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.

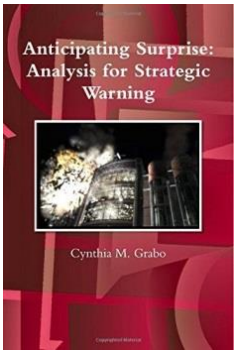
Planes of Perception - "How does surprise happen?"

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]

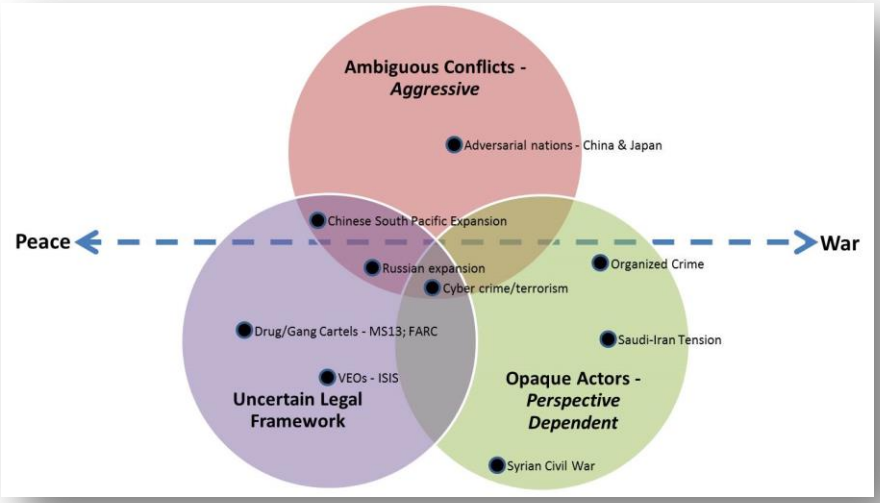


Figure 1 Gray Zone Characteristics

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?

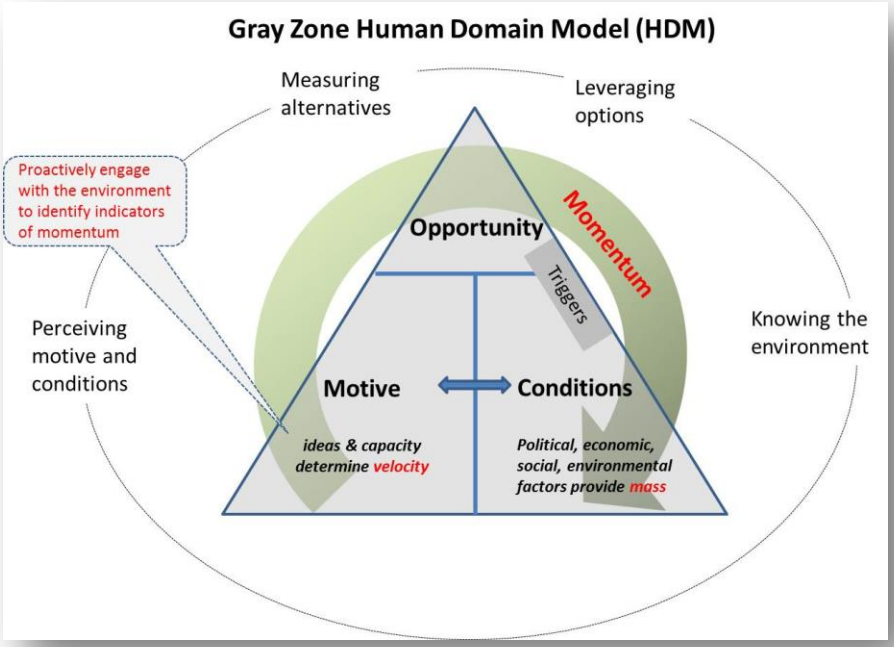


Figure 2 Human Domain Model (HDM)

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