UNITED STATES ARMY SPECIAL OPERATIONS COMMAND

White Papers

- Expanding Maneuver
- Comprehensive Deterrence
- Operationalizing Deep Knowledge
- Redefining the Win
- Perceiving Gray Zone Indications

UNITED STATES ARMY
SPECIAL OPERATIONS COMMAND

White Paper

Expanding Maneuver

in the Early 21st Century Security Environment

12 January 2017

"Our adversaries know they cannot prevail against us…So they have done the logical thing... Low-intensity warfare is their answer to our conventional and nuclear strength — a flanking maneuver, in military terms."[1]

— George Shultz, Secretary of State, January 15 1986

Introduction

When we look at Russian aggression in Eastern Europe, we see an adversary maneuvering in careful, calculated ways that undermine current theater campaign designs. One study from the Army War College puts it this way: "[China, Russia, and Iran] have outmaneuvered their seemingly less nimble U.S. competitor."[2] Across the Range of Military Operations (ROMO), we need to think about designing campaigns around a different maneuver paradigm. Designing a campaign to prepare maneuver space for positional advantages is currently guided by a thought paradigm centered on arranging physical force options in a narrow frame of time and space. These approaches are oriented toward achieving objectives through physical maneuver. This does not match with what the operational environment is telling us. This paper builds on conceptual explorations of cognitive maneuver and suggests we need to expand the practice of maneuver. Expanding maneuver is not only about the process of maneuvering; it is about the design of that process — designing operations and campaigns oriented toward synchronized cognitive and physical objectives. In an increasingly interconnected and complex environment highlighted by population-centric aspects of competition and conflict — we must consider an expanded concept of maneuver that considers both physical and cognitive maneuver across the ROMO to move both force and ideas in time and space.

The Operational Environment Tells Us to Change

What is the operational environment telling us? At the moment, it is telling us that five identified security challenges frustrate the order of the international system.[3] A sixth challenge remains unknown in the confluence of accelerating changes.[4] Russian aggression in Eastern Europe is

---

[1] Shultz, George. "Low-Intensity Warfare: The Challenge of Ambiguity." *Current Policy No. 783.* Washington, D.C.: Unites States Department of State Bureau of Public Affairs, January 15, 1986.

[2] Freier, Nathan P., ed. "Outplayed: Regaining Strategic Initiative in the Gray Zone." Carlisle Barracks: Strategic Studies Institute and U.S. Army War College Press, June 2016, p. 6. Hereafter AWC Gray Zone Study.

[3] Carter, Ash. "Taking the Long View, Investing for the Future." *Defense Posture Statement 2017.* Washington, D.C.: Department of Defense, February 2016, p. 4. Hereafter, Defense Posture Statement 2017.

[4] Consideration of a sixth challenge is derived from recent thinking about fragility in the international system by such theorists as Dr. Nasim Taleb, Dr. Yaneer Bar-Yam, and Chairman of the National Intelligence Council, Dr. Gregory F. Treverton. Additionally the JOE 2035 describes that the character of conflict will be affected by the intersection of trends in world order, science, technology and engineering and human geography. For more, see Taleb, Nassim Nicholas, and Gregory F. Treverton. "The Calm Before the Storm." *Foreign Affairs* 94, no. 1 (2015): 86-95. See also JOE 2035.

stressing the cooperative security arrangement of member states through NATO.[5] China's rise as a global economic competitor is giving the state's leadership justification to acquire space in the South China Sea and to increase the pace of Chinese militarization efforts.[6] North Korean intentions remain uncertain as the country's dictator persistently provokes regional partners as well as U.S. Pacific interests through nuclear and ballistic missile tests.[7] Iran continues to influence regional powers through its support of malign actors, including Assad in Syria, Hezbollah in Lebanon, and motivators in Yemen.[8] An extremist cancer continues to metastasize in the form of ISIL, which threatens the physical security of both regional and trans-regional partners.[9] Finally, the accelerating pace of technological, social, and structural changes are creating conditions for a sixth, as of yet unknown strategic surprise. The difficulty with this sixth looming challenge is figuring out where and when to look for it, let alone what to look for.

Conflict Character Changes

- Primacy of nonmilitary factors: politics, diplomacy, economics, finance, information, and intelligence
- Primacy of the information domain: use of cyberwarfare, propaganda, and deception, especially toward the Russian-speaking populace
- Use of armed civilian proxies, self-defense militias, and imported paramilitary units
- Asymmetric, nonlinear actions

(Johns Hopkins University Applied Physics Laboratory 2015)

Focusing on Russian aggression in particular, we find many clues as to a changing character of conflict. A Johns Hopkins University study on Russian unconventional warfare identified multiple lines of effort to annex Crimea and pursue conflict in Eastern Ukraine. The study illuminated several key efforts in the campaign, which were primarily nonmilitary factors and primacy of the information space. The nonmilitary factors include "politics, diplomacy, economics, finance, information, and intelligence" and information space "use of cyberwarfare, propaganda, and deception, especially toward the Russian-speaking populace."[10] Russia has been waging an unconventional warfare — some say hybrid war — to secure objectives without crossing a threshold of major armed conflict.[11] Secretary of State John Kerry testified that "Russia's clear and unmistakable involvement in destabilizing and engaging in separatist activities in the east of Ukraine…agents have been the catalyst behind the chaos."[12] One reason why those agents were such effective catalysts is that a form of cognitive mass had been built within the population. Rather than massing materiel and formations, Russia's hybrid approach

[5] Ibid.
[6] Defense Posture Statement 2017, p. 21.
[7] Defense Posture Statement 2017, p. 22.
[8] Defense Posture Statement 2017, p. 23.
[9] Defense Posture Statement 2017, p. 4.
[10] Johns Hopkins University Applied Physics Laboratory. *"Little Green Men:" A Primer on Modern Russian Unconventional Warfare.* National Security Analysis Department, Fort Bragg: United States Army Special Operations Command, 2015, p. 5. Hereafter JHU Study.
[11] JHU Study, p. 17. See also, Kofman, Michael, and Matthew Rojansky. *A Closer Look At Russia's "Hybrid War".* Kennan Cable No. 7, Kennan Institute, Washington, D.C.: The Wilson Center, 2015.
[12] *Testimony John Kerry Opening Statement Before the Senate Committee on Foreign Relations.* April 8, 2014. http://www.state.gov/secretary/remarks/2014/04/224523.htm (accessed August 11, 2016).

effectively massed information, ideas, and non-military influences to create cognitive space for freedom of action. They then directed that mass to achieve specific objectives. *They outmaneuvered challengers by physically operating in an abstract domain*.

This kind of activity by a major state power raises concerning questions about future behaviors of both state and non-state international actors. Collectively, these challenges set the security environment on a trajectory of "contested norms" and "persistent disorder."[13] This means we need to take operational approaches that recognize the physical, moral, and cognitive spheres with which disruptive actors' motives generate dangerous momentum. The commander of U.S. Special Operations Command (USSOCOM) suggests we need to take a "people-access approach: being there ahead of time, having relationships there ahead of time, identifying problems before they become crises, developing that partner capacity, prior, not after, a response."[14] *We need to maneuver toward cognitive objectives.*

Objectives are a fundamental principle of Joint operations. They are one of the most important elements of operational design. They describe the specific goal to which operations are directed. Objectives orient a force along lines of operation and lines of effort to create desired outcomes. Generally, Joint and Army doctrine describe how to apply capabilities toward physical objectives, such as securing entry points or isolating populations. However, when we look at challenges in the operational environment, like Russian aggression, we see the orientation of capabilities toward wholly different kinds of objectives — cognitive ones. These include marginalizing factional influencers, mobilizing popular support, and promoting specific languages or cultures.[15] These kinds of efforts entail arranging multi-domain capabilities in a different manner than that of applying force. Therefore, what would a pre-crisis campaign that took a "people-access" approach, predominantly toward cognitive objectives, look like?

The Operational Framework

We need a framework — a form of scaffolding — to organize activities toward physical and cognitive objectives. That framework broadly comprises six elements: understanding the human environment, visualizing and shaping the security environment, engaging with partners, societies, and influential actors, influencing decision behaviors, acting on perceived security challenges and reframing baseline understanding of the human environment. These broad groupings are recast ideas generally contained within current Joint and Army doctrine. We recast them here to describe an

> *"[we need a] people-access approach: being there ahead of time, having relationships there ahead of time, identifying problems before they become crises, developing that partner capacity, prior, not after, a response."*
>
> — General Tony Thomas, CDR, USSOCOM, 25 May 2016

[13] JOE 2035, p. iii.
[14] Thomas, Raymond "Tony" General as cited by Patrick Tucker. *America's New Special Operations Commander Wants to Predict the Future.* May 25, 2016. http://www.defenseone.com/threats/2016/05/americas-new-special-operations-commander-wants-predict-future/128583/ (accessed August 10, 2016).
[15] Specific examples of these kinds of objectives can be seen in Russia's approach to annex Crimea and instigate conflict with Ukraine. See JHU Study, pp. 51-62.

assembly of activities that could be more coherently synchronized, but in practice may not be.[16]

Figure 1 shows that below a certain security threshold a campaign's objective is to maintain continual positions of advantage — to continually manage a change-state rather than to enforce an end state. *If successful, such a campaign would influence the trajectory of events without triggering a more forceful intervention*. However, when the security environment crosses a security threshold, the Joint force intent changes to dominating the security situation, to seeking a particular end state. These actions to dominate the situation would take place within the Joint construct of Major Combat Operations (MCO).

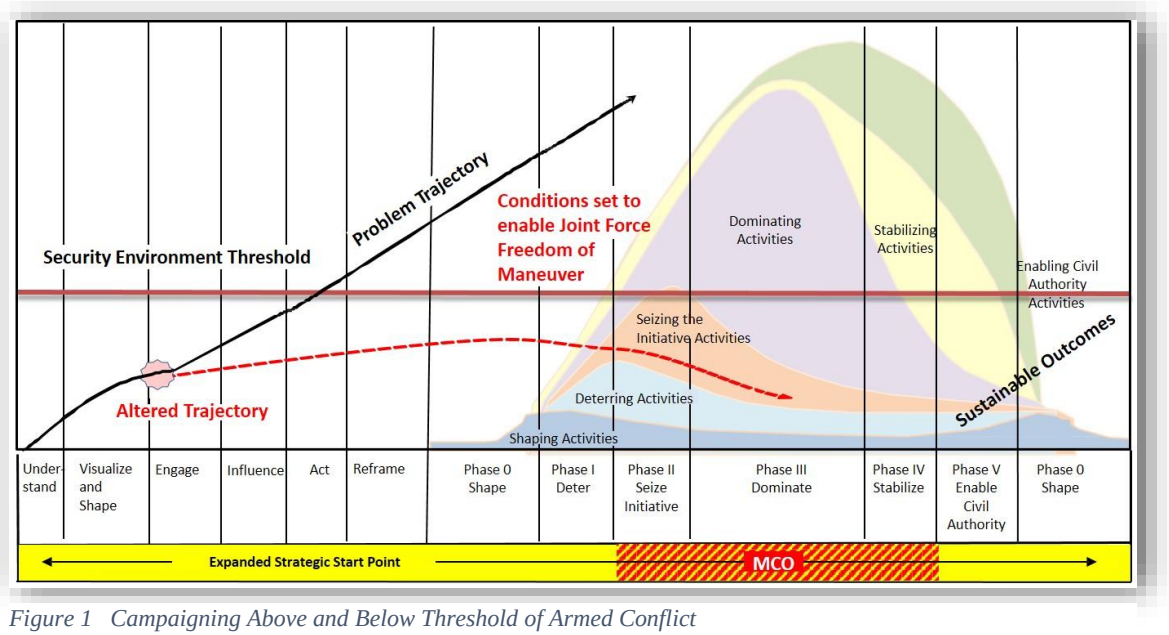


Figure 1 Campaigning Above and Below Threshold of Armed Conflict

While traditional approaches are vital, a cognitive maneuver approach matters to such security challenges as those that we currently see in the Gray Zone and traditional Phase 0. The nature of a campaign approach below the security threshold should be distinct from traditional ones. Key elements of operational design must be reframed, such as the military end state, objectives, termination, culmination and arranging operations.[17] Security environments below a threshold of major conflict demand altogether different thinking about how they comprise perpetual campaigning. The demand for altogether different thinking also applies above that threshold because complex terrain including empowered and dense human populations restrict freedom of action. That is why this paper argues for an open-ended campaigning framework — one guided

[16] The contemporary idea of campaigning during a non-war setting comes from the Joint concept of Phase 0 operations. Phase 0 came into Joint parlance around 2006 as way to describe the complementary activities that GCCs were conducting in support of CENTCOM efforts to directly combat terrorism through Operations ENDURING FREEDOM and IRAQI FREEDOM. For more see, Wald, Charles F., General. "The Phase Zero Campaign." *Joint Force Quarterly*, no. 43 (4th Quarter 2006): 72-75, p. 72.

[17] "Joint Operation Planning." *Joint Publication 5-0.* Washington, D.C.: Joint Chiefs of Staff, August 11, 2011, p. III-18. Elements of operational design are conceptual tools that help commanders and staffs think through critical planning considerations in the design of operations and campaigns.

by the balanced arrangement of physical and cognitive objectives to orient operations toward physical and cognitive maneuver approaches.

Understand

Commanders' tasks include "understanding, visualizing, describing, directing, leading, and assessing operations."[18] Doctrinally, understanding is the meaning derived from data and information synthesized to generate knowledge.[19] In the context of aggressive competition and theater setting activities, this task to understand largely emphasizes understanding an environment comprised of human characteristics. To do this commanders must extend their operational reach conceptually into the deep area of operations, proactively developing understanding and wielding influence. One critical observation notes this requirement: "Current thinking has concluded that military doctrine has been too focused on hard power, hardware and technology…and has tended to ignore, downplay, or simply misunderstand the vital role of what [Clausewitz] termed 'the clash of wills.'"[20]

Visualize and Shape

As we visualize the battlefield geometry for the application of power in a hyper connected world, our understanding of how we prepare maneuver space in the deep and close battle area will likely need to change. Shaping needs to be a continual process of adapting conditions that a Joint force can use to access crisis-afflicted areas or mitigate crises. Current Joint doctrine describes how "joint capabilities in military engagement, security cooperation, and deterrence activities helps *shape* the operational environment and keep the day-to-day tensions between nations or groups below the threshold of armed conflict."[21]

Engage

Part of understanding — of generating deep knowledge of an area — comes from persistent engagement with partners and populations, which is where we join social interactions. Decision makers can seize the initiative early by generating cognitive mass through indigenous approaches that combine the power of populations and partners. One goal of engagement is to circumvent potential conflict, while a broader aim is to curtail the exacerbation of conflict by getting into the environment and participating in it. One multinational study recognizes that "The goal is…not to prevent conflict *per se* but to *engage* with it in ways that seek to bring about positive change."[22]

---

[18] "Mission Command." *ADRP 6-0, C2.* Washington, D.C.: Headquarters Department of the Army, March 28, 2014, p. V.
[19] Ibid, p. 2-7.
[20] Great Britain, Austria, Canada, Finland, Netherlands, Norway, United States of America. "Understand to Prevent: The military contribution to the prevention of violent conflict." *Government of the U.K.* November 2014. https://www.gov.uk/government/publications/understand-to-prevent-the-military-contribution-to-the-prevention-of-violent-conflict (accessed July 8, 2016), p. 15. Hereafter U2P 2014.
[21] "Joint Operations." *Joint Publications 3-0.* Washington, D.C.: Joint Chiefs of Staff, August 11, 2011, p. V-1. Emphasis added.
[22] U2P 2014, p. 11. Emphasis added to "*engage*."

Influence

According to Joint doctrine, "A campaign is a series of related major operations aimed at achieving strategic and operational objectives within a given time and space."[23] Influence causes an adversary or relevant population to behave in a manner that broadens strategic options to attain campaign objectives. The ability to "alter the behavior of the other side" is a function of the ability to "outthink an opponent to gain and maintain the initiative," especially when war fighting is "fundamentally [a] human clash of wills often fought among populations."[24] This could mean a broad application of actions and messages that promote a narrative. It could also mean precision targeting operations that create multiple dilemmas for an adversary's ability to maintain unity. Generating influence depends upon a deep and nuanced understanding of the human terrain along with an ability to wield influence. Because it is rooted in human aspects of military operations, influence is perishable. It requires persistent understanding of to maintain them, extend them, and increase them.

Act

Joint Forces act on security challenges to attain their campaign objectives by means of concerted physical actions and cognitive activities. Physical actions and cognitive activities should serve to strengthen influence. Together, they set the conditions for reframing our baseline understanding of the human dimension across the range of military operations. Together they also give the Joint force flexibility to respond in crises. Crisis response reduces friendly vulnerability to acute and evolving surprises preventing an adversary from acquiring an unexpected advantage.

Reframe

Essentially, reframing our baseline understanding of the human environment integrates the lessons learned from the other five elements of the cognitive approach to campaigning. It results in a deeper, more nuanced level of understanding. This understanding improves our ability to attain objectives by either avoiding mistakes or reinforcing success. To succeed it demands honesty, objectivity, and a willingness to be brutally self-critical.

Implications to Campaigning – a Cognitive Maneuver Approach

Upon that framework, we can then design operational approaches that fit the specific security challenge context. Some security challenges will be focused on competing with aggressive states that push the boundaries of competitive statecraft.[25] Others will involve tamping the effects instability caused by destabilizing non-state actors.[26] In many cases, their character changes the rules of the game, so to speak, by remaining below a threshold that would trigger an MCO

---

[23] "Doctrine for the Armed Forces of the United States." *Joint Publication 1*. Washington, D.C.: Joint Chiefs of Staff, March 25, 2013, p. I-9.
[24] "Operations," *Army Doctrine Publication 3-0*. Washington, D.C.: Headquarters, Department of the Army, November 11, 2016, p. 2. Hereafter, ADP 3-0.
[25] AWC Gray Zone Study, p. 4. State interactions that push the boundary of normal relations are viewed as "high-stakes statecraft."
[26] AWC Gray Zone Study, p. 5. Non-state interactions that elicit an international security response are a function of "destabilizing forces."

intervention. Depending on the context of the security challenge, wholly different operational approaches should be designed to overcome them.

Contexts

Whether operating above or below an armed conflict threshold, campaign objectives should be both cognitive and physical. They include affecting beliefs, opinions, and decisions as well as securing people and terrain. Consider the variety of permutations campaign designers could arrange to overcome the following context-specific security challenges.

- State competition such as Russia's aggressive actions in Eastern Europe
- Non-state aggression such as the pursuit of a caliphate by ISIS
- Revision of international norms and rules such as China's expansion into the South China Sea
- U.S. foreign policy moves that appear provocative to some, such as the strategic pivot to Asia.[27]

Each context necessitates arranging a multitude of Joint and indigenous capabilities in time and space to sequence overlapping cognitive and physical outcomes. Those outcomes should also complement the variety of competitive engagement capabilities throughout the USG.[28] Incidentally, the United States Army Special Operations Command (USASOC) has been examining similarly contextual security challenges — specifically using cognitive maneuver — by testing several approach methodologies through its SILENT QUEST experimentation platform.

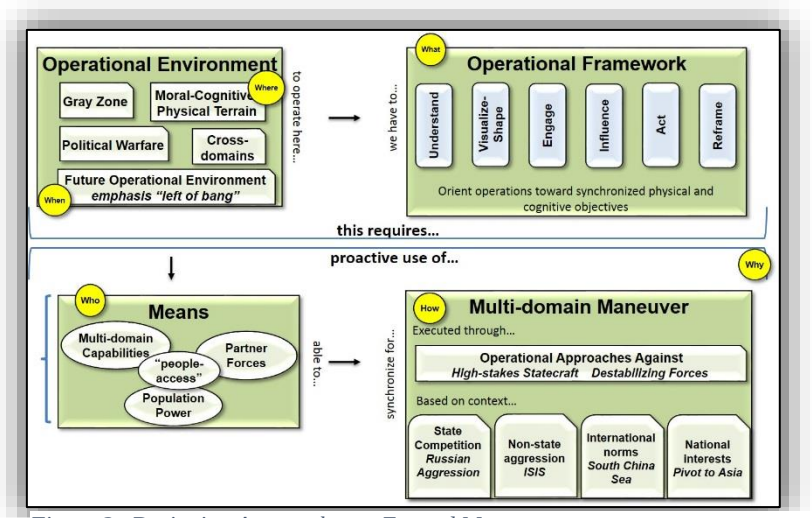


Figure 2 Designing Approaches to Expand Maneuver

Theory to Practice

In 2014, SILENT QUEST exercises looked at the impact of state competition and shaping theater conditions to uphold international norms. In 2015, SILENT QUEST 15-1 and 15-2 both looked at generational approaches to getting ahead of emerging non-state aggressors. In 2016,

[27] From 2010-2011, the President and his administration began messaging a shift in strategic priorities from Europe and the Middle East to Asia and the Pacific. This "pivot to Asia" or rebalance to Asia is expressly captured in his remarks made to the Australian Parliament in 2011. The policy was formally proposed in an essay by Secretary of State, Hillary Clinton. See Clinton, Hillary. "America's Pacific Century: The Future of Geopolitics will be decided in Asia, not in Afghanistan or Iraq, and the United States should be right at the center of the action." *Foreign Policy*, no. 189 (November 2011): 56-63.

[28] Schadlow, Nadia. "Competitive Engagement: Upgrading America's Influence." *Small Wars Journal.* November 5, 2012. http://smallwarsjournal.com/printpdf/13476 (accessed August 17, 2016). Schadlow describes competitive engagement as a shift from using military tools to define foreign policy to using civilian, diplomatic tools.

SILENT QUEST 16-1 wargamed both physical maneuver approaches and one centered around cognitive maneuver in a scenario focused on state competition. The most recent exercise, 16-2, looked at how an integrated theater staff could do cognitive maneuver campaigning in a near real-time security environment below the threshold of armed conflict.

The consistent takeaway from SILENT QUEST is that efforts emphasizing human domain activities more effectively get ahead of emerging security challenges. In other words, maneuver approaches synchronizing a blend of cognitive and physical objectives provide early off-ramps to alter the trajectory of those security problems.

A common counter argument from many organizations and participants with regard to existing processes is "Well, we do that already." Yes they do, but no they do not. People within different disciplines do separate aspects of cognitive maneuver. Military Information Support Operations (MISO) practitioners do convey messages. Practitioners within the Information Operations (IO) discipline do perform various activities to affect perceptions. Civil Affairs teams do engage with host nation populations. Organizations within the cyber proponency do engage in an information environment, and so on.

They all do a function related to maneuver, but are they united by a common purpose? Are they synchronized within an organizing framework to achieve operational objectives or a sequence of operational objectives? The short answer to that question is no. There has been a real struggle to orchestrate information related capabilities in a coherent manner toward a synchronized objective. Consequently, operational designs tend to favor traditional thinking that decisive actions comprise activities that sequence the arrangement of force and forces. However, an analysis of the way Russia has waged warfare in recent years indicates their decisive actions are largely information related operations that are supported by tactical ground maneuvers. That is why we urge rethinking the way the Joint force conceptualizes maneuver. The combination of all capabilities, arranged in time and through physical, virtual, and cognitive spaces, oriented toward a particular cognitive objective is how this paper argues we need to expand maneuver.

The obvious question, then, is how? Answering this question will require a concerted effort to collaborate ideas among maneuver forces and those throughout the community of information related capabilities. This would entail reimaging our understanding of all these entities as maneuverists. Many ideas have already been recognized. Some include organizational changes akin to a Directorate of Understanding or a dedicated center for cognitive maneuver operations. Some include institutional adaptations like reorganizing operations centers to function as a team of teams — physical maneuver team and cognitive maneuver team. Other ideas center on a recasting of operational design, to more deliberately layer in cognitive objectives as part of the schema for operational maneuvers. Still others include doctrinal adaptations to better synchronize activities in human terrain with those across the land terrain. *Incidentally, the Army's recent publication of their foundational maneuver doctrine, ADP 3-0 lays the groundwork for this kind of rethinking by characterizing the operational environment as two integrated components:* ***human context and land operations****.*[29]

[29] ADP 3-0, p. iv.

How Do We Respond to the OE?

Planning traditional maneuver constructs for a security environment that Secretary of Defense Carter suggests is trans-regional, multifunctional, occurring across multiple domains is likely problematic. Sequencing actions through a physical movement and maneuver paradigm does not address the true character of security problems across the ROMO. There is an opportunity to expand the idea of maneuver to account for using capabilities to move both *force* and *ideas* in time and space. Underpinning such a synthesis is a recognition that maneuvering in the operational environment today takes place within the nexus of land and cognitive objectives.

This opportunity to innovate maneuver beyond the physical raises the potential for future JIM experiments and exercises — a key defense initiative outlined by Deputy Secretary of Defense, Robert Work.[30] One could envision coordinated innovation efforts driving toward a unified concept for how we interact with the security environment when that environment remains below a MCO threshold.

Conclusion

Today's challenges reveal that population-centric aspects of warfare are increasing and contribute to the more decisive features of conflict. Given our current adversary's approaches in the human environment, the Joint force needs to expand its view of maneuver to orient multi-domain operations toward objectives that are both physical and cognitive in substance. An expanded understanding of maneuver purposefully uses capabilities across multiple domains to move both *force* and *ideas* in time and space. Within this context, the Joint force's understanding of operational design should seize the initiative early through operational time by blending physical and cognitive objectives in a comprehensive multi-domain maneuver campaign.

[30] Work, Robert O. "Wargaming and Innovation." *Memorandum.* Washington, D.C.: Deputy Secretary of Defense, February 09, 2015.

References

Carter, Ash. "Taking the Long View, Investing for the Future." *Defense Posture Statement 2017*. Washington, D.C.: Department of Defense, February 2016.

Clinton, Hillary. "America's Pacific Century: The Future of Geopolitics will be decided in Asia, not in Afghanistan or Iraq, and the United States should be right at the center of the action." *Foreign Policy*, no. 189 (November 2011): 56-63.

"Doctrine for the Armed Forces of the United States." *Joint Publication 1*. Washington, D.C.: Joint Chiefs of Staff, March 25, 2013.

Freier, Nathan P., ed. "Outplayed: Regaining Strategic Initiative in the Gray Zone." Carlisle Barracks: Strategic Studies Institute and U.S. Army War College Press, June 2016.

Great Britain, Austria, Canada, Finland, Netherlands, Norway, United States of America. "Understand to Prevent: The military contribution to the prevention of violent conflict." *Government of the U.K.* November 2014. https://www.gov.uk/government/publications/understand-to-prevent-the-military-contribution-to-the-prevention-of-violent-conflict (accessed July 8, 2016).

Johns Hopkins University Applied Physics Laboratory. *"Little Green Men:" A Primer on Modern Russian Unconventional Warfare.* National Security Analysis Department, Fort Bragg: United States Army Special Operations Command, 2015.

"Joint Operating Environment 2035." Washington, D.C.: Joint Chiefs of Staff, July 14, 2016.

"Joint Operation Planning." *Joint Publication 5-0.* Washington, D.C.: Joint Chiefs of Staff, August 11, 2011.

"Joint Operations." *Joint Publications 3-0.* Washington, D.C.: Joint Chiefs of Staff, August 11, 2011.

Kofman, Michael, and Matthew Rojansky. *A Closer Look At Russia's "Hybrid War"*. Kennan Cable No. 7, Kennan Institute, Washington, D.C.: The Wilson Center, 2015.

"Mission Command." *ADRP 6-0, C2.* Washington, D.C.: Headquarters Department of the Army, March 28, 2014.

Obama, Barak. "Remarks by President Obama to the Australian Parliament." *The White House.* November 17, 2011. https://www.whitehouse.gov/the-press-office/2011/11/17/remarks-president-obama-australian-parliament (accessed August 12, 2016).

"Operations." *Army Doctrine Publication 3-0.* Washington, D.C.: Headquarters, Department of the Army, November 11, 2016.

Schadlow, Nadia. "Competitive Engagement: Upgrading America's Influence." *Small Wars Journal.* November 5, 2012. http://smallwarsjournal.com/printpdf/13476 (accessed August 17, 2016).

Sheftick, Gary citing General Mark Milley. "CSA explains how skeletal advisory brigades could regenerate force." *U.S. Army.* June 23, 2016. https://www.army.mil/article/170344/csa_explains_how_skeletal_advisory_brigades_could_regenerate_force (accessed September 9, 2016).

Shultz, George. "Low-Intensity Warfare: The Challenge of Ambiguity." *Current Policy No. 783.* Washington, D.C.: Unites States Department of State Bureau of Public Affairs, January 15, 1986.

Taleb, Nassim Nicholas, and Gregory F. Treverton. "The Calm Before the Storm." *Foreign Affairs* 94, no. 1 (2015): 86-95.

Testimony John Kerry Opening Statement Before the Senate Committee on Foreign Relations. April 8, 2014. http://www.state.gov/secretary/remarks/2014/04/224523.htm (accessed August 11, 2016).

Thomas, Raymond "Tony" General as cited by Patrick Tucker. *America's New Special Operations Commander Wants to Predict the Future.* May 25, 2016. http://www.defenseone.com/threats/2016/05/americas-new-special-operations-commander-wants-predict-future/128583/ (accessed August 10, 2016).

Wald, Charles F., General. "The Phase Zero Campaign." *Joint Force Quarterly*, no. 43 (4th Quarter 2006): 72-75.

Work, Robert O. "Wargaming and Innovation." *Memorandum.* Washington, D.C.: Deputy Secretary of Defense, February 09, 2015.

UNITED STATES ARMY

SPECIAL OPERATIONS COMMAND

White Paper

Comprehensive Deterrence

12 April 2016

Executive Summary.

The emerging concept of Comprehensive Deterrence is an initial effort to broaden strategic options for our National leaders to meet current and emerging security challenges. Comprehensive Deterrence internalizes the challenge from then Secretary of Defense Hagel's Defense Innovation Memorandum (15 November 2014) to pursue innovative ways to sustain and advance U.S military superiority for the 21st Century. Comprehensive Deterrence also acknowledges the guidance from General Martin Dempsey, Chairman of the Joint Chiefs of Staff, on 11 January 2015 when he noted that, "We're going to have to think our way through the future, not bludgeon our way through it."[1]

Comprehensive Deterrence seeks to expand upon traditional concepts of deterrence to account for the totality and the variety of the threats we face in the early 21st Century security environment. It posits that deterrence, particularly on the left-side of the operational continuum, is not only about preventing something from happening, but also about preventing something from escalating beyond our strategic depth and our capability to respond, in a manner consistent with our National values.

Comprehensive Deterrence is defined as the prevention of adversary action through the existence or proactive use of credible physical, cognitive and moral capabilities that raise an adversary's perceived cost to an unacceptable level of risk relative to the perceived benefit.

Key themes within the concept of Comprehensive Deterrence include: 1) Existing theories of deterrence generally focus on high-end conflict conducted by Nation States on the right-side of the operational continuum. Investment in deterrence thinking on the left-side of the operational continuum is warranted to meet the growing challenges the United States and its Allies face in the Gray Zone; 2) The totality of the security challenges and the varied nature of these challenges require reframing of what constitutes strategic power and strategic risk in a complex and unpredictable world; 3) The growing trans-regional aspects of competition and conflict require new planning models, new operational constructs, new ways of thinking, and fully integrated partner networks to rescale security challenges earlier in their trajectory; 4) Select state and non-state actors are effectively operating in the Gray Zone, which demands study of how we build the nuanced inter / intra governmental multi-year campaigns that are required to successfully compete and win in this space; and 5) Comprehensive Deterrence points to a grand strategy to deliver more effective security for the Nation.

The conceptual lines of effort within Comprehensive Deterrence are; 1) Expanding the Strategic Start Point, 2) Rethinking Strategic Power and Reframing Power Projection with two sub-components, Partner Based Power and Population Based Power, 3) Rethinking Asymmetric Approaches, 4) Rethinking the Strategic Nexus between the Land and Human Domains, 5) Broadening Considerations of Strategic Risk, and 6) Expanding Technology Solutions for the Human Domain.

Comprehensive Deterrence White Paper

The concept of Comprehensive Deterrence is an outgrowth of the United States Special Operations Command's (USSOCOM) and the United States Army Special Operations Command's (USASOC) futures and wargaming platforms. The adjective, comprehensive, speaks to deterrence across the operational continuum and to the application of a Whole of Government / Whole of Partner framework to enable its full realization.

Framing Assumptions.

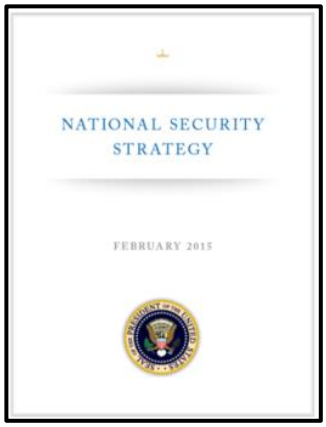
The following assumptions framing the emerging concept include; 1) The operating environment will remain complex, and disordered, 2) International norms will continue to constrain the application of force, 3) The totality and variety of the security challenges demand a relook at what constitutes strategic risk in the early 21st Century operating environment, 4) The fiscal reset will likely continue to reduce governmental resources which presents obvious challenges. However, it presents opportunities to consider new frameworks, new operational approaches and new capabilities, 5) The political will to conduct large scale military campaigns as the primary approach will likely continue to wane, and 6) The march of commercial technology and its militarization will likely accelerate in the coming years.

Central Idea. Existing theories of deterrence largely focus on deterring state adversaries capable of employing large scale conventional forces and nuclear weapons, with conflict occurring on the right-side of the operational continuum. The U.S. must always be ready to win decisively in this space, but must also be prepared to compete and win on the left-side of the operational continuum, in the Gray Zone between peace and war, where select state and non-state actors are effectively challenging U.S. and Allied interests.

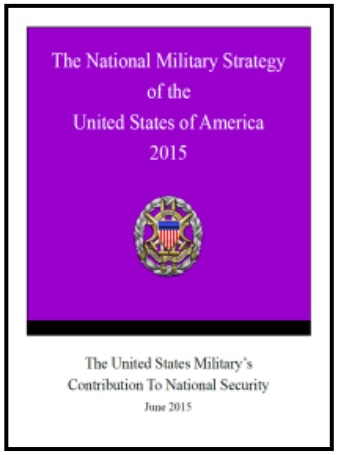
Based on the totality and complexity of security challenges facing the U.S. and its Allies, now and into the foreseeable future, we no longer have the luxury in terms of operational time, fiscal resources, and political will to allow these challenges to escalate to a level that exceeds our strategic depth and ability to respond, in a manner consistent with our National values.

We will lead with a long-term perspective. Around the world, there are historic transitions underway that will unfold over decades. This strategy positions America to influence their trajectories, seize the opportunities they create, and manage the risks they present. Five recent transitions, in particular, have significantly changed the security landscape, including since our last strategy in 2010. (February 2015 p.4-5)

- **Power among states is more dynamic.**
- **Power is shifting below and beyond the nation-state.**
- **The Increasing interdependence of the global economy and rapid pace of technological change are linking individuals, groups and governments in unprecedented ways.**
- **A struggle for power is underway among and within many states of the Middle East and North Africa.**
- **The global energy market has changed dramatically.**



The application of the military instrument of power against state threats is very different than the application of military power against non-state threats. We are more likely to face prolonged campaigns than conflicts that are resolved quickly…that control of escalation is becoming more difficult and more important…and that as a hedge against unpredictability with reduced resources, we may have to adjust our global posture. (June 2015 p. i)



Introduction.

This concept has been informed by the National Security Strategy (2015), National Military Strategy (2015) the Defense Innovation Initiative Memorandum (2014), and the Defense Wargaming and Innovation Memorandum. It has also been informed by USSOCOM's SHADOW WARRIOR, the Army's UNIFIED QUEST and USASOC's SILENT QUEST futures and wargaming platforms. It was also informed by the senior leader insights from USASOC's Modern Russian Unconventional Warfare Case Study Forum in March of this year. Further insights were generated during USSOCOM 's Comprehensive Deterrence Workshop in August of this year This effort to broaden strategic options has also been informed by Secretary of Defense Carter's and former Secretary of Defense Perry's book, Preventive Defense, A New Security Strategy for America.

This concept internalizes three critical takes from the National Security Strategy (2015) and the National Military Strategy (2015); 1) Historic global transitions are underway that must be understood and influenced where and when possible, 2) The totality of the security challenges we face and their varied nature requires reframing of what constitutes strategic power and strategic risk in a complex and unpredictable world; and 3) Delivering more effective security outcomes for the U.S. and its Allies requires a new paradigm, a new planning model, a new operational approach, and fully integrated partner networks to conduct the nuanced inter / intra governmental campaigns to win in the Gray Zone.

Strategic Appreciation in the Early 21st Century Security Environment.

We no longer have the luxury in terms of operational time, fiscal resources, and political will to allow security challenges to escalate to a level that exceeds our strategic depth and ability to respond.

Existing theories of deterrence largely focus on deterring state adversaries capable of employing large scale conventional forces and nuclear weapons, with conflict occurring on the right-side of the operational continuum. The U.S. and its Allies must always be ready to win decisively in this space, but we must also be ready to compete and win on the left-side of the operational continuum, in the space between peace and war, where select state and non-state actors are effectively challenging our interests.

The hypothesis for the emerging concept of Comprehensive Deterrence is that in the current and emerging global security environment, deterrence is not only about preventing something from happening, but also about preventing something from escalating beyond our strategic depth and capability to respond, by imposing, in a manner consistent with our National values, what adversaries perceive as increased costs and risks for their actions.

Strategic Guidance.

The National Security Strategy (2015) states that "Five recent transitions, in particular, have significantly changed the security landscape, including since our last strategy in 2010 ... power among states is more dynamic ... power is shifting below and beyond the nation-state … the increasing interdependence of the global economy and rapid pace of technological change are linking individuals, groups, and governments in unprecedented ways … a struggle for power is underway among and within many states of the Middle East and North Africa… the global energy market has changed dramatically."[2]

Further, the National Security Strategy (2015) also notes that "more than 50 percent of the world's people are under 30 years old. Many struggle to make a life in countries with broken governance. We are taking the initiative to build relationships with the world's young people, identifying future leaders in government, business, and civil society and connecting them to one another and to the skills they need to thrive. The popular uprisings that began in the Arab world

took place in a region with weaker democratic traditions, powerful authoritarian elites, sectarian tensions, and active violent extremist elements, so it is not surprising setbacks have thus far outnumbered triumphs. Yet, change is inevitable in the Middle East and North Africa, as it is in all places where the illusion of stability is artificially maintained by silencing dissent."[3]

The National Military Strategy (2015) states that "the application of the military instrument of power against state threats is very different than the application of military power against non-state threats. We are more likely to face prolonged campaigns than conflicts that are resolved quickly…that control of escalation is becoming more difficult and more important…and that as a hedge against unpredictability with reduced resources, we may have to adjust our global posture."[4]

The National Military Strategy (2015) establishes the following national objectives: "deter, deny, and defeat state adversaries; disrupt, degrade, and defeat violent extremist organizations; and strengthen our global network of allies and partners."[5]

It is imperative, given the challenges posed by the contemporary and future operating environment, that the U.S. and its Allies consider new approaches to deliver more effective security in the 21st Century.

The Operating Environment.

The foreseeable future is characterized by complexity, scarcity of resources, ecological challenges, compelling ideologies, game-changing technologies, resistance movements and opportunistic competitors employing multiple capabilities. A survey of conflict over the past 200 years indicates that 80 percent of conflicts were irregular in nature and that this trend is likely to continue.[6] The Global Trends 2030 Report, *"Alternative Worlds"*, from the National Intelligence Council (NIC), forecasts an increasing diffusion of power to regional competitors and non-state actors.[7]

Secretary of Defense Secretary Carter's and former Secretary of Defense Perry's book, Preventive Defense, A New Security Strategy for America, 1999, states that "Preventive Defense is a defense strategy for the United States in the twenty-first century that concentrates national security strategy on the dangers that, if mismanaged, have the potential to grow into true A-list-scale threats to U.S. survival in the next century, bringing the current era to an abrupt and painful end. These dangers are not yet threats to be defeated or deterred; they are dangers that can be prevented".[8]

In his recent book Strategic Vision, former U.S. National Security Advisor Zbigniew Brzezinski noted "the changing distribution of global power and the new phenomenon of mass political awakening intensify, each in its own way, the volatility of contemporary international relations. Accordingly, the U.S. must seek to shape a broader geopolitical foundation for constructive

cooperation in the global arena, while accommodating the rising aspirations of an increasingly restless global population."[9]

USSOCOM's recently published White Paper, *"The Gray Zone"*, further highlights new global security challenges. "The current international order is largely a Westphalian construct, emphasizing human rights, free market economies, sovereignty of the nation-state, representative government and self-determination. In the past, Gray zone challenges typically emanated from state-sponsored groups or nation-states adopting strategies seeking to avoid escalation. Now, non-state and proto-state organizations such as al Qaeda and Daesh (ISIS) can amass resources and connect enough formerly disparate individuals to constitute threats that cannot be ignored… Nation-states remain strong cornerstones of the international system, but the myriad of challenges they face are proliferating and strengthening faster than states' powers. Any international system maintaining a reasonable level of world order must account for numerous powerful non-state actors and multiple sources of legitimacy and governance."[10]

The U.S. and its Allies must consider evolving trends in international competition and conflict and the associated impact on the global security environment.

Evolving Considerations of Deterrence.

Secretary of Defense Melvin Laird published the "National Security Strategy of Realistic Deterrence" on February 22, 1972, in which he described the national security challenges facing the nation. The strategy acknowledged growing fiscal constraints, the political impact of a decade of war in Vietnam, and the emerging challenges presented by the Soviet Union. Laird described the ultimate goal of the strategy is "to discourage - and ultimately to eliminate - the use of military force as a means by which one nation seeks to impose its will upon another."[11] Furthermore, the strategy asserted the primacy of sustaining nuclear capabilities and the "nuclear umbrella." The strategy advocated applying all the elements of national power across the entire operational spectrum by maintaining deterrence through nuclear and technological means as well as addressing a range of lesser threats and building partner capabilities. "The basic purpose of this implementing strategy is to provide, through strength and partnership, for the security of the United States and its Free World allies and friends … It seeks to deter war, but insures adequate capabilities to protect our nation and its interests should deterrence fail."[12]

The National Security Strategy of January 1987 reflects a more traditional approach to deterrence resulting from the longstanding bipolar challenges of the Cold War, stating "deterrence is the most fundamental element of our defense policy and the cornerstone of our alliance relationships. Deterrence must not only prevent conventional and nuclear attack on the United States, but must extend such protection to our allies. Deterrence can best be achieved if our defense posture makes the assessment of war outcome by the Soviets or any other adversary as dangerous and uncertain as to remove any possible incentive for initiating conflict.

Deterrence depends both on nuclear and conventional capabilities, and on evidence of a strong will to use military force, if necessary, to defend our vital interests."[13]

The National Security Strategy for a New Century, May 1997, begins to reflect a more active approach to deterrence as a result of numerous late 20th Century crises such as Iraq and Bosnia, stating "when efforts to deter an adversary occur in the context of a crisis, they become the leading edge of crisis response. In this sense, deterrence straddles the line between shaping the international environment and responding to crises. Deterrence in crisis generally involves signaling the United States' commitment to a particular country or interest by enhancing our warfighting capability in the theater. The U.S. may also choose to make additional declaratory statements to communicate the costs of aggression or coercion to an adversary, and in some cases may choose to employ U.S. forces in a limited manner to underline the message and deter further adventurism."[14]

In more recent history, as a result of the attacks of September 11, 2001, we witnessed the reevaluation of the United States' approach to addressing divergent asymmetric threats in the application of national power. The National Security Strategy of 2002 posited that "traditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents; whose so-called soldiers seek martyrdom in death and whose most potent protection is statelessness."[15]

As we move forward, U.S. strategic approaches must continue to evolve to provide effective security for the Nation.

Deterrence theory is not new, though the application of deterrence thinking to Gray Zone challenges requires a critical examination of existing paradigms and the utilization of all elements of national power.

Defining Comprehensive Deterrence.

First, it is important to make a distinction between "Prevention" and "Deterrence". Joint Publication 3-0, Joint Operations, defines deterrence as "The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[16] "Prevention" is distinct from "Deterrence" in that prevention is about averting something from ever existing and deterrence is about averting something from happening. It is possible to get far enough *left* of a problem (i.e. during peacetime steady state operations) to recognize the indicators and warnings of nascent threats, and apply measures very early on to avert these threats long before they materialize.

The premise of the concept of Comprehensive Deterrence is that in an era of neither peace nor war (i.e. persistent conflict), where multiple threats are altering the global security environment to the extent that prevention is no longer an option, or at least no longer a priority, the focus now must be on deterrence - preventing these threats from acting, or at a minimum from escalating beyond our strategic depth and ability to respond, underpinning the hypothesis: **"In the current**

and emerging security environment, deterrence, particularly on the left-side of the operational continuum, is not only about preventing something from happening, but also about preventing something from escalating beyond our strategic depth or capability to respond, in a manner consistent with our National values."

Referencing the totality and variety of the security challenges, GEN Dempsey noted "since the last military strategy was published in 2011, global disorder has significantly increased while some of the military's comparative advantage has begun to erode. We now face multiple, simultaneous security challenges from traditional state actors and trans-regional networks of sub-state groups - all taking advantage of rapid technological change."

In a world characterized by increased complexity and unpredictability, "Comprehensive Deterrence" recognizes the need to expand deterrence thinking beyond high end conventional or nuclear capabilities, and consider threats to national security across the range of actors and spectrum of conflict. Though the pre-conflict space (i.e. left-side of the operational continuum) has and will continue to be Department of State led, strategic guidance suggests a Whole of Government approach with increased DoD support is critical to assess, sort, form a response, and rescale security threats long before they spiral beyond the Nation's strategic depth and ability to respond.

In consideration of security threats and capabilities across the continuum, **Comprehensive Deterrence is defined as "prevention of adversary action through the existence, or proactive use of credible physical, cognitive and moral capabilities that raise an adversary's perceived cost to an unacceptable level of risk relative to the perceived benefit."**

GEN Dempsey notes "the National Military Strategy describes how we will employ our military forces to protect and advance our national interests. We must be able to rapidly adapt to new threats while maintaining comparative advantage over traditional ones. Success will increasingly depend on how well our military instrument can support the other instruments of power and enable our network of allies and partners."[17]

There is a strong correlation between Preventive Defense and ideas within Comprehensive Deterrence as both seek to broaden considerations of (strategic) power. The ideas within Comprehensive Deterrence are consistent with Secretary of Defense Carter's book in that it considers the expansion of deterrence beyond its traditional military frame, while also taking into account changes in the security environment since the book was published in 1999. "Preventive Defense is a defense strategy for the United States in the twenty-first century that concentrates national security strategy on the dangers that, if mismanaged, have the potential to grow into true A-list-scale threats to U.S. survival in the next century, bringing the current era to an abrupt and painful end. These dangers are not yet threats to be defeated or deterred[18]; they are dangers that can be prevented."[19] Furthermore, "As a guide to national security strategy, Preventive Defense is fundamentally different from deterrence[20]: it is a broad politico-military strategy, and therefore draws on all the instruments of foreign policy: political, economic, and military".[21]

There is some debate as to whether non-state actors, or even individuals, can be deterred, but that discussion is far from settled. Though those bent on wanton destruction and mass murder in the name of their religion don't have the same cost calculus or possess the same assets to put at risk as a nation state, and may at first appear to be not able to be deterred, "martyrdom" achieved through a highly successful terrorist act is much preferred to that resulting from a failed or lackluster effort. So perhaps the focus could be on deterrence through the delay or denial of action. The main point here is that we recognize containing or disrupting these threats is a strategic imperative…and through deterrence activities in this space, we can successfully prevent these threats from spiraling beyond our strategic depth and ability to respond.

The formulation of the concept and definition of Comprehensive Deterrence centers on six conceptual lines of effort; 1) Expanding the Strategic Start Point, 2) Rethinking Strategic Power and Reframing Power Projection with two sub-components of Partner Based Power and Population Based Power, 3) Rethinking Asymmetric Approaches, 4) Rethinking the Strategic Nexus between the Land and Human Domains, 5) Broadening Considerations of Strategic Risk, and 6) Expanding Technology Solutions for the Human Domain.

Integrating the Comprehensive Deterrence lines of effort into existing Joint and Partner capabilities will serve to broaden strategic options for the U.S. and its Allies in the early 21st Century security environment.

Expanding the Strategic Start Point.

The totality of the security challenges facing the U.S. and its Allies and the evolving character of these threats require an operational framework to win early to prevent these challenges from scaling beyond the Nation's strategic depth and ability to respond. An earlier "Strategic Start Point" requires new thinking about the traditional military Phase 0 and most importantly for this effort, new thinking about "Left of Phase 0" campaigns and operations to consider how we assess, sort, form a response and rescale security challenges to win early and preserve strategic depth and decision space for our National Leaders. The framework for this approach centers on a persistent forward presence in and around the people with deep knowledge of the environment to generate decisive situational awareness to better inform the strategic start point for campaigns where the "Win" occurs at a much lower level of National effort. An example of this approach is the U.S. effort to aid the El Salvadoran Government from 1980-1992, which cost approximately $6.0 billion, and consisted of 55 U.S. in-country advisors enabled by an out of country support element that assisted the government in the defeat of the communist backed Farabundo Martí National Liberation Front (FMLN) insurgents.

An expanded strategic start point demands a focus far left of the traditional JOPES Phase 0 construct to assess, sort, form a response, and rescale security threats earlier in their trajectory at a much lower level of effort and risk.

Rethinking Strategic Power and Reframing Power Projection.

Traditional considerations of power projection generally center on long-range stand-off or expeditionary capabilities. Rethinking strategic power to address security challenges emanating from the left-side of the operational continuum considers power beyond traditional warfighting capabilities to examine the full range of National, Allied, Partner, and Population based power. Reframed power projection envisions leveraging bi-lateral capabilities through a focus on extant partner and population based power in and around the operational area in support of nuanced and persistent "Left of Phase 0" campaigns to mitigate threats early in their development and risk profile. In an era of persistent conflict and a political setting wary of large scale military intervention, the utilization of indigenous mass is a fundamental component of power projection.

Partner-Based Power. Partner based power is a vital component of Comprehensive Deterrence and centers on persistent presence to shape, develop, enable, and integrate indigenous governments, militaries, and security forces into a broader consideration of strategic power. It focuses on developing and leveraging host nation capabilities to produce extant power forward to achieve relative superiority over the physical, cognitive, and moral security of key populations and locations in areas we choose to campaign. Enabling partners to provide for the needs of the populace, ensure their own internal security, or to conduct operations either unilaterally or as part of an international coalition substantially increases the capability and capacity of the U.S. and its Allies to address global security challenges[22]. At its core, partner based power is centered on operating "with and through" foreign governments, militaries, security forces, and non-governmental organizations[23] to support local, regional, and global deterrence efforts. Operations in Colombia, El Salvador, and the Philippines offer contemporary examples of partner based power.

Population-Based Power. Population-based power is also a vital component of Comprehensive Deterrence and centers on persistent influence to shape, develop, enable, and integrate local perceptions, attitudes, behaviors, decision making processes, and actions into broader considerations of strategic power. Population-based power relies upon influence over time to address trends in international competition to achieve relative superiority over the physical, cognitive, and/or moral security of key populations in areas we choose to campaign. Population based power includes actions and/or messaging to encourage desired behavior in targeted populations, such as support to legitimate government, counter-radicalization, counter VEO recruitment, etc., or in semi-permissive or denied environments, leveraging select populations, groups, or individuals to facilitate moderation of adversarial regime objectives or policies, or in extreme cases, to facilitate regime change. Persistent influence requires a Whole of Government approach leveraging the Diplomatic, Informational, Military, and Economic (DIME) aspects of power to achieve desired behaviors and actions in indigenous populations in a manner that impacts the adversary's cost calculus. Population based power focuses on achieving desired behaviors in targeted populations, or in some cases operating "with and through" relevant persons and populations, both of which are designed to create indigenous mass forward to

support local, regional, and global deterrence efforts. The "Arab Spring" revolts offer a compelling example of the potential for leveraging population based power.

Reframed power projection leverages bi-lateral capabilities through a focus on extant partner and population based power in and around the operational area in support of nuanced and persistent "Left of Phase 0" campaigns to mitigate threats early in their development and risk profile. Persistent presence and influence that enables partner and population based power significantly increases the capability and capacity of the U.S. and its Allies to respond to global security challenges.

Rethinking Asymmetric Approaches.

Joint Publication 1-02 defines asymmetry in military operations as "the application of dissimilar strategies, tactics, capabilities, and methods to circumvent or negate an opponent's strengths while exploiting his weaknesses."[24] "Asymmetric approaches on the left side of the operational continuum seek to optimize forces, capabilities, relationships and operational trust to achieve relative positional advantage in operational time and space to checkmate a competitor's strengths and exploit his weaknesses."[25] One form of asymmetry that warrants further examination is a revitalized variant of Political Warfare. During the Cold War, Political Warfare was a highly sophisticated approach to competing with the former Soviet Union in the contested space between peace and war. In the 21st Century, Political Warfare could serve to inform a thoroughly modern Whole of Government approach to achieve unity of purpose and effort through integrated strategies and cohesive policy options. Modern Political Warfare has the potential to become the centerpiece of deterrence activities on the left-side of the operational continuum, employing subtle, synergistic, and evolving "overt, covert, and clandestine" tools with an emphasis on coercive diplomatic and economic engagement, Security Sector Assistance (SSA), Influence activities, and diverse forms of Unconventional Warfare (UW).[26] An asymmetric approach to deterrence in the Gray Zone focuses on understanding an adversary's strategic objectives from their cultural and ideological perspective, and presenting multiple physical, cognitive, and moral dilemmas that alter their cost calculus, presenting risks or consequences that outweigh the perceived benefit.

Asymmetric approaches on the left side of the operational continuum optimize forces, capabilities, relationships and operational trust to achieve relative positional advantage in operational time and space to checkmate a competitor's strengths and exploit his weaknesses.

Rethinking the Strategic Nexus between the Land and Human Domains.

There is an emerging recognition of the strategic nexus between the land and human domains. Economic, social, political, informational, and ideological trends in international competition are converging among State, Non-State actors, and others for the relative superiority over the physical, cognitive, moral security and adequate governance of populations and increasingly, in a hyper-connected world, the traditional concepts of sovereignty and identity.

The characterization of these trends and the inherent challenges they present is best described in USSOCOM's White Paper "*The Gray Zone*". "Some level of aggression is a key determinant in shifting a challenge from the white zone of peacetime competition into the Gray Zone. The U.S. seeks to address disputes through diplomacy, but has always reserved the right to take military action to defend its interests…The post-World War II international system was established by and to the advantage of the United States and the West. A slew of state and non-state actors now aggressively oppose this Western-constructed international order, but in ways that fall short of recognized thresholds of traditional war. In simple terms, we understand war and peace and how to act during these instances, but there is a vast range of conflicts between these well-understood poles where we struggle to respond effectively."[27] This speaks to the need for an integrated framework that can generate the inter / intra governmental approach this space demands.

Current Department of the Defense planning focuses primarily on campaigns designed for use on the right-side of the operational continuum with the focus of reducing and / or eliminating an adversary's physical forces. Campaigns, in the space between peace and war, occur primarily in the Human Domain with the operational focus being on the population.

Of note, as part of the Defense Innovation Initiative, there is renewed emphasis on research and development in support of leap-ahead technologies to underpin a Third Offset Strategy, a component of which will likely include an examination of the applicability of AirLand Battle Doctrine to meet current and emerging security challenges. As part of this review, it will be critical to consider how we maneuver physically and cognitively across the entire operational continuum with emphasis on how we maneuver in the population-centric Gray Zone. To that end, understanding the strategic nexus between the Land and Human domains will be critical in framing a follow-on version of AirLand Battle.

Strategic success in a complex and unpredictable security environment will require greater understanding of the Human Domain and will demand new ways of thinking about the application of power.

Broadening Considerations of Strategic Risk.

The National Military Strategy identifies several risks, with note of the use of traditional military power against non-state threats, the growing importance and difficulty in controlling the escalation of conflict, and the need for a hedge against unpredictability.

The following assumptions frame the emerging concept include; 1) The operating environment will remain complex and disordered, 2) International norms will continue to constrain the application of force, 3) The totality and variety of the security challenges demand a relook at what constitutes strategic risk in the early 21st Century operating environment, 4) The fiscal reset will likely continue to reduce governmental resources which presents obvious challenges; however, it presents opportunities to consider new frameworks, new operational approaches and new capabilities, 5) The political will to conduct large scale military campaigns as the primary approach will likely continue to wane, and 6) The march of commercial technology and its militarization will likely accelerate in the coming years.

With regard to assumption 2), above, it is likely, in an increasingly hyper-connected world that can readily see and internalize the effects of war, that what is considered acceptable in the application of violence will have major implications for when and how the US and its Partners engage security challenges.

Reference assumption 3), above, the most telling example is highlighted in the foreword of the 2015 National Military Strategy where GEN Dempsey notes that "since the last military strategy was published in 2011, global disorder has significantly increased while some of our military comparative advantage has begun to erode. We now face multiple, simultaneous security challenges from traditional state actors and trans-regional networks of sub-state groups, all taking advantage of rapid technological change."[28]

Broadening considerations of strategic risk is a critical component of Comprehensive Deterrence requiring appropriate perspective, thinking, and models. Measuring strategic risk is a function of considering the following; 1) Positional Advantage: the degree to which we are able to assess, sort, form a response, and rescale challenges while preserving strategic depth and decision space, 2) Strategic Power: the degree to which adversaries are compelled to expend strategic power while we preserve ours, 3) Influence: the degree to which we retain influence, legitimacy, and prestige, 4) Governance: the extent to which we can set conditions for adequate governance, partner nation stability, and rule of law, 5) Access: the extent to which we are able to maintain physical, cognitive, and moral access to other countries and populations, and 6) Cumulative Effects: the degree to which we are able to mitigate the effects of multiple, simultaneous challenges that could potentially impact strategic depth and ability to respond.

We no longer have the luxury in time, resources, will, and norms to wait for security challenges to clearly present themselves as envisioned in the Joint Operations Planning (JOPES) construct. In the aggregate, Gray Zone security challenges pose a potential systemic risk to the U.S. and its Allies. The danger we face is failing to understand and to interdict the trajectory of these security challenges much earlier in their development.

Expanding Technology Solutions for the Human Domain.

Forward presence and proximity in and around populations is paramount to maintaining a competitive advantage in the Human Domain. To that end, technology based deterrence solutions have long been a key element in the national security calculus. During the Cold War deterrence required a new level of technological sophistication to counter the former Soviet Union and roll back the spread of Communism. Early on, the focus was on state-on-state conventional as well as nuclear capabilities enabled by a purposeful and robust investment in technology. In the 1970s, Secretary of Defense Harold Brown and Under Secretary William Perry implemented a plan to again emphasize advanced technology solutions to deter the former Soviet Union and gain technical superiority, but this time focused on stealth capabilities, precision strike weapons and improved command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).[29] Historically referred to as the First and Second Offset Strategies, both approaches enabled the US to attain a sizable, albeit temporary, comparative advantage over our adversaries.

The contemporary and future operating environment requires technology solutions for the Human Domain. Social, political, informational, and economic trends in international competition are converging among state, non-state actors, and others for relative superiority over key populations. Such technologies to address these complex challenges may include enhanced cyber-enabled collection and analytical capabilities leveraging open source information and a robust reachback to subject matter expertise to conduct social media exploitation and analysis, human terrain mapping, sentiment analysis, trend analysis, pattern-of-life analysis, and predictive analysis.

Leveraging technology solutions, informed by the social sciences, is fundamental in furthering our understanding of how we maneuver and better compete in the Human domain.

Key Findings to Date.

As noted earlier, the framing of the emerging concept of Comprehensive Deterrence has been informed by USSOCOM's and USASOC's futures and wargaming platforms with emphasis on the senior leader insights garnered from USASOC's Modern Russian Unconventional Warfare Case Study Forum from March of this year. Several key findings have emerged that support the emerging concept of Comprehensive Deterrence. These findings are binned in terms of policy, thinking, Strategic / Operational, and Institutional. In terms of policy, there is a need to develop a Defense Planning Scenario that exercises the deterrence of war and our readiness, across a Whole of Government framework, to compete in this space. In terms of thinking, there is a need to update Political Warfare for the early 21st Century security environment. In the strategic / operational bin, there is a need to develop strategic indicators and warning for the non-standard campaigns that state and non-state actors are pursuing on the left-side of the operational continuum. In the institutional bin, there is a need to develop a cadre of DoS and DoD planners

for campaigning in the Gray Zone. Finally, there is a need to define what a "Win" or strategic success looks like in the world we face. To that end, USASOC has attempted in its White Paper, "Redefining the Win in a Complex World," to outline the characteristics of a win. We acknowledge we are not done on this effort. However, given the rapidly changing security environment in the early 21st Century, a win may be more accurately framed as the retention of positional advantage in terms of time, forces and trust to advance U.S. and Allied interests. [30]

Conclusion.

State and non-state actors are increasingly employing irregular and hybrid strategies on the left-side of the operational continuum to achieve their objectives. Russia's actions in Eastern Europe, China's activities in the South China Sea and the rise of the virtual caliphate are contemporary examples that suggest a need to relook deterrence thinking and what a "Win" looks like in the Gray Zone.

Comprehensive Deterrence considers deterrence across the entire operational continuum to confront low and high-end competitors in the early 21st Century security environment. It offers a way to address the escalation of many security challenges we face earlier in their development and risk profile. In doing so, it will broadens strategic options in terms of time, decision space and approaches for our National leaders.

We must possess the thinking, capabilities and readiness to "Win" in the Gray Zone.

---

[1] General Martin Dempsey, interview by Chris Wallace, Fox News Sunday, Fox News, January 11, 2015, http://www.foxnews.com/on-air/fox-news-sunday-chris-wallace/2015/01/11/gen-dempsey-reacts-paris-attacks-sens-hoeven-coons-talk-keystone-showdown.
[2] *National Security Strategy of the United States* (Washington, DC: The White House, 2015), 4-5.
[3] *National Security Strategy of the United States* (Washington, DC: The White House, 2015), 21.
[4] *The National Military Strategy of the United States of America,* Washington D.C.: Chairman Joint Chief of Staff., 2015, i.
[5] *The National Military Strategy of the United States of America,* Washington D.C.: Chairman Joint Chief of Staff., 2015, 5.
[6] Sebastian Gorka, *Army Special Operations Forces Operating Concept Strategic Setting Paper*, Virginia Tech Applied Research Corporation and Threat Knowledge Group, September 2013, 7-8. See also Sebastian Gorka and David Kilcullen, "An Actor-centric Theory of War: Understanding the Difference Between COIN and Counterinsurgency," *Joint Force Quarterly* 60 (1st Quarter 2011), 14-18.
[7] National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington D.C.: U.S Government Printing Office, December 2012), ii. The Megatrends are individual empowerment, diffusion of power, demographic patterns, and food, water, energy nexus.
[8] Ashton Carter and William Perry, Preventive Defense: A New Security Strategy for America (Washington, DC: The Brookings Institute, 1999), 14.
[9] Zbigniew Brzezinski, *Strategic Vision: America and the Crisis of Global Power*, New York: Basic Books, 2013, 1.
[10] U.S. Special Operations Command, "The Gray Zone" White Paper (09 Sept 2015), 4.
[11] Melvin Laird, Secretary of Defense, "National Security Strategy of Realistic Deterrence," 17 February 1972, 21.
[12] Ibid, 2.
[13] *National Security Strategy of the United States* (Washington, D.C.: The White House, 1987), 21.
[14] *National Security Strategy of the United States* (Washington D.C.: The White House, 1997), 14-15.
[15] *National Security Strategy of the United States* (Washington D.C.: The White House, 2002), 15.

[16] JP 3-0, *Joint Operations*, 11 August 2011, GL-9.
[17] *The National Military Strategy of the United States of America,* Washington D.C.: Chairman Joint Chief of Staff*.*, 2015, i.
[18] The term "deterrence" throughout "Preventive Defense" refers to "traditional" concepts of deterrence, i.e. state on state, high end conventional or nuclear deterrence.
[19] Ashton Carter and William Perry, Preventive Defense: A New Security Strategy for America (Washington, DC: The Brookings Institute, 1999), 14.
[20] The term "deterrence" throughout "Preventive Defense" refers to "traditional" concepts of deterrence, i.e. state on state, high end conventional or nuclear deterrence.
[21] Ashton Carter and William Perry, Preventive Defense: A New Security Strategy for America (Washington, DC: The Brookings Institute, 1999), 18.
[22] Lt.Gen Charles T. Cleveland and Lt. Col Stuart L. Farus, "A Global Landpower Network Could Be the Ultimate Anti-Network," *Army*, August 2014, 55-56.
[23] The U.S. Army defines mass as: "Concentrate the effects of combat power at the decisive place and time." FM 1-02, *Operational Terms and Graphics*, September 2004, 1-121.
[24] Joint Publication 1-02, DOD Dictionary of Military and Associated Terms 08 November 2010, as amended through 15 November 2014, http://www.dtic.mil/doctrine/dod_dictionary/index.html.
[25] "SOF's Role in Comprehensive Deterrence." Lecture, Combined USSOCOM J5/USASOC G9 Deep Dive Draft Briefing Notes from Mr. Miller, USSOCOM J5 and Mr. Warburg, USASOC G9, MacDill, AFB, February 26, 2015.
[26] U.S. Army Special Operations Command, "Support to Political Warfare" White Paper (29 April 2015), 11.
[27] U.S. Special Operations Command, "The Gray Zone" White Paper (09 Sept 2015), 3.
[28] *The National Military Strategy of the United States of America,* Washington D.C.: Chairman Joint Chief of Staff*.*, 2015, i.
[29] Robert Martinage, "Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantage to Restore U.S. Global Power Projection Capability," (PowerPoint Presentation), Center for Strategic and Budgetary Assessments, 2014, 5.
[30] "Redefining the Win." United States Army Special Operations Command G9 White Paper, 06 January 2105.

Page for Reader Notes / Comments

UNITED STATES ARMY
SPECIAL OPERATIONS COMMAND

White Paper

Operationalizing Deep Knowledge

15 April 2016

"Mendel's concept of the laws of genetics was lost to the world for a generation because his publication did not reach the few who were capable of grasping and extending it; and this sort of catastrophe is undoubtedly being repeated all about us, as truly significant attainments become lost in the mass of the inconsequential."[1] *Vannevar Bush, 1945*

Overview

One of the key findings that emerged from the recent SILENT QUEST (SQ) 15-1 exercise venue, sponsored by the U.S. Army Special Operations Command, was the need to identify potential problems on the international stage before they became crises.[2] The premise underlying this research effort is that somehow, somewhere knowledge exists that could potentially indicate a burgeoning crisis or conflict situation. The question is, where is that knowledge and how does the U.S. military exploit this knowledge?

The basis for this concept is derived from senior leader guidance to consider "methods to sustain deep knowledge" and "what to consider in order to warehouse data and keep knowledge beyond the length of the assignment cycle/POM cycle." This focused effort has been a recurring theme since SILENT QUEST (SQ) 13-2 exercise two years prior. In order to address this recurring theme, one aim during the SQ 15-2 event is to use "deep knowledge" as part of the exercise framework, to guide decision-making. Key leaders will determine how this will be done based on outputs from working group discussions during SQ 15-2 Enabling Event #1 and Enabling Event #2.

The U.S. military needs to analyze two factors in order to begin testing this concept. First, what does "deep knowledge" mean, and more generally, what forms of knowledge does the U.S. military currently employ? Second, in what way could units store or access information that leads to deep knowledge? In a broader sense, where does knowledge currently reside? What mechanisms and methods could the force use to reframe the use of information and data as enterprise assets?

The following figure depicts a framework to guide deep knowledge discussions. It is a design feature to frame our knowledge environment. The goal of framing the environment is to uncover key areas where the U.S. military can take better advantage of its existing knowledge base. Additionally, we want to reveal advanced ways that information and data could inform decisions. Those revelations will lead to new approaches to harvesting deep knowledge, which will be tested as mission command solutions during SQ15-2.

Figure 1: Deep Knowledge Discussion Framework

"How do we have a conversation with the data?"[3] *SGM Houston, USASOC G9*

Purpose

This paper frames a discussion on how the U.S. military can use vast amounts of information to achieve decisive situational advantage. Moreover, this paper aims to elevate that discussion to consider options for using that information in more integrated ways. By doing so, the U.S. military will create a synthesized understanding of the operational environment by leveraging *deep knowledge*. **Deep knowledge can be defined as "a new perspective of the operational environment derived from acquiring, sifting, integrating, and interpreting diverse tacit and explicit data**."[4] International security trends of disorder, scarcity of resources, ecological challenges, toxic ideologies, game-changing technologies, emerging resistance movements and opportunistic competitors employing hybrid warfare capabilities are creating new challenges in the operational environment.[5] This demands new approaches to managing shared knowledge. The U.S. military must maintain a competitive advantage against adaptive threats by using deep knowledge to understand how the human domain overlaps with other physical and virtual domains. Doing so will enable the U.S. military to seize the cognitive initiative in a complex environment.

Rapidly evolving integrated technologies enable organizations to look deeply into areas of the world and see billions of disparate data as an aggregated picture. *The ability to see through those data and create meaning is the "deep knowledge" this paper seeks to explore*. How then does the U.S. military operationalize deep knowledge and understand the operational environment at an entirely new level? The information challenge the community faces is to move beyond our "know-what" and "know-how" and shift the paradigm of information management to become "professionals with know-why [that] can anticipate subtle interactions and unintended consequences" in our operating environments.[6] At the core of Mission Command lie the human experience and systems technologies, along with the organization's culture of learning to collect and analyze data relevant to operational decisions.[7] One of the primary tasks of mission command is to conduct knowledge management and information management; therefore, an opportunity exists to capitalize on the intersection of advanced computing capacity and myriad institutional information to achieve greater situational understanding than previously attainable.[8]

A mixed-methods approach was used to study how the DoD could interpret and envision using deep knowledge. Research on current business and government trends related to maximizing corporate knowledge occurred through surveys of various academic, businesses, organizational, and international publications. There are vast references to knowledge, knowledge management, data, big data, data analytics, global mapping, social networking, and other similarly related technology and social science disciplines. Additionally, the USASOC sponsored SILENT QUEST Wargaming venue fielded much of the grassroots conversation throughout the ARSOF enterprise as participants in associated enabling events debated and discussed interpretations and implications of deep knowledge. Incidentally, the topic of deep knowledge emerged from the SILENT QUEST enabling events as one of the key topics for senior leader to discuss during SILENT QUEST 15-2. Separately, the research team convened key stakeholders, including functional staff and subordinate organizations through one-on-one interviews and collaboration meetings to share perspectives of similar ongoing initiatives throughout the enterprise. The

research team was also able to leverage the reach-back capability of contracted concept development teams to collaborate with colleagues engaged in similar knowledge utilization initiatives in commercial business sectors. This broad study approach revealed that the time is right to advance the concept of deep knowledge beyond conversation to operationalization.

Deep Knowledge

Operating based on a profound, evolving understanding of the operating environment is at the core of Mission Command and Operational Art. The Army recognizes two forms of knowledge: tacit and explicit.[9] Essentially knowledge consists of what one knows and what an organization records. These are "gained through study, experience, practice, and human interaction and [are] the basis for expertise and skilled judgment."[10] Although these two forms of knowledge represent a foundation for what one might know, this paper raises the question: Is there another aspect of associating disparate information to include the digitized data to reveal new knowledge?

Deep knowledge needs to encompass a broad range of considerations relative to an area of operation, with granularity focused to operational echelons. It could account for stores of information within existing repositories internal to the organization. It could also account for information from data sources external to the organization. Examples of these domain topics include:

- Cultures
- Religions
- Ideologies
- Histories
- Infrastructure
- Economics
- Militaries and defenses
- Language
- Environment
- Geography
- Expertise
- Education

Along with these considerations, deep knowledge should be functionally unique by linking and dynamically relating numerous sources and diverse categories of information about an operating environment. This is an expansion of intelligence analysis to combine intelligence disciplines with operations experience. Employing “big data” capacities and methodologies, deep knowledge could thus extract interpretation from data. Mission Command could therefore assess the direction and implications of trends and events, perceived in near real time. In effect, operations planners could map the human domain with the geographic fractals of data.[11] At a minimum, this could include:

- Networked relationships
- Personal experiences
- Human transactions
- Ongoing or emerging trends
- Nuanced anomalies
- Virtual conversation trends
- Georeferenced metadata
- Multimodal societal sentiment analysis[12]
- Opinion mining (polarity classification and detection)[13]
- “Culturomics”[14]

Problem Statement

As the U.S. military confronts an increasingly complex operational environment, rapidly evolving computing technologies will advance information control in a globally connected world. How then do commanders and staff leverage massive amounts of data and information to make better, more rapid decisions? Moreover, how does the U.S. military use an information capability to derive deep knowledge of operational environments to gain a decisive advantage in situational awareness? Through better implementation of technology systems, streamlined information processes, and mission command emphasis, in essence, "How do we have a conversation with the data?"[15]

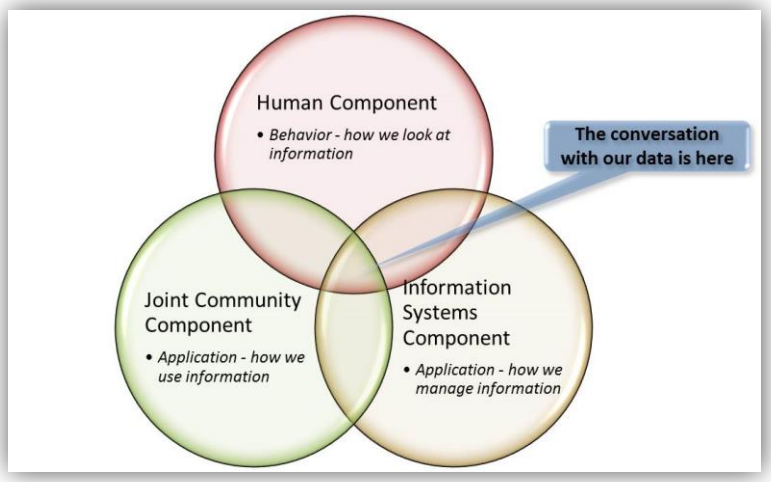


Figure 2: Conversation With the Data

The U.S. military has an opportunity to seize the initiative using knowledge as a weapon system by:

- collecting and retaining tacit forms of knowledge to include social and professional connections, operational experiences, civilian education, personal skills and abilities
- piecing together existing sources of tacit and explicit information
- integrating information from external sources
- leveraging advanced data systems to analyze content and synthesize data

Central Idea

Since one of DoD's roles is to maintain persistent presence throughout the world, day-to-day observations coupled with historic data should reveal nuances that otherwise would go unnoticed. The Joint Force is uniquely postured to take those inputs in aggregate and synthesize them into actionable knowledge. This factor is particularly true of future maneuver within the human domain. Collective interactions in the human domain should reveal potential security conditions when analyzed with aggregating data tools by both intelligence and operations experts. The hypothesis behind deep knowledge suggests that fusing multidisciplinary information practices ought to reveal situational insights that otherwise would go unnoticed. Much like the Ishihara Color test reveals hidden numbers embedded within a colored plate, new revelations in the human domain could be gleaned from digitized data that is pieced together by multidisciplinary efforts (Fig. 3). [16]

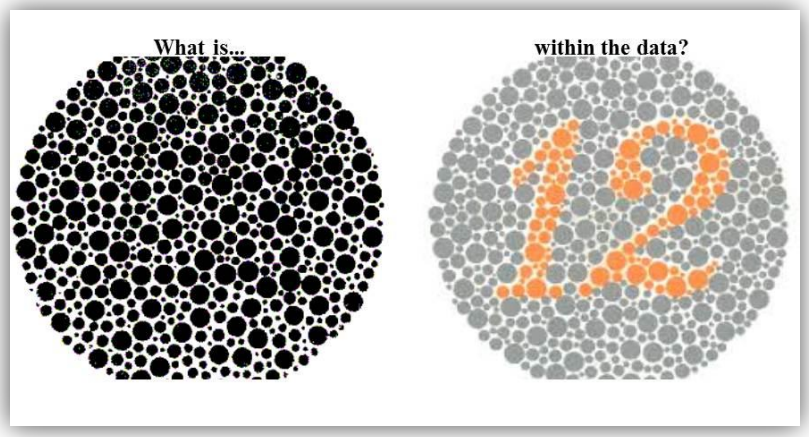


Figure 3: Information in Data

Components of a Solution

Managing People

As the U.S. military seeks comprehensive solutions to operationalizing knowledge, three key areas of emphasis will drive the thinking about leveraging information. The first area considers the operator. This is the human element. This human element consists of the management of information our operators knows explicitly and intuitively. The DoD personnel enterprise is both highly talented and highly aware of nuances within operational environments. Therefore, in order to extract the most from what operators know, an approach to gaining deep knowledge needs to account for managing the talent with the ranks and the personal knowledge developed through experiences, social connections, professional contacts, and individual competencies.

Data Repositories - Managing Information

Currently information exists throughout the force in a wide variety of information management systems (SharePoint), databases, shared drives, file documents, reports, etc. Some of that information is readily accessible to those within the enterprise network. However, access restrictions, systems constraints, and data storage practices limit collaboration of information thereby reducing the utility of it as useful knowledge. Therefore, through what repository methodology could operators exploit tacit and explicit knowledge buried within the data?

Solutions to data exploitation could consider new ways of storing and accessing information as well as new ways to associate bits of data. One way to think about solutions to a repository idea would be to compare card catalog libraries to digital encyclopedias, such as Wikipedia. In the former example, one would need to consult a physical cataloging index or librarian for directions to a particular book or subject of books. They would then need to manually sift through those books in hopes of finding relevant information - an inefficient and time-consuming process. The latter example virtually connects the information dots by providing summarized, user-defined information. Moreover, it digitally links to source references. The latter example could be taken

further through an automated mechanism that sifts through the referenced data and extracts associated information.

One critical observation is that a culture exists throughout the force that, unfortunately, is not fully maximizing an opportunity to put both tacit and explicit information into a collaborative data environment. The strongest case example of this behavior is the general tendency to forego the use of the enterprise collaboration tool, SharePoint, for more rudimentary and inefficient repository solutions, namely shared drives. This paper will not attempt to explain why there is a significant reluctance to use SharePoint; however, the SharePoint example illustrates an inherent behavior representative of the emphasis placed on how information is used to generate knowledge.

Information that is difficult to reach is difficult to use. Current business technology trends are seizing upon information management and data technology solutions to design agile learning organizations that maximize both tacit and explicit knowledge.[17] It is for this reason that this white paper suggests that deep knowledge is a form of a weapons system when Mission Command emphasizes its use to frame the operational environment.

Tools to Manage Knowledge

Finally, how does the U.S. military leverage analytical tools to piece together these key areas to develop deep knowledge? Many tools currently exist and could be models for off-the-shelf information systems to employ as a sort of dashboard that could be used within an operationalized CONUS base. One example, merely for illustration, is the GDELT Project platform that provides real-time monitoring of open-source information sources.[18] Through open access Application Program Interface (APIs), the service culls billions of available database information sets to visualize and explore data.[19]

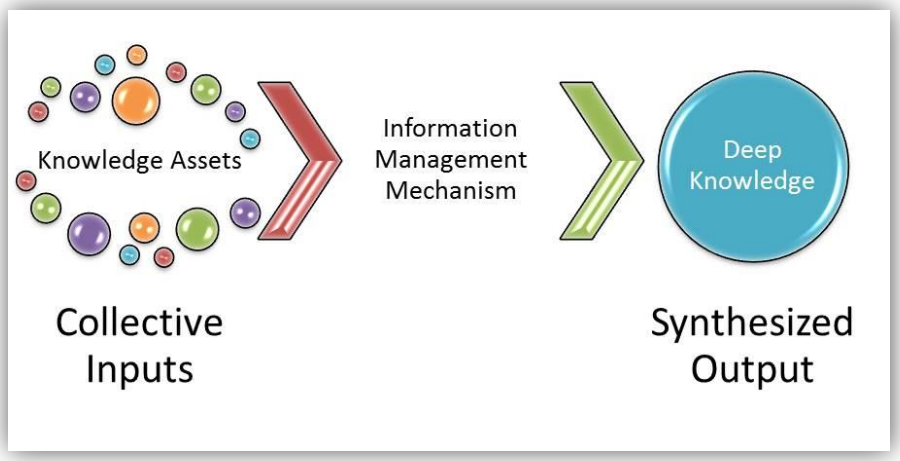


Figure 4: Inputs to Outputs

Other similar commercial services include IBM's Watson platform and Dataminr's real-time information engine.[20] Similarly intelligence and mission command systems such as Palantir, Distributed Common Ground System-Army (DCGS-A), and Command Post of the Future (CPOF) attempt to present visualizations of multi-variant information. Other information systems also exist to store lessons learned, operational observations, area studies, and even unit specific training and operations events. These can be found on both classified and unclassified networks. The problem with these few examples is that the data are often either difficult to transfer, or cannot be transferred between systems. Moreover,

the value of the data is a function of input and access. Information has to be added in a useful way, and the information must be accessible. If the information is not accessible because it is hard to find, or security classifications limit authorized access, or it exists in incompatible forms, then the information cannot be turned into knowledge.

Capabilities

What capabilities does the force need to operationalize deep knowledge? The following aspects should be considered as the U.S. military finds solutions to maximize available data.

- Searchable across classification systems
- Able to assess multi-source inputs for trends, tipping points, thresholds, anomalies with organization information and with non-standard indicators (e.g. independent metadata)
- Possibly new expertise to facilitate exploitation of data mined knowledge
- Able to tailor parameters for necessary levels of analysis from MACOM to operator
- Ability to associate multiple sources of information
- Develop predictive models of human behavior
- Negotiate access restrictions through institutional firewalls and systems
- Illuminate real and fabricated narratives from multi-source media analysis
- Intuitive interface that encourages participation
- Secured at relevant levels based on classification limitations
- Real-time and historic data analysis
- Battlefield networking to share information
- Tactical biometric matching

Context for Deep Knowledge

The Army initiated a series of challenges to orient the force's thinking about how future capabilities should address current problems. The first warfighting challenge looks at "[how] to develop and sustain a high degree of situational understanding while operating in complex environments against determined, adaptive enemy organizations."[21] The lead for this challenge has been the Intelligence Center of Excellence. Incidentally, the Intelligence community has specifically taken on certain aspects of broadening situational understanding. The effort that intelligence functions are doing to build better and more responsive threat understanding correspond with an underlying difficulty in operationalizing deep knowledge. Based on recent surveys of the force and iterative concept testing through SILENT QUEST 15-2 enabling events, we are coming to understand more fully the artificial and virtual walls that separate functions (such as operations and intelligence) and organizations from capitalizing on existing access to information.[22] A key takeaway from the SILENT QUEST events was that the force already has many mechanisms to generate knowledge, but the ability to consolidate the effect of those mechanisms collectively unfortunately keeps institutional knowledge disaggregated.

Aside from the Army's warfighting challenge, one consistent theme emerges from the variety of national strategy guidance; that is the demand for decisive situational awareness. Grasping the

complexities and nuances of the future operating environment requires collective efforts of intelligence disciplines and operations expertise. The lash up of those efforts, if managed in a synthesized manner, could more clearly portray the environment to scalable degrees of granularity from multiple narrative vantage points.

The 2015 National Security Strategy recognizes an interconnected global system of participants. Consequently, struggles for power are anticipated both among states and beyond state structures.[23] Deep knowledge could illuminate those tension points when they appear and as they increase in intensity. Doing so would inform policy considerations to shape the trajectory of power outcomes. *Moreover, the ability to identify particular indicators and warnings of security conditions early in an operational timeline would enable decision making that gets ahead of potential instability trajectories*.

Most recently, state-on-state challenges resurface in priority based on their risk potential. The 2015 National Military Strategy (NMS) identifies a global security context that requires a "competitive advantage…[in] early warning and precision strike."[24] Moreover the NMS notes the global nature of information and information technologies which both enable and empower people. The power of information and the power of access to information is changing the velocity of decision-making. Competition for control of resources and the social narratives that lead to political and economic stability are based in part on a competitive advantage to information.

Together these strategic policy frameworks point to a need for comprehensive approaches to establish international deterrence credibility. In part, the relative advantage of credibility favors the actor able to weigh the cost of benefits against associated and even unintended risks. Those measurable variables must be ascertained through deliberate and inadvertent capture means. In other words, data that reveal information about an operational environment provide the knowledge needed to guide mission command. This paper suggests that the Joint Force can achieve a level of situational awareness that is decisively more valuable to decision makers because of the fundamental understanding of the human domain.

Knowledge Sharing Example from Crisis Mappers

One way to illustrate how tacit forms of knowledge, such as social connections, could provide deep knowledge is to look at how humanitarian practitioners leverage international networks to anticipate and respond to crises. An example of socially connected knowledge is seen through the work of international "crisis mappers."[25] Crisis mapping utilizes crowdsourcing concepts to leverage networked individuals participating in crisis response efforts through web-based and mobile applications. These interconnected digital ecosystems are able to move massive quantities of data about impending crises and virtually *ex nihilo* form rapid responses to those crises.[26]

Although technology tools are maximized to make the process of information sharing efficient, technology only serves as a secondary element that supports a cultural behavior of information sharing. One crisis mapping researching noted that, "grassroots organizations foster practical approaches that focus on relationship building, information analysis and *fusion*, rather than software development."[27] One critical lesson that the Joint Force can learn from the way crisis mappers have redefined international humanitarian responses is to embrace an inherent motivation to share information rather than store it.

Solution Options

Deep knowledge solutions should be comprehensive, addressing multiple factors simultaneously. No one-solution approach will solve any problems with the way the force uses its information. Incidentally, an approach will likely need to synthesize the relationships among human components, information systems components, and the broader joint community. The intersection of a data oriented mindset within the community, the expertise to manage and manipulate those data, and the data themselves is where DoD operationalizes deep knowledge (Fig. 2).[28]

What follows (Fig. 5) is a menu of options along the aforementioned lines of effort. These options are scalable within each dimension, so, collectively, they can be scoped to achieve required advantages. The way to engage with the data is to apply elements from each component to comprehensively leverage information and use knowledge as a weapon system.

Human Dimension	Develop organizational architecture of SME managers - "help desk" model or fusion cell centers of operational knowledge managers and technical knowledge managers
	Adopt new behaviors of information managment that integrates practitioners with technologists
	Combine Intelligence and Operations information functions through integrated organizational processes
Information Systems	Adopt new advanced information aggregating systems capable of extracting information across multiple platforms and domains
	Adapt current ARSOF information systems to use more collaborative and integrated protocols
	Broaden Intelligence data collaboration initiatives to fuse with operations information and personal information
Joint Force Community	Adopt new training and education practices that teach leveraging information
	Prioritize information management practices to instill a culture of knowledge specialists
	Design and enforce new business rules to capture, exploit, and use tacit and explicit forms of operational knowledge

Figure 5: Options to Comprehensive Solution

Implications

The implication of achieving deep knowledge at the individual operator and institutional level is clear: the U.S. military could derive a much more profound and proactive understanding of likely operational regions, along with a more attuned grasp of potential or emergent triggers to crises in these regions. Units would thus be able to focus on critical interpretive indicators in likely areas of operation, enabling much more rapid and responsive mission planning.

Through analysis of associated knowledge, the U.S. military could potentially get ahead of the crisis curve. The force could also determine the degree to which figurative "gray zones" are transitioning from stages of peace to war. Layered depths of knowledge management could reveal broader understanding across traditional information seams.

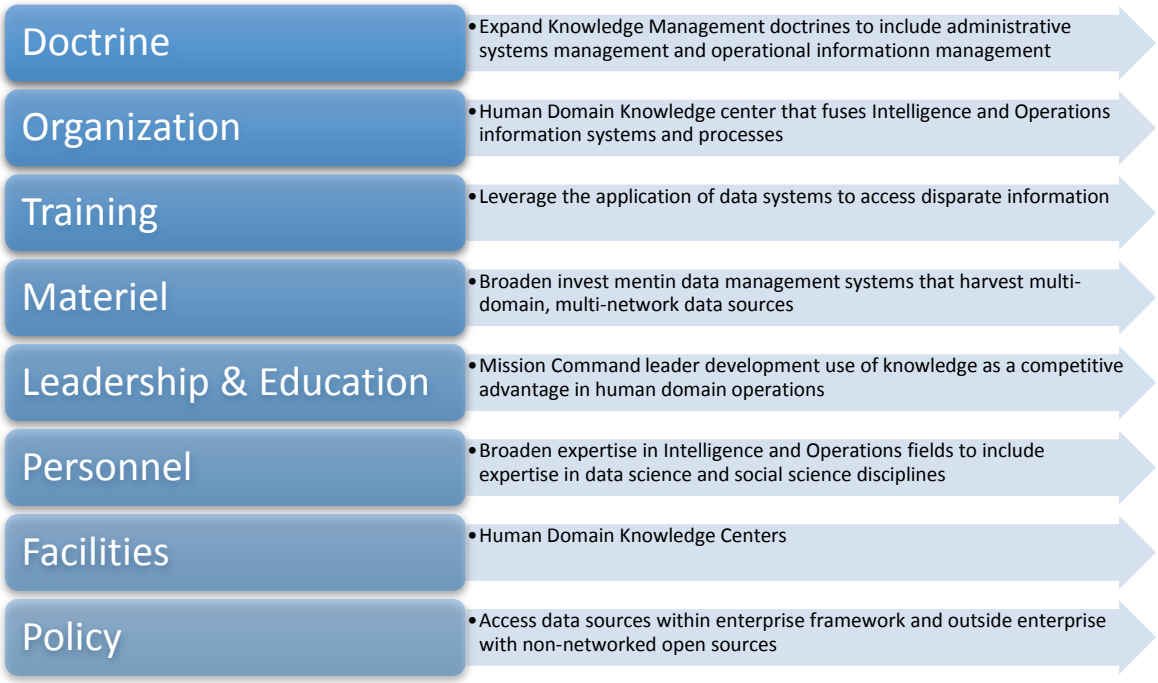
Conclusion

"[Man] has built a civilization so complex that he needs to mechanize his record more fully if he is to push his experiment to its logical conclusion and not merely become bogged down part way there by overtaxing his limited memory."[29] *Vannevar Bush, 1945*

Can the U.S. military arrive at new meaning from existing knowledge and synthesized data? By exploiting repositories of information, and collecting operationally relevant data with method-driven technology solutions, Joint forces can overcome the limitations of individual and institutional memory. To do that, we must better integrate personal and organizational knowledge with useful management, storage, and access to such information. However, if operators continue to rely on its current panoply of independent information systems and methods of managing information, then the organization runs the risk of falling behind other government agencies, joint partners, and potentially competitors in the arena of information dominance. This risk is further exacerbated by the rapid rate with which data technologies are advancing across the global information market, making the ability to acquire new knowledge both easy and relatively inexpensive – an advantage to adversaries and allies alike.

Appendix: DOTMLPF-P Considerations to Manage Adaption of Deep Knowledge

A DOTMLPF-P framework is one way to consider instituting long-term organizational change. The following considerations only illustrate themes of thought derived through collaboration with various ARSOF enterprise functions and organizations. These illustrations are intended to generate further discussion as to the use of Deep Knowledge during SILENT QUEST 15-2.



Notes

[1] In his seminal work, *As We May Think*, Vannevar Bush made a prescient argument for the exploitation of scientific advances to contain, record, and reuse man's vast base of knowledge.
[2] SILENT QUEST 15-1 Final Report (Draft)
[3] During the SILENT QUEST 15-2 Enabling Event #1, one of the most informative analyses that came out of small group collaboration sessions was a remark by USASOC G9 Sergeant Major, SGM Houston. He asked this prescient question, which elevates the deep knowledge discussion from one of just managing repositories to one of connecting the human dimension with information technology.
[4] This definition of deep knowledge is derived from iterative SILENT QUEST working group sessions. It is also derived from one-on-one interviews with various functional and subordinate USASOC elements.
[5] See USASOC White Paper "Redefining the Win"
[6] Quinn *et. al*. describe how organizations can maximize the inherent knowledge in people by managing professional intellect.
[7] Ibid.
[8] ADRP 6-0 Mission Command, p. 1-4. Knowledge is a central theme of Mission Command as information is analyzed and turned into knowledge through command discernment.
[9] ATP 6-01.1, p. 1-3.
[10] Ibid.
[11] For more human domain mapping see Raymond, Derek. *Human Domain Mapping in 21st Century Warfare*.
[12] For an overview of sentiment analysis and opinion mining see: Cambria, Erik, Bjorn Schuller, Yunqing Xia, and Catherine Havasi. "Knowledge-Based Approaches to Concept-Level Sentiment Analysis." *Intelligent Systems, IEEE* 28, no. 2 (March/April 2013): 15-21.
[13] Ibid.
[14] "Culturomics" is an emerging discipline that looks at "the application of high-throughput data collection and analysis to the study of human culture." For more see: Michel, Jean-Baptiste et. al. "Quantitative Analysis of Culture Using Millions of Digitized Books." *Science* 331, no. 6014 (January 2011): 176-182. See also Leetaru at http://firstmonday.org/ojs/index.php/fm/article/view/3663/3040.
[15] SGM Houston, SILENT QUEST 15-2 Enabling Event #1.
[16] These images are from the Ishihara Color test, Test Plate 12, used to test for colorblindness. The black and white plate represents a collection of data points that when filtered in color reveals the number 12.
[17] In a 1988 Harvard Business Review essay, Peter Drucker observed that "to remain competitive – maybe even to survive – businesses will have to convert themselves into organizations of knowledge specialists."
[18] For more on the GDELT Project see http://gdeltproject.org/ . Note that GDELT is one example of many platforms currently exploring the aggregation and analysis of "big data" information.
[19] Kalev Leetaru, the founder of the GDELT Project discusses "realtime [sic] programmatic access" to massive amounts data made possible through APIs. See more at: Leetaru, Kalev H., Shaowen Wang, Guofeng Cao, Anand Padmanabhan, and Eric Shook. "Mapping the global Twitter heartbeat: The geography of Twitter." *First Monday* . May 6, 2013. http://journals.uic.edu/ojs/index.php/fm/article/view/4366/3654 (accessed May 20, 2015)
[20] There are many commercial projects led by numerous technology companies that are trying to use complicated algorithms and API interfaces to extrapolate correlations that can be visualized. See: https://www.dataminr.com/technology/ ; http://www.ibm.com/smarterplanet/us/en/ibmwatson/explorer.html.
[21] For more on the Army's Warfighting Challenges, see http://www.arcic.army.mil/Initiatives/army-warfighting-challenges.aspx.
[22] During SILENT QUEST Enabling Events 1 and 2, participants discussed the difficulty their organizations have had sharing information with other ARSOF organizations as well as organizations external to ARSOF. These challenges are technical (e.g. classifications, system firewalls, permissions), cultural (e.g. perceived expertise difference between operators and analysts), administrative (including agency policies, formal and informal business rules), and technological (e.g. limits on data aggregating software, limits on access to open data sources, user understanding of technology capabilities).
[23] See 2015 National Security Strategy, pp. 3-5.
[24] See 2015 National Military Strategy, p. 1.
[25] One of the largest networks of humanitarian workers exists through crisismappers.net, which hosts a community of humanitarian practitioners and others interested in collaborating through open sourced crowdsources applications.
[26] For more on how government can learn from grassroots crisis responses see Crowley, pp. 21-23.

[27] Crowley, p. 28. *Emphasis added*. Crowley notes that "Large system integrators have perpetuated this confusion [preeminence of technologies]: it is far easier to sell a silver-bullet technology to the government than to build the combination of community, technology, and best practices…" p. 31.
[28] Mayer-Schonberger and Cukier discuss how the online corporation, Amazon, broke from institutional norms by approaching its business model as "the mindset, the expertise, and the data." See *Big Data* p. 132.
[29] Bush, p. 46.

References

Army Doctrine Reference Publication 6-0, C2 Mission Command. Washington, D.C.: Headquarters, Department of the Army, March 28, 2014.

Army Training Publication 6-01.1 Techniques for Effective Knowledge Management. Headquarters, Department of the Army, March 2015.

Bush, Vannevar. "As We May Think (Reprinted from The Atlantic Monthly, July 1945)." *Interactions*, 1996: 35-46.

Cambria, Erik, Bjorn Schuller, Yunqing Xia, and Catherine Havasi. "Knowledge-Based Approaches to Concept-Level Sentiment Analysis." *Intelligent Systems, IEEE* 28, no. 2 (March/April 2013): 15-21.

Chaudhry, Abdus Sattar. "Leveraging Personal Networks to Support Knowledge Management in a Public Sector Organisation in Kuwait." *Libri: International Journal Of Libraries & Information Services* 64, no. 4 (2014): 341-349.

Crowley, John. *Connecting Grassroots and Government for Disaster Response.* Washington, D.C.: Woodrow Wilson International Center for Scholars, 2013.

Hansen, Morten T., Nitin Nohria, and Thomas J. Tierney. "What's Your Strategy for Managing Knowledge?" *Harvard Business Review.* March-April 1999. https://hbr.org/1999/03/whats-your-strategy-for-managing-knowledge (accessed May 15, 2015).

Ihrig, Martin, and Ian MacMillan. "Managing Your Mission-Critical Knowledge." *Harvard Business Review.* January-February Issue 2015. https://hbr.org/2015/01/managing-your-mission-critical-knowledge (accessed May 28, 2015).

Joint Chiefs of Staff. "The National Military Strategy of the United States of America 2015." June 2015.

Leetaru, Kalev. "Culturomics 2.0: Forecasting Large-Scale Human Behavior Using Global News Media Tone in Time and Space." *First Monday, Volume 16, Number 9.* September 5, 2011. http://firstmonday.org/ojs/index.php/fm/article/view/3663/3040 (accessed May 22, 2015).

Leetaru, Kalev H., Shaowen Wang, Guofeng Cao, Anand Padmanabhan, and Eric Shook. "Mapping the global Twitter heartbeat: The geography of Twitter." *First Monday* . May 6, 2013. http://journals.uic.edu/ojs/index.php/fm/article/view/4366/3654 (accessed May 20, 2015).

Mayer-Schonberger, Viktor, and Kenneth Cukier. *Big Data.* New York: Houghton Mifflin Harcourt Publishing, 2013.

Michel, Jean-Baptiste et. al. "Quantitative Analysis of Culture Using Millions of Digitized Books." *Science* 331, no. 6014 (January 2011): 176-182.

Quinn, James Brian, Philip Anderson, and Sydney Finkelstein. "Making the Most of the Best." *Harvard Business Review.* March-April Issue 1996. https://hbr.org/1996/03/making-the-most-of-the-best (accessed June 18, 2015).

Raymond, Derek. "Human Domain Mapping in 21st Century Warfare." *Small Wars Journal.* August 22, 2015. http://smallwarsjournal.com/jrnl/art/human-domain-mapping-in-21st-century-warfare (accessed August 27, 2015).

UNITED STATES ARMY

SPECIAL OPERATIONS COMMAND

White Paper

"Redefining the Win"

06 Jan 2015

Redefining the Win

The Redefined Win Concept

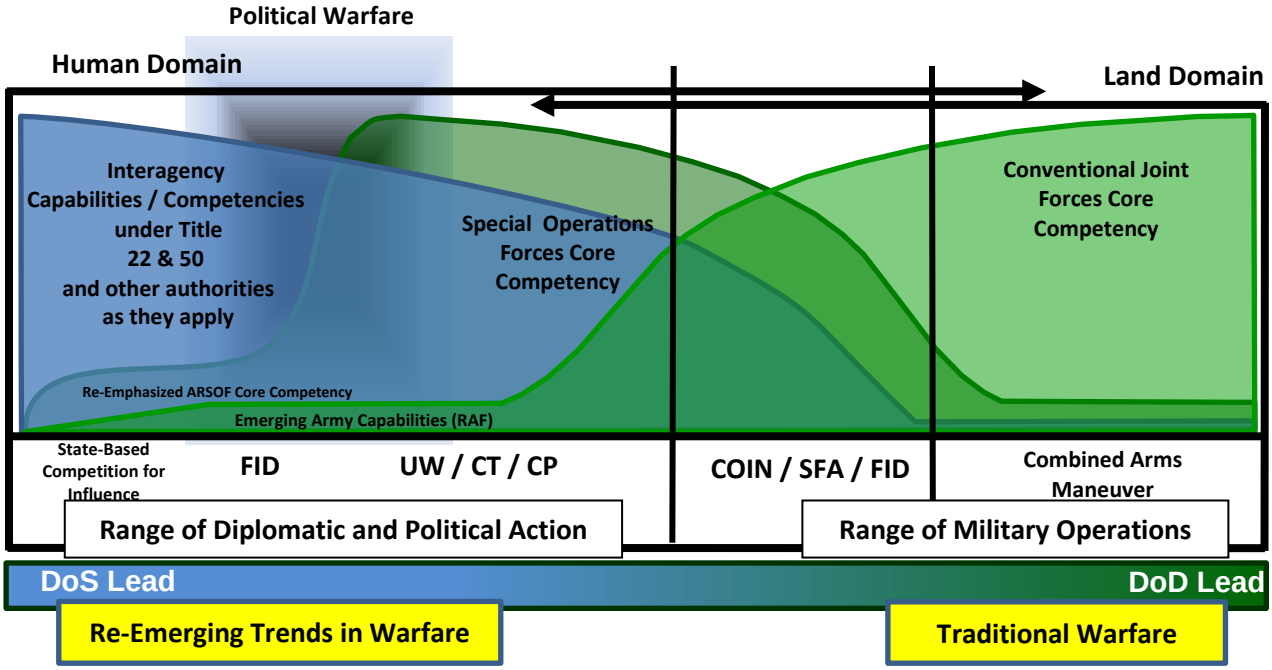
The Redefined Win Concept centers on proactive U.S. competition with State / Non-State Actors for the relative superiority over the physical, cognitive and moral security of key populations in the areas we choose to campaign. This paper sets forth the SOF contribution to the larger Redefined Win. It acknowledges but does not discuss the vital contributions of the JIIM community.

The Win is framed as follows: (1) Decision space has been preserved for our National leaders. Of note, decision space is characterized as providing decision makers with scalable, cost imposing options to hold, either unilaterally or with our partners, potential adversary interests at risk. (2) Conditions are set for an acceptable political outcome in the areas that matter to the United States. (3) Positional advantage is retained in terms of time, forces and relationships to advance U.S. interests.

Trends in International Competition

The United States is facing a strategic inflection point characterized by an "uncertain strategic security environment paradoxically framed by diminishing defense resources and an increasing number and variety of potential threats."[1] Social, political, informational and economic trends in international competition are converging between state and non-state actors and others for the relative superiority over the physical, cognitive, and moral security, and adequate governance of populations. This competition generally centers on the left side of the operational continuum where the Department of State is the lead department as noted in the slide below.

Trends in International Competition



[1] LTG Charles T. Cleveland and LTC Stuart L. Farris, "Toward Strategic Landpower," *Army Magazine*, July 2013, p. 22.

Framing the Environment

The operational environment is characterized by disorder, scarcity of resources, ecological challenges, toxic ideologies, game-changing technologies, emerging resistance movements and opportunistic competitors employing hybrid warfare capabilities. As the foreseeable future's "new-normal," this setting will challenge the effectiveness of traditional forms of power while enabling non-traditional forms. We need to effectively engage in this environment.

The requirement to protect and advance U.S. interests will demand new ways of thinking, with unique approaches that broaden strategic options for our National Leaders. Essential to any new approach will be a comprehensive definition of what strategic success, or "the Win," looks-like in an increasingly disordered world punctuated by competitors capitalizing on hybrid warfare capabilities.

Hybrid Warfare to Challenge the United States

Select Nation-State and Non-State competitors are developing hybrid warfare capabilities to compete in the Human Domain and dominate the left-side of the operational continuum. Russian and Chinese military doctrines recognize the growing necessity of synchronized political, diplomatic, economic, military-kinetic, cyber and mass-media operations to advance their respective interests.

We need not imagine the character of the competition on the left-side of the operational continuum. We must only observe Russia's actions in Georgia, Crimea, and eastern Ukrainian provinces and its use of a multi-echeloned approach consisting of coercive diplomacy, cyber capabilities, propaganda, unconventional warfare and surrogates has challenged U.S. and NATO efforts to craft a comprehensive strategic response.

The actions of the "Islamic State of Iraq and the Levant" demonstrate that non-state entities can also engage in hybrid warfare, and they have been particularly successful in the use of mass-media operations to shape perceptions of the conflict. These examples illustrate once again that we do not get to choose the domains we compete and fight in - they choose us.

Redefining Win - Winning Early on the Left Side of the Operational Continuum

The totality of the security challenges facing the Nation and the evolving character of these threats require an operational framework to "Win Early" to prevent these challenges from scaling beyond our level of strategic depth and capacity to respond.

The Special Warfare operational framework to "Win Early" is presented in a separate USASOC White Paper. A brief summary is presented below to add context to the Redefined Win Concept.

> Theater Special Operations Commands, enabled by the Global SOF Network and the Global Landpower Network, conduct Special Warfare Campaigns to solve security challenges outright, or rescale these challenges to manageable levels. If a security challenge cannot be rescaled, the option for conventional major combat operations always exists. The Special Warfare Operational Approach assumes an earlier "Strategic Start Point" and envisions three operational lines effort to

meet current and emerging National Security challenges. These are: (1) Expanded SOF Support to Joint Forcible Entry, (2) Unconventional Warfare, and (3) SOF Support to Political Warfare.

An earlier "Strategic Start Point" requires new thinking about the traditional, military Phase 0 and most importantly for this effort, new thinking about "Left of Phase 0" campaigns and operations to consider how we assess, sort, form and rescale security challenges to win early and preserve strategic depth and decision space for our National Leaders. The framework for this approach centers on a persistent SOF forward presence in and around the people with deep knowledge of the environment to generate decisive situational awareness to better inform the strategic start point for campaigns where the "Win" occurs at a much lower level of National effort. An example of this approach is the U.S. effort to aid the El Salvadorian Government from 1980-1992, that cost approximately $6.0 billion, and consisted of 55 U.S. in-country advisors enabled by an out-of country support element that assisted the government in the defeat of the communist backed FMLN insurgents.

The Redefined Win Concept acknowledges the trends in international competition and the necessity to proactively compete with State / Non-State Actors and others for the relative superiority of the physical, cognitive and moral security of key populations. The Win is defined as:

- ***Strategic Power Retained*** **-** Current and emerging security challenges will present many opportunities to commit significant resources, including service member lives, fiscal strength, good will and partner trust. These resources along with the diplomatic, information, military and economic elements of power constitute a finite capacity. Similarly, the support and will of the American people must be considered as well. The U.S. must consider its strategic power **when imposing a cost to hold, either unilaterally or with our partners, potential adversary interests at risk.**

- ***Influence Expanded*** **-** In a hyper-connected, social-media enabled cognitive world, the positive perceptions, beliefs, trust and credibility that others (Nation-States, Non-State Actors, Sub-Groups, and yet known entities) hold of the United States will be the center of gravity in relation to our ability to conduct successful campaigns, operations and activities to advance U.S. interests.

- ***Governance Increased*** **-** In an under-governed, resource-constrained and fragile world, governance will be relative, particularly in conflict and at risk zones. Our ability along with our partners (Nation-States / Non-State Actors and others) to increase the moral security of key populations through adequate governance supported by development programs and enabling efforts like the Institute for the Military Support to Governance (IMSG) will be a decisive point in how populations in the operational area view and support U.S. actions.

Winning in a Disordered World

In summary, the totality of the security challenges facing the Nation and the evolving character of hybrid threats demand earlier action to prevent these challenges from scaling beyond our level of strategic depth and capacity to respond. ***Winning in a disordered world requires a proactive stance to successfully compete with State, Non-State Actors and others for the relative superiority over the physical, cognitive and moral security of key populations in the areas we choose to campaign.***

UNITED STATES ARMY

SPECIAL OPERATIONS COMMAND

White Paper

Perceiving Gray Zone Indications

15 March 2016

> We are confronted with ambiguity on the nature of the conflict, the parties involved, and the validity of the legal and political claims at stake.
>
> —GEN Joseph L. Votel, Commander USSOCOM, *Remarks before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*, 18 March 2015

Executive Summary

This paper explores the hypothesis that accurately seeing, assessing, and understanding the challenges and risks within the current and the future strategic operating environment will require new thinking about indications of strategic challenges, threats, and opportunities for a complex world. This paper recognizes the need to consider new indications across the entire operational continuum. However, the paper confines its exploration to strategic indications for the Gray Zone. Critical to this effort will be to develop a comprehensive understanding of the Human Domain with emphasis on the physical, cognitive and moral frames within the environment, and what they represent to successfully compete and win in the space between peace and war.

Framing the Central Idea

> The requirements placed on ARSOF will not remain static. Technological, social, and human development, and the focused efforts of our adversaries, will ensure that change will remain constant. Our track record suggests the our attempts to predict this change will fall short; regardless, we must get the arc of change about right and then be flexible enough to adjust when appropriate.
>
> —LTG Kenneth E. Tovo, Commanding General, United States Army Special Operation Command, *USASOC Mission, Vision, and Priorities*, 10 December 2015

Central Idea

Current strategic indications predominantly focus on state adversaries capable of employing large-scale conventional forces and/or nuclear weapons, with conflict envisioned as occurring on the right side of the operational continuum. We must continue to see, assess, and understand risk for state and non-state capabilities on the right side of the operational continuum. However, we must also develop the ability to see, assess, and understand risk for state and non-state capabilities in the Gray Zone. The competition unfolding in the Gray Zone requires that we develop indicators and warning to assess, sort, form responses, and rescale security challenges much earlier in their development and risk profiles.

Key Themes

1) Thinking about strategic indications, which has its roots in Cold War ballistic missile defense, largely focuses on high-end conflict conducted by Nation States on the right side of the operational continuum.
2) Investment in thinking for strategic indications in the Gray Zone is warranted to meet the growing challenges we face in this space.
3) Strategic indications for a complex world will require a shift from primarily observing and calculating physical capabilities to also include seeing, assessing, and understanding the physical, cognitive, and moral frames within the strategic operating environment. Most notably, this shift to a broader, more inclusive framework will require greater understanding of how we think about and visualize cognitive maneuver.
4) The growing trans-regional implications of competition and conflict will require exploration of the trans-regional indications for state and non-state actors.
5) Strategic indications for the Gray Zone will require a multi-disciplinary approach to better inform risk, readiness and decision-making.
6) The totality and the varied nature of the security challenges across the operational continuum require consideration of the potentially systemic risk we face in a complex world.

The initial exploration of Perceiving Gray Zone Indications focused on the context of Russian activities in the Ukraine and Crimea. It yielded seven leading indications of state-based aggression falling under the threshold of UN Article 2 use of force.[1] We want to note up front that the leading indications are context specific based on an assessment of case studies in the Eastern European theater. Other theaters of operation may notice these similar Gray Zone characteristics; however, there may also be other context specific indications related to the unique nature of regional actors and conditions. The following leading indications are guide to understanding how states aggressively pursue interests through ambiguous means as viewed through the lens of a human domain model.

1. **Unconventional Measures**: tactics short of conventional war to coerce, destabilize, or overthrow a government.
    a. Use of persistent, low-level actions across the physical, cognitive and moral frames to desensitize observers of future action.
    b. Use of clandestine and covert intelligence and special operations elements to conduct Preparation of the Environment and other activities
    c. Increased activity within the human domain to "hide" campaign "in plain sight."
2. **Non-Military Measures**: political, economic, and diplomatic means to create positional advantage in regards to time, forces, relationships, ideas and geography.
    a. Development of political/economic ties to nations, key officials and/or the private sector within the area of interest.

    b. Employment of targeted political/economic ties toward campaign objectives.
3. **Leverage Population-based Power**: influencing and mobilizing groups to action.
    a. Use of aggrieved/exploitable population segments to potentially "host" follow-on forces.
    b. Increased activity of the targeted population directed toward campaign objectives
4. **Information Measures**: messaging and propaganda for deception and denial to set conditions for follow-on action.
    a. Use of macro/micro narratives to provide pretext for future action
    b. Increase in public opinion and propaganda efforts to foster ambiguity and misdirection toward the nature, scope and duration of unfolding campaign
5. **Lawfare Measures**: self-identified legal frameworks and processes to advance interests and coerce or compel others.
    a. Declaration of intent based on legal premise to take action.
    b. Expansion of territory based on caveat, national law or precedent.
6. **Technology Measures**: the use of existing and new technologies in standard and non-standard ways including the use of: Cyber, Unmanned Aerial Systems, basic and advanced weapons, such as precision munitions, robotics, and CBRN.
    a. The use of cyber domain to conduct recruitment, finance operations, operational planning and propaganda.
    b. The use of cyber-domain attacks against civil, military, and governmental targets.
7. **Conventional Military Measures**: the employment of conventional forces to support strategic objectives by employing capabilities including Combined Arms Maneuver, Wide Area Security, Show of Force, Deception, Denial and Incursion.
    a. The conduct of large scale Conventional Force exercises near a potential cross-border area of operations.
    b. Increased deployment of Conventional Forces, positioned in a country by formal agreement to expand capabilities in pre-existing bases.

Winning the current and the future strategic operating environment will require new indications of challenges, threats, and opportunities across the operational continuum with particular emphasis on the Gray Zone.

> …we must prioritize human considerations in planning and execution and find ways to influence the 'will to fight' and decision-making of relevant actors in the environment.
>
> —GEN Joseph L. Votel, Commander USSOCOM, Remarks to Strategic Multilayer Assessment Conference, 28 October 2015

Introduction

This paper explores the hypothesis that accurately seeing, assessing, and understanding the challenges and risks within the current and emerging security environment will require new thinking about indications for a complex world. This paper recognizes the need to consider a new and broader range of strategic indications of challenges, threats, and opportunities across the entire operational continuum, however, the paper confines its exploration to strategic indications in relation to the Gray Zone. Critical to this effort will be a comprehensive understanding of the Human Domain with emphasis on the physical, cognitive and moral frames, within the environment, and what they represent to successfully compete and win in the space between peace and war.

The United States Special Operations Command (USSOCOM) white paper, *The Gray Zone*, recognizes that Gray Zones are characterized by ambiguity and uncertainty regarding who or what an adversary may be.[2] This ambiguity poses distinct challenges to the current warning intelligence paradigm premised on an identified adversary.[3] Adding to the ambiguity are the methodologies that may be employed in Gray Zone conflicts. The Cold War model of a "threat/response cycle" of move and countermoves is predicated on a defined doctrinal or situational template (SITEMP), which is elusive to frame when considering Gray Zones.[4] This raises an important question. What are the SITEMPs of known and unknown adversaries and threats in the Gray Zones?

This paper frames thinking how the U.S. can develop human domain indications that inform actions to meet Gray Zone security challenges early on the left side of the operational continuum. It will inform the Department of Defense's direction to "[clarify] the roles and responsibilities of the Department of Defense in providing indications and warning of, and protection against, acts of unconventional warfare."[5] Moreover, understanding indicators that lead to warnings of Gray Zone challenges requires a more comprehensive analytic mindset to appreciate ambiguity.

A key finding from USASOC's Modern Russian Unconventional Warfare Case Study Forum in March, 2015 highlighted both Comprehensive Deterrence and the need to understand Gray Zone indications to inform deterrence decisions. In terms of thinking, there is a need to update the Cold War concept of Political Warfare for the early 21st Century security environment. In the strategic and operational arenas, there is a need to perceive indications of challenges, threats, and opportunities for the non-standard campaigns that state and non-state actors are pursuing on the left side of the operational continuum.

A persistent challenge of strategic warning is collecting sufficient indications of emerging challenges, threats and opportunities. A related challenge is the subsequent assessment of those indications, without which the indications are merely data points. While continuing to rely on the intelligence community to collect and assess many information requirements for strategic warning in the Gray Zone, DoD has organic capabilities to gain a unique deep knowledge of operational environments. DoD can apply knowledge obtainable only through persistent presence involving personal interactions and relationships to the collection and assessment of indicators. If this deep knowledge and perception is captured and shared properly, we could integrate it with more robust open source analytic methods and technologies to more clearly see social currents emerge. This understanding allows decision makers to see and assess challenges, threats, and opportunities early and to apply resources that can influence problem trajectories to favor U.S. objectives.

Framing Assumptions

Within the environment, we see economic, social, political, informational, and ideological trends in international competition are converging among State, Non-State actors, and others. They seek relative superiority over the physical, cognitive, moral security and adequate governance of populations. In a hyper-connected world, they increasingly challenge the traditional concepts of sovereignty and identity.

The following assumptions can be applied to the future operational environment:

1) The operational environment will remain complex, and disordered. International norms will continue to constrain the application of force.
2) The totality and variety of the security challenges demand a relook at what constitutes strategic risk in the early 21st Century operating environment.
3) The fiscal reset will likely continue to reduce governmental resources, which presents obvious challenges. However, it presents opportunities to consider new frameworks, new operational approaches and new capabilities.
4) The political will to conduct large-scale military campaigns against non-existential threats will likely continue to wane.
5) The march of commercial technology and its militarization will likely accelerate in the coming years.

Central Idea

Current strategic indications predominantly focus on state adversaries capable of employing large-scale conventional forces and/or nuclear weapons, with conflict envisioned as occurring on the right side of the operational continuum. We must continue to see, assess, and understand risk for state and non-state capabilities on the right side of the operational continuum. However, we

must also develop the ability to see, assess, and understand the risk of state and non-state capabilities in the Gray Zone. The competition unfolding in the Gray Zone requires that we develop indications to assess, sort, form responses, and rescale security challenges much earlier in their development and risk profiles.

Based on the current and future strategic operating environment, the U.S. must develop strategic indications of challenges, threats, and opportunities for Gray Zone security challenges with the same rigor as done during the Cold War.

Key Themes

1) Thinking about strategic indications, which has its roots in Cold War ballistic missile defense, largely focuses on high-end conflict conducted by Nation States on the right side of the operational continuum.
2) Investment in thinking for indications in the Gray Zone is warranted to meet the growing challenges we face in this space.
3) Gray Zone indications will require a shift from primarily observing and calculating physical capabilities to also include seeing, assessing, and understanding the physical, cognitive, and moral frames within the strategic operating environment. Most notably, this shift to a broader, more inclusive framework will require greater understanding of how we think about and visualize cognitive maneuver.
4) The growing trans-regional implications of competition and conflict will require exploration of the trans-regional indications for state and non-state actors.
5) Indications for the Gray Zone will require a multi-disciplinary approach to better inform risk, readiness and decision-making.
6) The totality and the varied nature of the security challenges across the operational continuum require consideration of the potentially systemic risk we face in a complex world.

Strategic Appreciation

The 2015 National Security Strategy (NSS) recognizes an interconnected global system of participants, with power struggles anticipated both among states and beyond state structures.[6] Critical considerations for decision makers thus center on the locus of power struggles; their impact on national interests; the advisability of reprioritizing regional and global security concerns; and the implications of all these considerations for preserving the elements of national power. The 2015 National Military Strategy (NMS) envisions such an eventuality, by identifying a global security context that requires a "competitive advantage… [in] early warning and precision strike."[7] Retaining a competitive advantage in precision strike and the host of advanced technologies remains an essential cornerstone of the national strategy. However, the

NMS also estimates that "the probability of U.S. involvement in interstate war with a major power is assessed to be low but growing,"[8] and another form of threat is more likely. This threat, "hybrid conflicts," serve(s) to increase ambiguity, complicate decision-making, and slows the coordination of effective responses and… will persist well in to the future."[9] Moreover, the NMS emphasizes the global nature of information flows and information technologies. The power of information and the power of access to information are moving the agency and velocity of decision making from the individual to the transnational level. Finding clarity in ambiguity and enabling decision-making to address the challenges of the new environment will be essential. This is in part why the U.S. Army Special Operations Command (USASOC) is purposely "[investing] in new ideas and capabilities to anticipate changing environments and new demands in order to maintain a competitive edge over our Nation's adversaries."[10]

Strategic Quality of the Gray Zone

Is the Gray Zone strategic? The short answer is, yes. What is strategic about the gray zone? The answer to that question depends on the context of a particular gray zone challenge. Adversarial competition in the Gray Zone can become highly consequential (and therefore strategic) over time and frequency due to, "cascading secondary and tertiary effects created by the development of the threat or its convergence with other trends." The pursuit to understand strategic indicators in the gray zone presumes that the gray zone is of strategic value. While this assumption is reasonable and likely valid, the very nature of Gray Zone ambiguity demands greater appreciation of the potential contained within various gray zone challenges.[11] One look at the ongoing challenge of ISIS demonstrates that the question of determining a strategic quality is not so simple.

The President said in his final state of the union speech "Both al Qaeda and now ISIL pose a direct threat to our people…[however] they do not threaten our national existence."[12] Did the President, in effect devalue the ISIS threat as something less than strategic? That depends, because in the same week as the President's speech, the former Acting Director of the CIA, Michael Morell, testified, "I believe ISIS poses a significant strategic and lethal threat to the United States of America."[13] The ISIS problem does constitute a gray zone challenge. However, is it a strategic threat?

Strategic Parameters

No document directly defines threats to the U.S. that are strategic in nature.[14] In practice, strategic understanding of the operational environment is derived from key strategy documents, namely the National Security Strategy and the National Military Strategy. They identify strategic risks and security interests that bound strategic parameters.

NSS Strategic Risks	NMS National Security Interests
Catastrophic attack on U.S. homeland or	Survival of the nation

critical infrastructure	
Threats or attacks against U.S. citizens abroad and our allies	Prevention of catastrophic attack against U.S. territory
Global economic crisis or widespread economic slowdown	Security of the global economic system
Proliferation and/or use of weapons of mass destruction	Security, confidence, and reliability of our allies
Severe global infectious disease outbreaks	Protection of American citizens abroad
Climate change	
Major energy market disruptions	
Significant security consequences associated with weak or failing states	

Together, the NSS and NMS form strategic considerations for how threats could be perceived. Just because one could consider a threat strategic does not necessarily mean it demands full priority for resourcing. In other words, strategic threats are not all equal. That demands a measure of strategic value, which underlies the point of this paper.[15] Are Gray Zones of strategic value?

Gray Zones are strategically important because the long-term effect of inattention or miscalculation of emerging patterns and trends result in strategic risks that affect national security interests. The challenge with determining the strategic value of gray zone activities is that by their ambiguous nature, they may not present immediately clear and present dangers. Instead, their strategic quality is a function of their potential to metastasize over time, becoming a strategic risk or of strategic interest. The Gray Zone demands proactive engagement, to monitor benign indications that over time reveal new security patterns. The risk of failing to appreciate the potential trajectory of an observed gray zone challenge is the strategic quality of the gray zone.

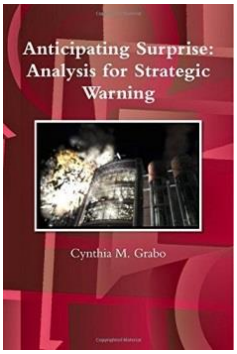
Planes of Perception - "How does surprise happen?"

Potential responses to this question could involve priorities, distraction, or gaps in policy or situational understanding. Strategic warning should drive proactive thinking and stimulate preemptive actions that mitigate the potential consequences of any surprise. To that end, in the framing of the paper we considered the following lines of inquiry for explaining Russia's annexation of Crimea in 2014.

1. We had the thinking, understanding and right mix of tools to observe indications in the Gray Zone but prioritized their use in other areas.
2. We had the thinking, understanding and right mix of tools to observe indications in the Gray Zone but were distracted by other priorities.
3. We had the thinking, understanding and right mix of tools to observe indicators but our response was limited by policy constraints.
4. We had the right tools, but did not have the thinking and understanding to observe indications in the Gray Zone.

In this paper, we pursue the fourth line of inquiry that we have the right tools, but don't have the thinking and understanding to observe indicators and provide strategic warning for the Gray Zone. We chose this line of inquiry to examine the overlapping physical, cognitive, and moral planes of perception in Gray Zone conflicts. **Understanding these planes and their integration underlines an enduring challenge of intelligence warning for the Gray Zone – that of synthesizing new kinds of information for analysis.**

Key Definitions



To make logical connections between observations of operators and / or analysts and resource decisions of commanders, a few definitions must be understood regarding strategic indications. Joint doctrine defines some of these terms but these definitions are insufficient for discussions of the Gray Zone. This paper will rely on the work of one of the intelligence community's foremost indications analyst, Cynthia Grabo, to add clarity and consistency to the remainder of this discussion.[16] She was a recognized authority in the field of strategic warning that wrote and lectured extensively on the subject in the Intelligence Community. Her originally classified textbook for the training of analysts in the field was condensed, declassified and reissued in 2004 under the title *Anticipating Surprise: Analysis for Strategic Warning*.[17]

Indications and Indicators

Indications include "information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action."[18] Sometimes the phrase "indications and warning" is used as a singular description of combined aspects of the environment. Furthermore, we should note that doctrinally, the phrasing "indications and warnings" or "indicators and warnings" has now been termed, simply "warnings."[19] Nevertheless, indications point to possibilities, positive, negative or ambiguous.[20] An indicator in intelligence usage is "an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action."[21] The way indicators fit together in context to the environment, such as the underlying social and political currents, may suggest evolving or emerging developments. This is why indicators are often found as "indicator lists."[22] They are known or anticipated factors that when observed confirm assumptions.

Strategic

Strategic is defined as: "Relating to the identification of long-term or overall aims and interests and the means of achieving them; Carefully designed or planned to serve a particular purpose or advantage; Relating to the gaining of overall or long-term military advantage; Of human or material resources essential in fighting a war." In some discourse, the term refers only to

systems or weapons related to high technology capabilities and the threats those capabilities are meant to deter or defeat, including existential threats. This paper uses the more broad meaning, which includes human resources, emphasizing activities that occur within the human domain.

Strategic Warning

Strategic warning is “a warning prior to the initiation of a threatening act”[23] and "relatively long-term, or synonymous with the 'earliest possible warning'"[24] in contrast to tactical warning, which is “warning after initiation of a threatening or hostile act.”[25] The idea of indications and intelligence warning is rooted in Cold War defense strategies, namely those related to ballistic missile defense. For example, in 1979, the U.S. Air Force initiated a Rand Corporation study to attempt to understand strategic warnings of intercontinental threats. Of importance throughout the study was the significance of interpreting myriad signs in context.[26] Much of what matters with a warning is that it is assessed accurately—that the warning is what one thinks. Accurate perception comes from the complementary association of observations and interpretation of those observations.

Human Domain

The USSOCOM Operating in the Human Domain concept asserts, "The people (individuals, groups, and populations) in the environment, including their perceptions, decision-making, and behavior. Description: Operations in the Human Domain depend on an understanding of, and competency in, the social, cultural, physical, informational, and psychological elements that affect and influence the domain. These operations require the application of capabilities through the five elements to identify and influence relevant populations to enhance stability, prevent conflict, and, when necessary, fight and defeat adversaries. The success of any strategy, operation, or tactical action depends on effective operations in the Human Domain. In some respects the Human Domain is a medium of people in the environment over which SOF must exercise influence and compete for advantage with adversary forces. The Human Domain is also a sphere of knowledge and activity."[27]

Comprehensive Deterrence

"The prevention of adversary action through the existence or proactive use of credible physical, cognitive, and moral capabilities that raise an adversary's perceived cost to an unacceptable level of risk relative to the perceived benefit." [28]

Perception - The Key to Perceiving the Human Domain

Perception relates to the proactive pursuit of information to apply deterrence approaches. Combined with an active process of assessment, it answers a number of vital questions. What do the emerging signals mean? What do they indicate? What warnings are recognized? Those are

critical questions that require deliberate and well-refined approaches to not only make sense of environmental observations but render credible warnings for actionable decisions.

In a 1979 Rand study on the "Role of Strategic Warning in Conflict Management," Edmund Brunner argued that "[all] other steps in the chain may be forged and in place, but unless this perception occurs there is no strategic warning." [29] Observing something and perceiving something are two entirely different but related aspects of deriving indications. One could observe a point of information but not perceive the implication that information might hold. Hence, perception is an active process.[30] It requires iterative testing of hypotheses, challenging biases, contextual understanding, and acknowledging expectations.

Those biases, understanding, and expectations reflect the complexity of the Human Domain. The Human Domain consists of the people (individuals, groups, and populations) in the environment, including their perceptions, decision-making, and behavior.[31] As such, the matter of perception is in part paradigmatic. It depends on the frame of reference in which one views the operational environment. A look at the recent annexation of Crimea by Russia offers a platform upon which we can examine differing planes of perception.

In 2014, Russia annexed Crimea after waging a subversive unconventional warfare campaign in which Russian influences seemingly materialized from within Crimea. In actuality, Russian influence occurred in the Human Domain, among the people of Crimea, hidden in plain sight.[32] They maneuvered within populations and groups in their perceptions, decision-making, and behavior. The Russians seized the initiative by working in the Human Domain to physically secure Russians in Crimea and achieve Russian national objectives. A record of studies foresaw the potential for Russia's actions. Unfortunately, many analysts did not.

Given the growing trans-regional nature of conflict, we need to consider as well the strategic indicators and warnings for the trans-regional operating environment.

Evolving Considerations of Indications - From Seeing to Perceiving the Environment

In the past, intelligence professionals and strategic planners relied on formulations from methodologies to explain actor behavior. Stakeholders invested in monitoring the environment for indicators that confirmed anticipated behaviors. Intelligence and information collection focused on relatively known adversarial challenges.

The literature discussing indicators, warnings, strategic surprise, and related early warning subjects are extensive. In the broadest sense, there are two schools of thought. One school of thought, generally skeptical of foresight, assumes that unforeseen events will always catch unsuspecting actors off-guard and that those events cannot be accurately predicted. They advocate for policies of resilience to *react* to inevitable surprises. The other school of thought

more optimistically presumes that future surprises can be anticipated. There are varying degrees of confidence associated with the latter school of thought ranging from random guessing, to possible scenarios, to probable scenarios, to forecasting particular events. One consistency in virtually all the literature surveyed for this paper is the importance of contextual understanding that overlays the assembly of environmental observations. [33]

In other words, the existing literature reinforces the concept of moving beyond seeing to perceiving currents in the environment. Moreover, there is a consistent voice emphasizing multidisciplinary synthesis of ideas to overcome thinking that is locked into a particular model. In a 1979 Rand study, Edmund Brunner notes, "The chances for deception and surprise can at least be diminished and chances for the perception of strategic warning be raised by systematic attention to measures for avoiding information failures and the evils of groupthink, for encouraging genuine Devil's Advocates and independent thinkers, and the expression of alternative and probably unpopular views."[34]

The various early warning literature also demonstrate that governments view the operational environment through two frames of reference: monitoring and discovering.[35] One frame of reference deliberately looks for key environmental observations. The other takes notice of observations as indicative some yet unknown pattern. Both frames of reference differ whether one looks for observations to confirm assumptions or whether one observes indications and determines what they indicate. The former is characteristic of Cold War monitoring, whereby relatively known adversarial challenges focus the attention of intelligence and information collection.[36] The latter is characteristic of steady state and Gray Zone environments where the nature of security challenges is ambiguous. In either situation, the way the U.S. combines human interactions with Human Domain analysis will give decision makers a more comprehensive understanding of cognitive and moral security dimensions.

Monitoring - Looking for Indications

When one cognitively or doctrinally constructs potential scenarios, they then look for indications confirming that those scenarios appear to be playing out. As mentioned, this Cold War activity assumes a degree of confidence understanding the security environment. The Cold War is instructive for thinking about Comprehensive Deterrence approaches and indicators of adversary intentions. During this period, the bipolar world witnessed persistent political warfare as a means to avoid general warfare.[37] The U.S. recognized that the USSR would use “tactics of division and subversion to weaken the free world alliances” and that “such political warfare [would] seek to exploit differences among members of the free world, neutralist attitudes, and anti-colonial and nationalist sentiments in underdeveloped areas.”[38] The U.S. sought to address the Soviet challenge through “feasible diplomatic, political, economic and covert measures to counter any threat…and exploit troublesome problems for the USSR…”[39]

During the Cold War, the Soviet Union provided the United States with a relatively definable threat. In order to predict Soviet actions, intelligence professionals and strategic planners relied on formulations from methodologies to explain actor behavior. Thus, stakeholders invested in monitoring the environment for indicators that confirmed anticipated behaviors.[40]

An example of that kind of methodology is in the current Joint Intelligence Preparation of the Operational Environment (JIPOE) process whereby likely and dangerous courses of action determine collection requirements to confirm those enemy courses of action.[41] This four-step process attempts to give analysts a holistic view of the environment.

Doing so necessarily demands situation templates or a likely scheme with which an actor will act based on their doctrine or historical patterns. In this case, one knows what they are looking for. They seek signs to validate a hypothesis. There is, however, an important risk associated with this warning lens. An overreliance on a particular behavior model could lead decision makers to either incorrectly or inadvertently take the wrong actions against a problem set.[42] In essence, faulty models could lead to faulty interpretations of observations.

Discovering - Noticing New Patterns of Indicators

In an environment without an obvious security concern, what does one look for when one does not know what to look for? The alternative frame of reference is more passive in nature, taking account of all observations as potential indications of some outcome. In some literature, this methodology is a form of discovery, to uncover the existence of patterns. Cavelty and Mauer describe this as "not about pattern recognition or detections of known patterns: it is about pattern discovery or the identification of new patterns."[43] This is about figuring out what the unknown unknowns are, which demands a creative way of thinking about the environment to see new patterns.

Institutionalizing imagination will lead to possible and probable scenarios. Any environment presents indications that when viewed in retrospect reveal the origins of outcomes. The challenge for decision makers is prioritizing resources to be in the right places at the right times either when situations emerge or as quickly thereafter to influence potential trajectories. One way to think about this approach is to consider business intelligence processes that seek environmental understanding to gain a market advantage against competitors.

Much like defense and national security agencies, businesses employ intelligence processes to understand their market environments. Those market observations give business leaders data for investment opportunities and strategic investment risks. Business intelligence is not a codified process recognized throughout various industries; however, the variety of methods businesses use to analyze their competition and the market environment fall within the strengths, weaknesses, opportunities, threats (SWOT) framework. The idea is that they use information within the environments of markets and consumers to understand such things as demands,

competitors, risks, trends, economics, growth opportunities, etc. In Gray Zone environments where uncertainty about potential and possible security challenges by definition is unclear, understanding requires broad, holistic, and in some ways wholly new approaches.

One illustration of an approach to begin seeing and understanding in a different manner comes from a draft consideration to an "expanded warning problem set." The draft *United States Army Functional Concept for Intelligence 2020-2040* suggests looking at "human factors" as a part of a broadened aperture.

> The warning problem set is expanded from conventional military indicators. Political, economic, cultural, criminal, social, and other human factors may threaten U.S. interests and trigger a security response that involves Army forces. Non-state actors, criminal enterprises, enemy and adversary information operations, state actors exercising political subversion, proxy sanctuary, intervention, coercive deterrence, and negotiated manipulation all may threaten U.S. interests. Warning intelligence must include those factors to support operational planning, to build regional knowledge, and to maintain currency in the knowledge base. Influences that affect human behavior and could impact U.S. interests is part of the warning intelligence process in the future OE.
>
> —United States Army Training and Doctrine Command, *United States Army Functional Concept for Intelligence 2020-2040*, Draft Version 0.9, 15 December 2015

A holistic view of the Gray Zone requires more than a threat focus: it demands a fused approach to not only identify threats but also to discover challenges and opportunities.

Considering Indications to Perceive New Patterns

In a recent monograph published by the Strategic Studies Institute, Dr. Michael Mazarr identifies that Gray Zones present a number of challenges, namely in characterizing what exactly constitutes their nature.[44] The fact that these ambiguous zones are not easily definable presents security planners and decision makers with a conundrum. What are the particular Gray Zone indicators that warn of emerging security challenges? This is a problematic question because it depends on the nature and character of the particular Gray Zone phenomenon occurring over a given space and time. The USSOCOM definition is important to remember in this regard. While the Gray Zone is the space between peace and war, gray zone challenges are three things specifically: ambiguous aggressive conflict, opaque perspective-dependent actors, and uncertain legal frameworks (Figure 1).[45]

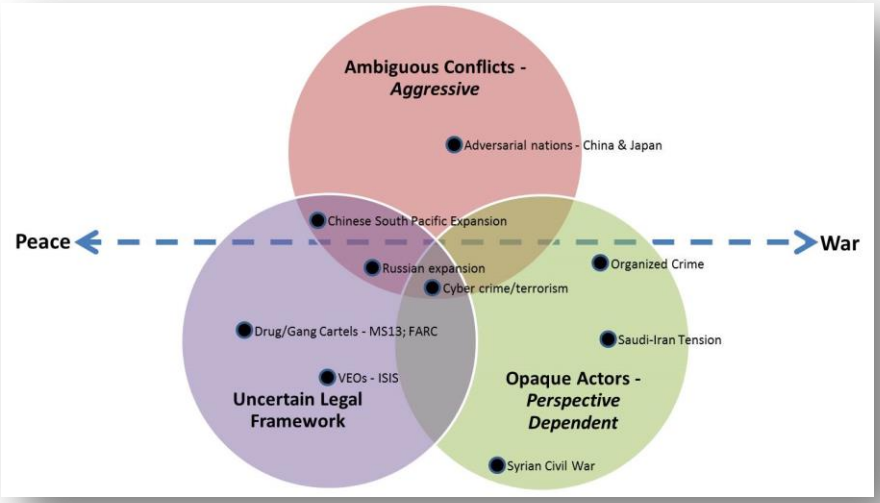


Figure 1 Gray Zone Characteristics

Establishing what the Gray Zone is more specifically points observers toward particular kinds of activities to assess changing security patterns. This paper has suggested that generally a pattern of cognitive maneuver precedes moral influence to affect physical control as a meta-thematic template to take note of changes in the security environment. ***If we consider the opening premise as valid, that trends in international competition are converging for relative superiority, then the place where those trends compete is in the Human Domain.***[46] We should look there to find previously unknown patterns and emerging security challenges. What, then, are we looking for?

This is a critical question because it rests on the assumption that actors are the key component of human domain security challenges. This assumption is premised on the notion that disruptive actors pursue non-normative interests. Those actors need a certain measure of capacity to act on their motives.[47] Ideological, economic, value, and power interests drive motives. In other words, the strength of an actor's ideas coupled with their capacity determines the potential *velocity* with which they choose to pursue underlying motives. This is predicated on existing conditions, such as political, economic, social, and environmental factors.[48] Those conditions provide *mass* for an actor's influence. The relationship between motives and conditions is symbiotic; one is a function of the other. Neither is independent.

The latent variables of motive and conditions are what USSOCOM refers to as the potential energy in the international system.[49] In order for that potential energy to emerge as a true security challenge, there must be a pretext for action. Actors seek or wait for opportunities through which they may seize an initiative. Opportunities include legal actions, economic tension, and socio-political disruptions. Depending on the context of the conditions, potential actors use mechanisms or triggers to generate momentum for their motives. These triggers are

how actors pursue their interests. They are the variety of cognitive maneuvers, moral influences, and physical controls that determine the trajectory of a security challenge.

A Human Domain Model that comprises the aforementioned elements is one of the principle consistencies characteristic of Gray Zone challenges (Figure 2). It frames how to view the Human Domain to synthesize interrelated aspects and perceive seemingly unnoticeable currents. Viewing the Human Domain in this way, how could one observe the operational environment to either anticipate gray zone challenges or understand the nature of an existing challenge?

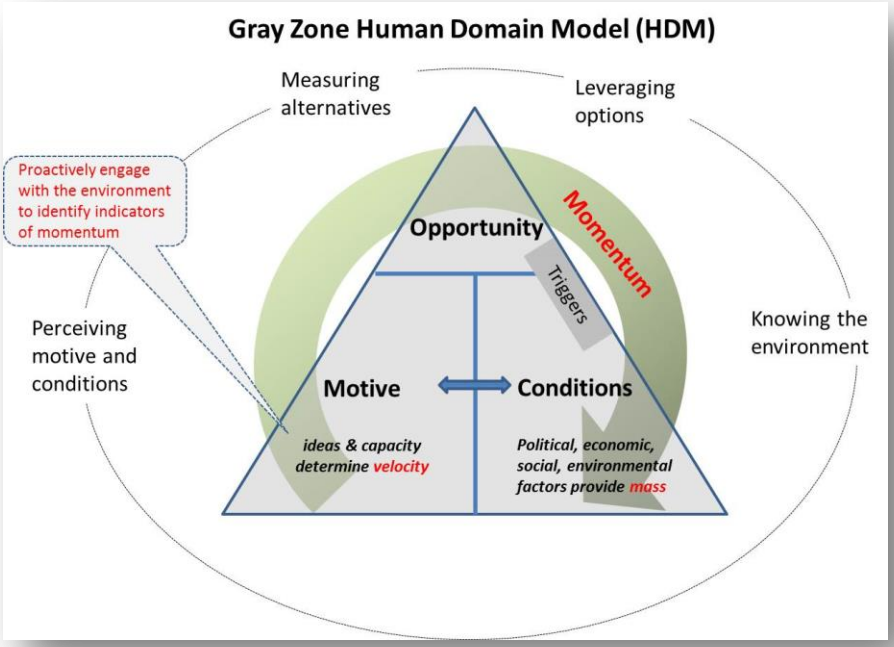


Figure 2 Human Domain Model (HDM)

Three interrelated functions should work together to assess how the Human Domain presents a strategic security challenge: information study, intelligence analysis, and operations knowledge. Together, these functions look for context-specific indicators with regard to motives, conditions, opportunities, triggers and momentum.

- They look for signs of actors with new or changing motives to include actors' capacity to act on those motives.
- They apply multidisciplinary lenses to study the conditions in the operational environment, evaluating the potential energy between the mix of motives and conditions.[50]
- They look for catalysts through which opportunity could be seized or positional advantage could be gained.

- They measure the concentration of triggers indicating the direction and magnitude of an actor generating momentum.
- They calculate that momentum along a potential trajectory to determine the zone in which to alter the conditions and change the trajectory's direction.

The ability to notice subtle signals in the operational environment demands a different form of discovery—different from intelligence analysis alone. It involves studying a wide array of factors to synthesize their interrelated relationship. No definitive list of factors sufficiently explains how latent potentials evolve into surprising security challenges.[51] For instance, one survey of 30 early-warning models arrived at 825 varying indicators.[52] The survey authors conclude, "different prediction models have different end-states in mind, and thus place a base value on very different issues."[53] Their observations as to the utility of predicative models appear skeptical, pointing out that "even the experts tend not to get it right any more than lay people do." However, they raise a fundamentally important point with respect to the human domain. In spite of the exponential number of permutations from any array of indicators, continual engagements with people in the environment lend perceptive credibility to observed data.[54]

Perceiving Gray Zone challenges requires the capacity to identify, understand, and synthesize complex elements in context. The synthesis requires a fusion of intelligence, information, and operational knowledge to provide the holistic view.

One demonstration of how we could assess the human domain used a similar survey analysis approach to categorize leading indications of state-based, UN Article 2 threshold aggression. The kinds of activities that likely precede state actions to forcibly attain national objectives through ambiguous conflict, opaque actors, and uncertain legal frameworks include the following:

1. **Unconventional Measures**: tactics short of conventional war to coerce, destabilize, or overthrow a government.
    a. Use of persistent, low-level actions across the physical, cognitive and moral frames to desensitize observers of future action.
    b. Use of clandestine and covert intelligence and special operations elements to conduct Preparation of the Environment and other activities
    c. Increased activity within the human domain to "hide" campaign "in plain sight."
2. **Non-Military Measures**: political, economic, and diplomatic means to create positional advantage in regards to time, forces, relationships, ideas and geography.
    a. Development of political/economic ties to nations, key officials and/or the private sector within the area of interest.
    b. Employment of targeted political/economic ties toward campaign objectives.
3. **Leverage Population-based Power**: influencing and mobilizing groups to action.
    a. Use of aggrieved/exploitable population segments to potentially "host" follow-on forces.

    b. Increased activity of the targeted population directed toward campaign objectives
4. **Information Measures**: messaging and propaganda for deception and denial to set conditions for follow-on action.
    a. Use of macro/micro narratives to provide pretext for future action
    b. Increase in public opinion and propaganda efforts to foster ambiguity and misdirection toward the nature, scope and duration of unfolding campaign
5. **Lawfare Measures**: self-identified legal frameworks and processes to advance interests and coerce or compel others.
    a. Declaration of intent based on legal premise to take action.
    b. Expansion of territory based on caveat, national law or precedent.
6. **Technology Measures**: the use of existing and new technologies in standard and non-standard ways including the use of: Cyber, Unmanned Aerial Systems, basic and advanced weapons, such as precision munitions, robotics, and CBRN.
    a. The use of cyber domain to conduct recruitment, finance operations, operational planning and propaganda.
    b. The use of cyber-domain attacks against civil, military, and governmental targets.
7. **Conventional Military Measures**: the employment of conventional forces to support strategic objectives by employing capabilities including Combined Arms Maneuver, Wide Area Security, Show of Force, Deception, Denial and Incursion.
    a. The conduct of large scale Conventional Force exercises near a potential cross-border area of operations.
    b. Increased deployment of Conventional Forces, positioned in a country by formal agreement to expand capabilities in pre-existing bases.

Ultimately, a view through some form of Human Domain Model or design methodology will enable a fused effort of multiple disciplines working together to anticipate the trajectories of emerging problems. Through iterative assessments and feedback mechanisms, they could adjust that hypothetical trajectory over time.

The U.S. must develop a new form of discovery for the Gray Zone, one that uncovers the existence of patterns in order to assess their larger meaning. We must be able to detect our adversaries' efforts of cognitive maneuver as manifested by observable or detectable indications and thereby provide warning of the subsequent effects within the Human Domain.

Anecdote - Russia Annexation of Crimea - a History of Russian Maneuver

The annexation of Crimea by Russia provides a useful anecdote to see how Russia's actions were actually observed, but on differing planes of perception. While the Russian encroachment came as a surprise to some in policy and defense planning communities, many signals were present and had been forewarned by those alert to Russia's historical context.[55] One report by the Atlantic Council even suggested that "[to] local residents and independent observers, the origins of the "little green men" were far from mysterious; their unmarked Russian military uniforms, Russian regional accents, and Russian-made weapons gave them away at first glance."[56] Moreover, the manner in which Russia leveraged popular support through subversive influence tactics fulfilled a longstanding doctrinal *modus operandi* to exploit strategic opportunities without instigating severe international reaction.[57]

A deeper look into the Russian-Crimea case example requires a separate study, so this paper will not attempt to fully analyze the situation. Nevertheless, what is relevant is to notice that Russia's intervention, either overtly or subversively should not have been any surprise at all. The following cursory sample of open source literature chronicles various signs revealing the trajectory Russia followed to annex Crimea from Ukraine.[58] These observations themselves may or may not be deemed "warnings;" however, they demonstrate that a deep understanding of the Human Domain could warn decision makers where they should invest security resources.

Timeline

- 1954 – "Indirect aggression works for the Russo-Chinese better than direct aggression. They have learned from their experience in Korea that direct military attack even when carried out by a subsidiary puppet irritates the free states…The Russians therefore operate only through their subversive fifth columns and propaganda in NATO."[59]
- 2009 – "Several actions could signal increased prospects for a major confrontation in Crimea…an upsurge in issuance of Russian passports in Crimea…Demonstrations in Sevastopol or elsewhere in Crimea also would raise the prospects, given the possibility of a clash (even if unintended) with Ukrainian internal security forces."[60]
- 2010 – "Russia's attempt to gain Western acceptance of spheres of influence is of concern because it coincides with other developments that seem designed to enable Russia to exert pressure on the states in the post-Soviet space and *in extremis*, even intervene militarily."[61]
- 2011 – "In fact, it appears that Russia is using *smart power*, a combination of hard military power and *soft power* operations (Nye 2008, 32), to use separatism as a geopolitical tool."[62]

These extracts from a wide range of references reveal a narrative over time of Russian subversion, their interest in Crimea, and the means to provoke secession.[63] While we can easily see the story unfold in retrospect, one should note that each of these references foretell of the eventual potentiality. In other words, those who made these observations about Russia and Ukraine were knowledgeable of the environmental context. They perceived a changing security challenge.

Using the Russia-Crimea example as a backdrop of how subversive maneuver in the cognitive space took place in one area of Eastern Europe, we can now piece together other similar actions in the region. When looking at the other examples, though, it is important to consider them from multiple layers to assess how similarly disruptive actions indicate a pattern of Russian operational campaigns that could be linked to broader strategic intentions. Indeed, Russia's recent political, military, and economic cooperation with China, Cuba, Syria, and Iran are indicative of their ability to be a trans-regional competitor.

Recent events have demonstrated the effectiveness of cognitive maneuver within the Human Domain. We must take these events as lessons learned to inform future U.S. efforts to detect aggression.

Estonia and Planes of Perception

In 2007, a series of cyber-attacks on government agencies, public goods and local business caused a significant disruption of Estonian life. What began as a seemingly benign decision by the Estonian government to move a statue, memorializing "the unknown soldier in WWII,"[64] resulted in a multi-pronged series of cyber-attacks targeting public and private facets of Estonian life. These virtual attacks coincided with a series of riots, which seemed to be further spurned by instructions distributed through various internet sites.[65] Instructions seemed to perpetuate from bloggers and other computers around the world. In many instances, those instructions came from unwitting personal computers, a result of dormant "botnets" having been surreptitiously installed by unsuspecting internet users.[66] Initially the attackers could not be identified, but evidence began mounting, pointing to Russian computer systems.

The question Estonia and the rest of the international community still wonder is, to what extent was the Kremlin complicit in the attacks? Were they merely a spontaneous virtual uprising by a disaffected Russian diaspora? If the Russian government perpetrated these attacks, they potentially indicate a situational template of preparatory virtual fires to shape an operational area. Alternatively, they represent a Gray Zone security challenge that is even more ambiguous. In a report analyzing the Estonian cyber-attacks, Stephen Herzog warns, "in the information age, computer-savvy individuals can now threaten the sovereignty and wellbeing of nation-states, oftentimes from the comfort of their own homes."[67] This is the kind of obscure threat that precisely represents the need to better understand Gray Zone indications.

How does the Estonian cyber example matter to this discussion of indications? If viewed from a local level, one might deduce that an increase in cyber-related attacks or denial of service operations indicate an impending follow-on attack. That was certainly the case in Georgia in 2008.[68] However, if we expand our view to a broader operational level, one might see a pattern forming whereby Russia is attempting to increase its operational reach. Broaden the aperture even further and the trajectory of Russian strategic intentions potentially point toward dominance as a superpower.

The point with this thought experiment is not to fully analyze Russian intentions. Instead, this conceptual anecdote demonstrates that on multiple levels, the perception of indications suggest different degrees of intention. The challenge, then, is to discern the ongoing patterns in the short to mid-term to apply resources toward them. Moreover, the Joint Force must discern emerging patterns of security challenges over the long term to focus strategic readiness considerations.

Strategic indications and warnings in the Gray Zone contain challenges in determining intentions because of the ambiguity of the environment and the inherent difficulty in assessing perceptions from multiple actors. Hence, we will need the requisite data and level of analysis to discern intent behind the capabilities.

The Human Domain - Maneuver in the Cognitive Space

Drawing the line between history, theory, and doctrine unveils an important principle of strategy that the post-modern military theorist, Colonel John Boyd, emphasized: "The central theme [of strategy] is one of interaction/isolation while the key ideas are the *moral-mental-physical means* toward realizing this interaction/isolation."[69] Boyd demonstrates that interacting with the environment, through cognitive approaches to influence the moral dimension, is mostly a competition in the Human Domain. As the Russian actions leading to the annexation of Crimea show, *they reveal maneuvers in the cognitive space for influence of Crimean moral and cognitive security, which transcends to their physical security.*[70] Similarly, GEN Joseph L. Votel, Commander of USSOCOM, described the contest in Gray Zones as, "a battle for the willingness of the people, the populations that are affected by it, the actors that are orchestrating it, the neutrals that are on the sidelines on this and it really is a struggle for influence with those different audiences."[71]

As the Gray Zone environment is characterized as one where influence serves as a significant instrument, it suggests that achieving influence could come about through an applied understanding of the elements associated with the Human Domain. It speaks to an approach that operates not in physical terrain but in a cognitive space, through people and populations. It resembles what Dr. Henry Kissinger noted in 1955 was an "immediate task [to] shore up the indigenous will to resist, which in the 'grey areas' means all the measures on which a substantial

consensus seems to exist: a political program to gain the confidence of local populations and to remove the stigma of colonialism from us."[72] This suggests that a planned, organized, and managed approach to this effort could be seen as a strategy of deliberate steps in a form of new maneuver, namely maneuver in the cognitive space. One of the questions this paper leaves open is the question of how to maneuver in the cognitive space. The anecdote of Russian activities in Crimea presents only one example of statecraft and a state's policies to influence other populations. The way the Russians developed and then employed both their meta narratives and their more nuanced micro narratives require further exploration. How do those meta narratives form and how do the micro narratives that shape social behavior change?

The idea of maneuver in the cognitive space demands further research and prototyping, particularly with respect to readiness considerations. One initial framework might see this form of maneuver as an umbrella construct for the many aspects related to achieving effects in the Human Domain. At the risk of unnecessarily prejudicing this early concept by a hasty assessment, the scope might present a line of operation within a strategy of Political Warfare. Disciplines such as PSYOP/MISO, Military Diplomacy, Public Affairs, and Information Operations would certainly fall into the construct. Incidentally, elements of the operational approaches found in hybrid tactics, the Chinese "Three Warfares," and the Russian "Gerasimov Model" might also fit. The scope could encompass leveraging the synchronized use of all instruments of national power. A framework such as maneuver in cognitive space might provide a context to consider operationalizing various related but disparate elements to address challenges in Gray Zone environments.

Conclusion

This paper has begun the process of illuminating the broad and varied set of current and future strategic operating environment challenges. It has made the case that addressing these challenges requires new understanding of the potentially systemic risk we face in a complex world. It has shown that our current thinking about strategic indications stems from Cold War thinking and largely focuses on high-end conflict conducted by Nation States on the right side of the operational continuum. This paper did not argue that such thinking is wrong. However, to meet the growing Gray Zone threat we face, we need to also think in terms of strategic indications on the left side of the operational continuum.

The strategic indications of a complex world will require a shift to a broader, more inclusive framework. The U.S. will need to move from simply observing and calculating physical capabilities to also observing, perceiving, and understanding the physical, cognitive and moral aspects within the Human Domain. This further requires expanding our concept of maneuver beyond the physical to include the moral and cognitive spaces. The growing trans-regional aspects of competition and conflict require new thinking about how we see and understand indications. We can no longer view them solely in regional frameworks.

Such a view requires a global context, which includes both security and governance challenges. Addressing Gray Zone challenges requires an iterative, multi-disciplinary approach to thinking about strategic indications. In turn, this must convincingly inform decision-makers as they determine readiness requirements for successful competition in an increasingly complex world.

Way Ahead

SILENT QUEST 16-1 will test the concept of comprehensive deterrence in the EUCOM AOR which will further inform our exploration of Perceiving Gray Zone Indications. SQ 16-1 will also continue USASOC's future force development efforts to maintain a competitive edge over our Nation's adversaries.

USASOC will further examine the themes identified within *Perceiving Gray Zone Indicators* with USSOCOM, Army, and USG partners and stakeholders through future iterations of SILENT QUEST, the USASOC Futures Forum, senior leader forums, and other venues as appropriate.

USASOC will continue coordination with the Intelligence Center of Excellence to develop the future broader, more inclusive framework for strategic indications requirements in the Gray Zone. To enable the framework USASOC sees its primary contributions as incorporating human domain factors and improving information sharing between "sensors" and analysts including joint, interagency, intergovernmental, and multinational (JIIM) partners. The "tools" are largely present, but we need to connect all of these "sensors" better, perhaps through breakthrough technologies and systems such as directed by *The Defense Innovation Initiative* Memorandum.[73]

Winning the current and the future strategic operating environment will require new indications and intelligence warnings across the operational continuum with particular emphasis on the Gray Zone.

Notes

[1] "Charter of the United Nations Chapter 1 Article 2." *United Nations.* Originally Signed 26 June 1945. http://www.un.org/en/sections/un-charter/chapter-i/ (accessed 03 14, 2016).
[2] US Special Operations Command, *The Gray Zone.* White Paper, Tampa : United States Special Operations Command, 2015, p. 1. Hereafter, *Gray Zone White Paper*.
[3] "Joint Intelligence," *Joint Publication 2-0.* Washington, D.C.: Joint Chiefs of Staff, October 22, 2013, p. I-28. Hereafter, JP 2-0.
[4] Strauch, Ralph, *Strategic Warning and General War: A Look at the Conceptual Issues.* Rand Note, Santa Monica: Rand Corporation, 1979, pp. 17-22. Strauch analyzes two types of threat/response cycles: single-track, and multi-track. The broader point with either type is that through analysis of a definable adversary, those anticipated tracks produce observable events based on template adversary behaviors.
[5] National Defense Authorization Act for Fiscal Year 2016, Public Law 114-92, § 1097.
[6] Barack Obama, *National Security Strategy* (Washington, D.C.: The White House, February 2015), p. 3-5. Hereafter, NSS 2015.
[7] U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015* (Washington, DC.: June 2015), p. 1. Hereafter NMS 2015.
[8] NMS 2015, p.4.
[9] NMS 2015, p.4.
[10] The USASOC commander, LTG Tovo, issued his revised mission and vision for the ARSOF in December, 2015, which specifically acknowledges the changing and uncertain nature of the future operating environment.
[11] *Ibid*.
[12] Obama, Barack, *Remarks of President Barack Obama - State of the Union Address As Delivered.* January 13, 2016. https://www.whitehouse.gov/sotu (accessed January 21, 2016).
[13] Morell, Michael, *Fight Against Islamic State Not Going So Well, Say Former Administration Officials.* January 12, 2016. http://www.armedservices.house.gov/index.cfm/2016/1/fight-against-islamic-state-not-going-so-well-say-former-administration-officials (accessed January 21, 2016).
[14] Differing theoretical approaches to international relations underpin each U.S. President's grand strategies. These approaches shape the degree to which American security interests emphasize participation in or retraction from regional and global affairs. For more see Layne, Christopher. "From Preponderance to Offshore Balancing." *International Security* 22, no. 1 (1997): 86-124. See also, Sestanovich, Stephan. *Maximalist: America in the World from Truman to Obama.* New York: Alfred A. Knopf, 2014.
[15] National interests are often qualified as some degree of importance. The U.S. Army War College teaches an intensity scale derived from social science practitioners, Donald Nuechterlein and Robert J. Art: survival, vital, important, and peripheral.
[16] Grabo, M. Cynthia, *Anticipating Surprise Analysis for Strategic Warning.* Washington, D.C.: Center for Strategic Intelligence Research, 2002 (Originally published as classified volumes between 1972-1974).
[17] "Cynthia M. Grabo, Notice," *Washington Post*, November 7, 2014, accessed December 23, 2015, http://www.legacy.com/obituaries/washingtonpost/obituary.aspx?pid=173080578.
[18] Department of Defense Dictionary of Military and Associated Terms," *Joint Publication 1-02.* Washington, D.C.: Joint Chiefs of Staff, March 15, 2015, p. 115. Hereafter JP 1-02.
[19] JP 2-0, p. iii.
[20] Grabo, p. 3
[21] JP 1-02, p. 115.
[22] Grabo, p. 3.
[23] JP 1-02, p. 233.
[24] Grabo, M. Cynthia, *Anticipating Surprise Analysis for Strategic Warning*. Washington, D.C.: Center for Strategic Intelligence Research, 2002 (Originally published as classified volumes between 1972-1974), p.3.
[25] JP 1-02, p. 241.
[26] Strauch, Ralph, *Strategic Warning and General War: A Look at the Conceptual Issues.* Rand Note, Santa Monica: Rand Corporation, 1979, p. 27.
[27] USSOCOM. *Operating in the Human Domain*. Operating Concept, Tampa: U.S. Special Operations Command, 2015, 76. Hereafter, Human Domain Operating Concept.

[28] USASOC, *Comprehensive Deterrence.* White Paper, Fort Bragg, NC: United States Army Special Operations Command, 2015, p. 9.
[29] Brunner, Edmund Jr., *Perception and Strategic Warning.* A Rand Note prepared for the United States Air Force, Santa Monica: Rand Corporation, 1979, p. 1. See also Grabo, p. 83. She concludes that "Warning has failed more often for lack of political perception than it has for lack of military evidence."
[30] Heurer, Richards J. Jr., *Psychology of Intelligence Analysis.* Center for the Study of Intelligence, Central Intelligence Agency, 1999, p. 7.
[31] USSOCOM. *Operating in the Human Domain.* Operating Concept, Tampa: U.S. Special Operations Command, 2015, p. 3.
[32] Czuperski, Maksymilian, John Herbst, Eliot Higgins, Alina Polyakova, and Damon Wilson, *Hiding in Plain Sight: Putin's War in Ukraine.* Washington, D.C.: The Atlantic Council, 2015.
[33] Walton, Oliver, "Helpdesk Research Report: Early Warning Indicators of Violent Conflict." *Governance and Social Development Resource Centre.* July 22, 2011. www.gsdrc.org/docs/open/HD777.pdf (accessed November 4, 2015).
[34] Brunner, Edmund Jr., p. 33.
[35] Cavelty, Myriam Dunn, and Victor Mauer, "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence." *Security Dialogue* 40, no. 2 (April 2009): 123-144, p. 129.
[36] Cavelty, Myriam Dunn, and Victor Mauer, p. 127.
[37] "A Report to the National Security Council," NSC 162/2 (Washington, D.C.: National Security Council, October 30, 1953). Hereafter NSC 162/2. Through the NSC 162/2, President Eisenhower established a "New Look," which was the administration's approach to sustaining a long duration challenge to the threat of Communism generally and nuclear attack in particular. The NSC 162/2 recognized that since atomic parity between the U.S. and the Soviet Union was forthcoming, the USSR would "continue to rely heavily on tactics of division and subversion to weaken the free world alliance" in an effort to avoid general war. Today the Joint Force distinguishes between traditional and irregular as the two forms warfare today.
[38] Ibid.
[39] Ibid.
[40] Cavelty and Mauer, p. 129-130.
[41] "Joint Intelligence Preparation of the Operational Environment." *Joint Publication 2-01.3.* Washington, D.C.: Joint Chiefs of Staff, May 21, 2014, p. V-1 – V-7. Hereafter, JP 2-01.3
[42] Cavelty and Mauer, p. 132.
[43] Ibid.
[44] Mazarr, Michael J., p. 101.
[45] *Gray Zone White Paper*, p. 1.
[46] Human Domain Operating Concept, p. 9.
[47] The capacity to act is a function of agency. Agency is a widely theorized element of international relations theory. This paper recognizes that with respect to potential gray zone actors, agency is the defining characteristic underlying that actor's potential; however, because the term is non easily understood, this paper will refer to an actor's motive and capacity interchangeably.
[48] Holsti, Kalevi J., "Theorising the Causes of Order: Hedley Bull's The Anarchical Societ." In *Theorising International Society*, edited by Cornelia Navari, 125-147. Great Britain: Palgrave Macmillan, 2009, p. 129.
[49] U.S. Special Operations Command, *USSOCOM's Strategic Appreciation.* Internal Document, Tampa: U.S. Special Operations Command, 2015, p. 1. Hereafter, *Strategic Appreciation*.
[50] *Ibid*.
[51] Barton, Frederick, and Karin von Hippel, *Early Warning? A Review of Conflict Prediction Models and Systems.* PCR Project Special Briefing, Washington, D.C.: Center for Strategic and International Studies, 2008. Frederick and von Hippel surveyed over 800 varieties of indicators across a multidisciplinary field of 30 early warning frameworks. One of their findings was that despite measured *post hoc* successes ranging from 70-90% in determining future outcomes, subjective analysis must still be applied and even then, policy maker must still be able to perceive the cost-benefit of optional countermeasures. See also associated early warning data set including indicator database.
[52] Barton, Frederick, and Karin von Hippel, see Appendix D, Matrix of Indicators, which captures the distribution of all 825 indicators across the 30 models.
[53] Barton, Frederick and Karin von Hippel, p. 11.

[54] *Ibid*. The authors recommend that, "Thorough, direct research involving a broad range of local actors and observers is likely to remain the best way to inform any early warning – and make the results credible."
[55] Czuperski, Maksymilian, John Herbst, Eliot Higgins, Alina Polyakova, and Damon Wilson. *Hiding in Plain Sight: Putin's War in Ukraine.* Washington, D.C.: The Atlantic Council, 2015, p. 4.
[56] Ibid.
[57] Finletter, Thomas K., *Power and Policy: US Foreign Policy and Military Power in the Hydrogen Age.* New York: Harcourt, Brace and Company, 1954, p. 101.
[58] Mazarr, Michael J., *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Monograph, Carlisle Barracks: United States Army War College Press, 2015, p. 35. Dr. Mazarr illustrates this point by noting "Aggressors can thus use "tactics of erosion," testing the "seriousness of a commitment by probing it in a noncommittal way, pretending the trespass was inadvertent or unauthorized if one meets resistance."
[59] Finletter, p. 101, 105.
[60] Pifer, p. 3.
[61] Larrabee, Stephen F.,"Russia, Ukraine, and Central Europe: The Return of Geopolitics." Journal of International Affairs, Spring/Summer 2010: 33-52, p. 37. Emphasis added.
[62] Roslycky, Lada L., "Russia's Smart Power in Crimea: Sowing the Seeds of Trust." Southeast European and Black Sea Studies 11, no. 3 (September 2011): 299-316, p. 299. Original emphasis.
[63] For a more complete chronology, see Appendix: Chronology of Russian Intentions Regarding Crimea
[64] Evron, Gadi, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Georgetown Journal of International Affairs* 9, no. 1 (2008): 121-126, p. 122.
[65] Evron, Gadi, p. 123.
[66] Clarke, Richard A., *Cyber War: The Next Threat to National Security and What to do About It.* New York: HarperCollins, 2010, p. 14.
[67] Herzog, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60, p. 54.
[68] Herzog, Stephen, p. 18.
[69] Boyd, John R. COL (Ret.). "John Boyd Compendium: Strategic Game of ? and ?" *Defense and the National Interest Project on Government Oversight.* December 2007. http://dnipogo.org/john-r-boyd/ (accessed December 9, 2015). Emphasis added. John Boyd, originator of the OODA loop theory of Observation-Orientation-Decision-Action, never published his thoughts. His ideas were captured in a series of lectures he presented throughout the 1980s and 1990s. Those presentations are available online at the cited reference. They are also available at: http://www.ausairpower.net/APA-Boyd-Papers.html.
[70] U.S. Army Special Operations Command, *Comprehensive Deterrence.* White Paper, Fort Bragg: U.S. Army Special Operations Command, 2015.
[71] GEN Joseph Votel interview by Howard Altman of the Tampa Tribune on 28 Nov 15, accessed December 15, 2015, http://www.tbo.com/list/military-news/gray-zone-conflicts-far-more-complex-to-combat-says-socom-chief-votel-20151128/.
[72] Kissinger, Henry A., "Military Policy and Defense of the "Grey Areas"." *Foreign Affairs* 33, no. 3 (1955): 416-428, p. 419.
[73] Charles Hagel, *The Defense Innovation Initiative*, Department of Defense, 15 November 2014, p. 2.

References

"A Report to the National Security Council." *NCS 162/2.* Washington, D.C.: National Security Council, October 30, 1953.

Bartkowski, Maciej. *Nonviolent Civilian Defense to Counter Russian Hybrid Warfare.* Study for Center for Advanced Government Studies, Washington D.C.: Johns Hopkins University Center for Advanced Government Studies, 2015.

Barton, Frederick, and Karin von Hippel. *Early Warning? A Review of Conflict Prediction Models and Systems.* PCR Project Special Briefing, Washington, D.C.: Center for Strategic and International Studies, 2008.

Bebler, Anton. "The Russian-Ukrainian Conflict Over Crimea." *Teorija in Praksa* 52, no. 1-2 (2015): 196-219.

Berzins, Janis. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy.* Policy Paper no. 2, Riga: National Defense Academy of Latvia, 2014.

Boyd, John R. COL (Ret.). "John Boyd Compendium: Strategic Game of ? and ?" *Defense and the National Interest Project on Government Oversight.* December 2007. http://dnipogo.org/john-r-boyd/ (accessed December 9, 2015).

Bremmer, Ian. "The Politics of Ethnicity: Russians in the New Ukraine." *Europe-Asia Studies,* March 1994: 261-284. International Security & Counter Terrorism Reference Center, EBSCOhost (accessed November 5, 2015).

Brunner, Edmund Jr. *Perception and Strategic Warning.* A Rand Note prepared for the United States Air Force, Santa Monica: Rand Corporation, 1979.

Brzezinski, Zbigniew. *Strategic Vision: America and the Crisis of Global Power.* New York: Basic Books, 2012.

Cavelty, Myriam Dunn, and Victor Mauer. "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence." *Security Dialogue* 40, no. 2 (April 2009): 123-144.

"Charter of the United Nations Chapter 1 Article 2." *United Nations.* Originally Signed 26 June 1945. http://www.un.org/en/sections/un-charter/chapter-i/ (accessed 03 14, 2016).

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to do About It.* New York: HarperCollins, 2010.

Czuperski, Maksymilian, John Herbst, Eliot Higgins, Alina Polyakova, and Damon Wilson. *Hiding in Plain Sight: Putin's War in Ukraine.* Washington, D.C.: The Atlantic Council, 2015.

"Department of Defense Dictionary of Military and Associated Terms." *Joint Publication 1-02.* Washington, D.C.: Joint Chiefs of Staff, March 15, 2015.

Evron, Gadi. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Georgetown Journal of International Affairs* 9, no. 1 (2008): 121-126.

Finletter, Thomas K. *Power and Policy: US Foreign Policy and Military Power in the Hydrogen Age.* New York: Harcourt, Brace and Company, 1954.

Giles, Keir, and Andrew Monaghan. *Russian Military Transformation - Goal in Sight?* Letort Papers, Carlisle Barracks: U.S. Army War College Press, 2014.

Gosu, Armand, and Octavian Manea. "The Consequences of the Militarization of Crimea for the Wider Black Sea Region." *Romanian Political Science Review* 15, no. 1 (2015): 9-20.

Grabo, M. Cynthia. *Anticipating Surprise Analysis for Strategic Warning.* Washington, D.C.: Center for Strategic Intelligence Research, 2002 (Originally published as classified volumes between 1972-1974).

Grant, Thomas D. "Annexation of Crimea." *American Journal of International Law* 109, no. 68 (2015): 68-95.

Hagel, Charles. *The Defense Innovation Initiative.* Memorandum, Washington DC: Department of Defense, 2014.

Halper, Stefan, ed. "China: The Three Warfares." Washington, D.C.: For Director, Office of Net Assessment Office of the Secretary of Defense, May 2013.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.

Heurer, Richards J. Jr. *Psychology of Intelligence Analysis.* Center for the Study of Intelligence, Central Intelligence Agency, 1999.

Holsti, Kalevi J. "Theorising the Causes of Order: Hedley Bull's The Anarchical Societ." In *Theorising International Society*, edited by Cornelia Navari, 125-147. Great Britain: Palgrave Macmillan, 2009.

Joint Chiefs of Staff. "The National Military Strategy of the United States of America 2015." June 2015.

"Joint Intelligence." *Joint Publication 2-0.* Washington, D.C.: Joint Chiefs of Staff, October 22, 2013.

"Joint Intelligence Preparation of the Operational Environment." *Joint Publication 2-01.3.* Washington, D.C.: Joint Chiefs of Staff, May 21, 2014.

Kissinger, Henry A. "Military Policy and Defense of the "Grey Areas"." *Foreign Affairs* 33, no. 3 (1955): 416-428.

Larrabee, Stephen F. "Russia, Ukraine, and Central Europe: The Return of Geopolitics." *Journal of International Affairs*, Spring/Summer 2010: 33-52.

Layne, Christopher. "From Preponderance to Offshore Balancing." *International Security* 22, no. 1 (1997): 86-124.

Lund, Michael S. "Conflict Prevention: Theory in Pursuit of Policy and Practice." *Wilson Center.* July 7, 2011. https://www.wilsoncenter.org/publication/conflict-prevention-theory-pursuit-policy-and-practice (accessed December 10, 2015).

Mazarr, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Monograph, Carlisle Barracks: United States Army War College Press, 2015.

Milevski, Lukas. "Strategy Versus Statecraft in Crimea." *Parameters* 44, no. 2 (Summer 2014): 23-33.

Morell, Michael. *Fight Against Islamic State Not Going So Well, Say Former Administration Officials.* January 12, 2016. http://www.armedservices.house.gov/index.cfm/2016/1/fight-against-islamic-state-not-going-so-well-say-former-administration-officials (accessed January 21, 2016).

Obama, Barack. *Remarks of President Barack Obama - State of the Union Address As Delivered.* January 13, 2016. https://www.whitehouse.gov/sotu (accessed January 21, 2016).

Pifer, Steven. *Crisis Between Ukraine and Russia.* Contingency Planning Memorandum No. 3, New York: Council on Foreign Relations Center for Preventive Action, 2009.

Roslycky, Lada L. "Russia's Smart Power in Crimea: Sowing the Seeds of Trust." *Southeast European and Black Sea Studies* 11, no. 3 (September 2011): 299-316.

"S.1356 - National Defense Authorization Act for Fiscal Year 2016, Section 1097." *Congress.Gov.* 11 25, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/1356 (accessed 12 8, 2015).

Sestanovich, Stephan. *Maximalist: America in the World from Truman to Obama.* New York: Alfred A. Knopf, 2014.

Stolberg, Alan G. "Crafting National Interests in the 21st Century." In *U.S. Army War College Guide to National Security Issues Volume II: National Security Policy and Strategy*, edited by J. Boone, Jr. Bartholomees, 13-25. Carlisle Barracks, 2012.

Strauch, Ralph. *Strategic Warning and General War: A Look at the Conceptual Issues.* Rand Note, Santa Monica: Rand Corporation, 1979.

U.S. Army Special Operations Command. *Comprehensive Deterrence.* White Paper, Fort Bragg: U.S. Army Special Operations Command, 2015.

U.S. Special Operations Command. *USSOCOM's Strategic Appreciation.* Internal Document, Tampa: U.S. Special Operations Command, 2015.

United States Army Special Operations Command. *"Little Green Men":a Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014.* ARIS Study, Fort Bragg: The United States Army Special Operations Command, 2015.

US Special Operations Command. *The Gray Zone.* White Paper, Tampa : United States Special Operations Command, 2015.

USASOC. *Counter-Unconventional Warfare.* White Paper, Fort Bragg: U.S. Army Special Operations Command, 2014.

USASOC. *SOF Support to Political Warfare.* White Paper, Fort Bragg: U.S. Army Special Operations Command, 2015.

USASOC, G9. *Redefining the Win.* White Paper, Fort Bragg: United States Special Operations Command, 2015.

USSOCOM. *Operating in the Human Domain.* Operating Concept, Tampa: U.S. Special Operations Command, 2015.

Votel, General Joseph L. "Statement of General Joseph L. Votel before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities." Washington, D.C., March 18, 2015.

Walton, Oliver. "Helpdesk Research Report: Early Warning Indicators of Violent Conflict." *Governance and Social Development Resource Centre.* July 22, 2011. www.gsdrc.org/docs/open/HD777.pdf (accessed November 4, 2015).

White House. "National Security Strategy." February 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

Work, Bob, and General Paul Selva. "Revitalizing Wargaming is Necessary to be Prepared for Future Wars." *War on the Rocks.* 12 8, 2015.

http://warontherocks.com/2015/12/revitalizing-wargaming-is-necessary-to-be-prepared-for-future-wars/ (accessed 12 8, 2015).

Wydra, Doris. "The Crimea Conundrum: The Tug of War Between Russia and Ukraine on the Questions of Autonomy and Self-Determination." *International Journal on Minority & Group Rights* 10, no. 2 (2003): 111-130. International Journal On Minority & Group Rights 10, no. 2: 111-130. International Security & Counter Terrorism Reference Center, EBSCOhost (accessed November 5, 2015).

Please direct any questions to:

USASOC Commander's Initiative Group (CIG)
910-432-8954

or

USASOC Deputy Chief of Staff, G9
910-432-7743