Walt Rutledge	Sandia National Laboratory
Dr. Dylan Schmorrow	Soar Technology, Inc
Dr. William Schneider	International Planning Services, Inc
Dr. Ralph Semmel	Johns Hopkins University Applied Physics Laboratory (JHU/APL)
Dr. Les Servi	MITRE Corporation
Dr. Michael Shatz	MIT Lincoln Laboratory
Mr. Lewis Shepherd	Private Consultant
Mr. James Shields	Private Consultant
Mr. Robert Stein	Private Consultant
VADM Edward Straw (RET)	Osprey Venture Partners
Dr. James Tegnelia	University of New Mexico
Mr. James Thomas	Center for Strategic and Budgetary Assessments (CSBA)
Mr. Davd Van Buren	L-3
Dr. David Van Wie	Johns Hopkins University Applied Physics Laboratory (JHU/APL)
Mr. Lewis Von Thaer	DynCorp International
Dr. Peter Weinberger	Google
Dr. David Whelan	The Boeing Company
Dr. Dean Wilkening	Lawrence Livermore National Laboratory (LLNL)
Dr. Robert Wisnieff	IBM

Government Advisors

Ms. Roxanne Cabral	Department of State
MG John Charlton	Joint Staff, J7
Mr. Andrew Steinfeld	Joint Staff
Mr. R. David Stephenson	Joint Staff, J7
COL George Thiebes	Joint Staff, J3
COL Isaiah "Ike" Wilson	USCENTCOM

Defense Science Board

CAPT Mike Flanagan	Deputy for Operations, U.S. Navy
Lt Col Victor Osweiler	Deputy for Operations, U.S. Air Force
Ms. Karen Saunders	Executive Director

Staff

Ms. Meghan Fitch	Strategic Analysis, Inc
Ms. Hannah Freeman	Strategic Analysis, Inc
Ms. Ashlee Gilligan	Strategic Analysis, Inc
Mr. Marcus Hawkins	Strategic Analysis, Inc
Dr. Toni Marechaux	Strategic Analysis, Inc
Mr. Michael Rauseo	Redhorse Corporation
Ms. Jeray Simms	Strategic Analysis, Inc
Ms. Stephanie Simonich	Strategic Analysis, Inc / Redhorse Corporation
Mr. Ted Stump	Strategic Analysis, Inc

List of Meetings and Briefings

January 27–28, 2016

Allies and Adversaries
> *Mr. James Baker, Director, Office of the Secretary of Defense, Net Assessment*

Preparing for Gray Zone Campaigns
> *Dr. Michael Mazarr, Senior Political Scientist and Interim Director, Strategy, Doctrine and Resources Program, Arroyo Center, RAND*

Joint Planning and Conflict in the "Gray Zone"
> *MAJ Ben Flosi, Joint Staff, Joint Operational War Plans Division and Strategy Development Division*
> *Mr. Jay Rouse, Strategic Planner, Joint Staff, Joint Operational War Plans Division and Strategy Development Division*

The Challenge of Commanding Under Conditions of 'Compounding Security' Dilemmas: A U.S. CENTCOM Perspective
> *Colonel Isaiah "Ike" Wilson III, U.S. Army, PhD, Chief, Commander's Initiatives Group (CIG), U.S. Central Command, Tampa Florida, MacDill A.F.B., Tampa Florida*

Turning on the DIME(S)
> *Mr. Robert Bestani, Professor and DOE Faculty Chair, National Security and Economic Policy, Eisenhower School of the National Defense University*

Context of Future Conflict
> *Mr. Jeffrey Becker, Futures Subject Matter Expert, Joint Staff J-7, Joint Concepts Division*

Discussion on Constrained Operations
> *Dr. Michael Vickers, former Under Secretary of Defense for Intelligence*

February 24–25, 2016

Foreign Approaches to Gray Zone Conflicts
> *Director, Global Security Program, Strategic Futures Group, National Intelligence Council, Office of the Director of National Intelligence*

New Global Realities
> *Intelligence Officer, Strategic Futures Division, Defense Intelligence Agency*

Insights as Former USD(P)
> *Dr. Jim Miller*

Constrained Military Operations
> *General John R. Allen, USMC (Ret.), Co-Director, Center for 21st Century Security and Intelligence, The Brookings Institution*

Constrained Military Operations
> *Mr. Paul Martin, Principal Director for Plans, OSD Policy (ODASD Plans)*

Strategy, Plans and Capabilities

Mr. Robert Scher, Assistant Secretary of Defense for Strategy, Plans and Capabilities, Office of the Secretary of Defense for Policy

Scenarios for Assessments of Constrained Military Operations

Mr. Jim Mitre, Director for Analysis, OSD Policy (ODASD Strategy & Force Development)

Analysis and Insights

Mr. Timothy Bright, Director of the Irregular Warfare Division, Cost Assessment and Program Evaluation

March 16–17, 2016

Strategic Multi-Layer Assessment Program

Dr. Hriar Cabayan (OSD)

Anticipatory Intelligence at IARPA

Dr. Philippe Loustaunau, Technical SETA, IARPA

Russian New Generation Warfare – Coming to a Theatre Near You?

Dr. Philip A. Karber, President, The Potomac Foundation

Inferring Organizational Intent Via Interactive Analytics

Dr. William B. Rouse, Professor, Stevens Institute of Technology

GEOINT Pathfinder

Mr. Chris Rasmussen, GEOINT Pathfinder Program Manager & Public Open Source Software Development Lead, National Geospatial-Intelligence Agency

Illicit Networks: We have Met the Enemy

LTC (Ret) David E.A. Johnson, USA, Executive Director, Center for Advanced Defense Studies (C4ADS)

April 20–21, 2016

Grey Zone Threats in the CENTCOM AOR

CPT Joshua Weinberg, Liaison Officer, Special Operations Command - Central

U.S. and Iran – Competition in the Gray Zone

Mr. Ben Pieczynski, Deputy Division Chief – CCJ5 Plans Division, USCENTCOM

Mr. Thomas Mortenson, Senior Strategic and Policy Planner, CCJ5 Plans Division, USCENTCOM

Gray Area Wars & Big Data

Dr. Brian Pierce, Information Innovation Office Director, DARPA

Squad X

Maj. Chris Orlowski, Tactical Technology Office Program Manager, DARPA

RAA/PCAS

Dr. Dan Patt, Tactical Technology Office Program Manager, DARPA

CODE

Mr. Jean-Charles Ledé, Tactical Technology Office Program Manager, DARPA

Intelligence for a Changing World

The Honorable Stephanie O'Sullivan, Principal Deputy Director of National Intelligence, Office of the Director of National Intelligence (ODNI)

100G
Dr. Ted Woodward, Strategic Technology Office Program Manager, DARPA

Radio Map & Mobile Hotspots
Dr. Joe Evans, Strategic Technology Office Program Manager, DARPA

PlanX
Mr. Frank Pound, Information Innovation Office Program Manager, DARPA

Observations from the Former 10th Group Commander
COL George K. Thiebes, Assistant Deputy Director of Special Operations, J-37

May 17–18, 2016

Integrated Country Strategies and Interagency Process
Mr. Daniel Kimmage, Policy Planning Staff, Office of the Secretary of State, Department of State
Ms. Ciara Knudsen, Policy Planning Staff, Office of the Secretary of State, Department of State

Understanding and Countering Extremist Propaganda and Russian Disinformation
Mr. Tom Miller, Public Diplomacy Fellow, Department of State

The Weaponization of Information and Cognitive Security in New Media
Dr. Rand Waltzman, Associate Director of Research, Software Engineering Institute, Carnegie Mellon University

Contingency Program Management
Mr. Schaffer Dearmond, Consultant, OSD AT&L Program Support
Ms. Lara Cantuti, Consultant, OSD AT&L Program Support

PeaceTech
Dr. Sheldon Himelfarb, Ph.D., CEO, PeaceTech Lab

New (Digital) World Requires Better Ways to Work
Mr. William D. Murray, Retired Intelligence Officer, Managing Member, Alphom Group, LLC

Countering Terrorist Financing: A Case Study on Hizballah
Mr. Adam Szubin, Acting Under Secretary, Office of Terrorism & Financial Intelligence, United States Department of the Treasury

IC Open Source Functional Management
Intelligence officers from DIA and CIA

June 21–22, 2016

SCO Briefing to the DSB Study on Capabilities for Constrained Military Operations
Dr. Will Roper, Director, Strategic Capabilities Office

Joint Warfare Analysis Center (JWAC): Analysis Supporting Phase 0/1 Operations
Mr. Ron Tiberio, Special Projects Division Head, JWAC
Mr. Gene Downum, Senior Analyst for Shaping and Deterrence, JWAC
Dr. Schuyler Porche, Senior Analyst for Shaping and Deterrence, JWAC
Mr. Jaren Luffman, Senior Analyst for Economic Analysis, JWAC

July 12–13, 2016

No plenary briefings

August 15–26, 2016

No plenary briefings