11th Annual Strategic Multi-Layer Assessment (SMA) Conference

Jointly with DHS, DNI/NIC NCTC

"A Utopian or Dystopian Future, or Merely Muddling Through?"

Joint Base Andrews
3-4 April 2018

Prepared by:
NSI, Inc.
Edited by Mr. Weston Aviles
waviles@nsiteam.com

This report represents the views and opinions of the conference participants.

This report does not represent official USG policies or positions.

Table of Contents

Conference Overview

This conference embodied the multidisciplinary nature of the Strategic Multilayer Assessment (SMA) project, by tackling issues both existential and precise, from historical and future-oriented mindsets that are inward and outward looking, and through the analysis of experts that boast a vast portfolio of background and expertise. SMA conferences allow contributors significant bandwidth to contend with the core question of how the USG should think, understand, and plan a path to US prosperity in an environment where uncertainty dominates predictability. Many of this conference's panelists based their subject matter on the fundamental notion that technological innovation is not only changing preconceived notions of national security, but the nature of society itself. Panelists also contended that many of the principles of warfare and human behavior remains the same; thus the vital task is deciphering where, and how, the USG's calculus needs to adapt or to persevere.

The fields of innovation and technology explored in this conference were contextualized by what experts argued is a flawed appraisal of strategic landscapes that do not reflect new and unfamiliar forces. Doctrine and policy leftover from the Cold War have failed in many respects, but shifts in geopolitics are not wholly accountable for these shortcomings. The ubiquity and effectiveness of technology has, perhaps not changed the fundamental nature of conflict, but rather the personality. Many panelists suggest that the strategic landscape now favors the ability to influence allies and adversaries over our ability to implement quick and lethal force; furthermore, the path to such influence must begin with a recalculation in our strategy to reflect this reality. Assessing the importance of influence in the strategy, operations, and internal functions of the DOD must occur across the board from the policy maker, operator, analyst etc.

A theme of concern over the integration of emerging and under-utilized technology and knowledge into our systems, planning, and strategy was expressed throughout the conference spanning USG's functions and theaters of operations. Recognizing the applicability of artificial intelligence (AI) in military applications, or analyzing social media in socio-political movements, or collecting data that reveals technological and cultural divides; is not enough. Quickly and efficiently transforming such advancements into useful tools and more competent strategy must be executed at a system level in order to maintain US superiority. Updating our complex systems, planning processes, and strategy still presents the inherent difficulty that is expected in any information environment; nevertheless, panelists detail notable results from these shifts and advise following the veins of success and learning from failed models and pursuits.

Conference Introduction

COL Senodja Sundiata-Walker (Joint Staff)

COL Sundiata-Walker welcomed conference participants on behalf of the Department of Homeland Security (DHS), the Office of the Director of National Intelligence (ODNI)/National Intelligence Council (NIC), and the National Counterterrorism Center (NCTC) to the 11th Annual SMA Conference. Entitled "A Utopian or Dystopian Future, or Merely Muddling Through?" this conference assessed what we rightly or wrongly perceive as historically unprecedented changes from the perspectives of politics and history, sociology, biology, information science, and technological innovation. There is a large body of scientific work that supports the notion that human societies are complex adaptive systems with emergent properties that contain core commonalities, but the actions of which cannot be predicted with certainty.

Given the properties of human cognition and social behavior, the question remains: how might nations and societies best position themselves to prepare for and manage the risks associated with rapid change under conditions of fundamental uncertainty? Conference speakers and panelists addressed these issues relevant to key domains and dimensions of global security.

Opening Session

Brig Gen Grynkewich (Deputy Director for Global Operations (J39))

Brig Gen Grynkewich (Deputy Director for Global Operations (J39)) participated via video teleconference. While expressing regret for being unable to attend in person, he wanted to set the stage as one of the conference's co-sponsors. He thanked the participants for attending, especially recognizing the attendance of participants from allied and partner nations who are willing to share their unique perceptions and perspectives, as well as their time.

Strategic Multilayer Assessment (SMA) is a joint effort supported by the Office of the Secretary of Defense. (OSD) and the Joint Staff (JS). It focuses on really hard problems that do not lend themselves to simple analysis. This kind of multi-layered assessment typically does not reside within Joint Staff or Combatant Command capabilities, which is why SMA reached out to interagency, academia, think tanks, and industry to provide multidimensional perspectives. This is a lean and mean effort that does not develop million-dollar widgets but provides the Department with a more complex understanding of vital issues.

SMA projects often fall between the seams of authorities, requiring a whole of government approach in alignment with allied and partner sensibilities. Previous projects have run the game of stability in Southern Sudan, security reform in the Palestinian Authority, nuclear deterrence, neurobiology of aggression, and geopolitical analysis.

SMA highlighted the longevity of the Islamic State when everyone thought they were a flash in the pan. SMA taps into and integrates a whole host of different perspectives, audiences, and issues. In the latest space protection study, SMA brought in dozens of representatives from the US private space industry. In addition to different SMA efforts, SMA also hosts hundreds of speaker series events every year that anyone can attend. This kind of effort is great news for the defense enterprise, particularly because SMA lives primarily in the unclassified realm and its findings are available to everyone in the room.

The topic of this year's conference seeks to assess what the US Government (USG) can do in the face of unprecedented historical change. From a historical perspective, it is not clear whether we are in a period of unprecedented change or if we simply perceive it that way. It is a question to be discussed by conference participants. Yet, staying ahead of the change curve will determine what the future is—and whether we muddle through or not.

This conference will help us understand how nations and societies manage this period of unprecedented change. Under the leadership of Secretary Mattis, the Department of Defense (DOD) has framed our response through the National Defense Strategy (NDS). The NDS highlights one major challenge, that is, returning to an era of great power competition and we have to reassess what that means. We often think back to the Cold War, but that may not determine what major power competition will be like in the future. In fact, it is likely to be different. We may be biased to revert to the norm, but great power competition

will increasingly take place to the left of phase zero. What will determine our success is how we posture forces, how we develop technologies to our advantage, and how we develop new forms of deterrence.

The NDS also addresses how we manage global power competition across three lines of effort: increasing lethality, strengthening allies and partners, and increasing efficiency. Increasing lethality does not necessarily mean employing lethal force. It could be a cognitive effect, or possessing that force for deterrent purposes that matter more. However, strengthening alliances and partnerships is key.

Succeeding in an increasingly complex environment requires innovation. While saving taxpayer dollars is important, this is really about making sure we have an engine of efficiency that allows new concepts to emerge. The bureaucracy is not by nature innovative and so we look to the SMA community of interest and the lessons we learn from this conference in particular, as part of the engine of innovation that will help determine which future comes to pass. Perhaps we can have a utopian future if we can adapt and innovate efficiently and effectively; if we do not, we need to start thinking about how to succeed in a period of unprecedented change.

The students who participated in the poster session represent the youngest and brightest minds driving the innovation engine. Brig Gen Grynkewich then encouraged conference participants to make time to view their work.

Dr. Charles Perkins (Principal Deputy, Deputy Assistant Secretary of Defense, Emerging Capability & Prototyping)

Dr. Chuck Perkins stated that while the majority of the DOD thinks a lot about the kinetic aspects of warfare, SMA is one of the few organizations that regularly thinks about the cognitive aspects of warfare. He argued that the DOD needs to focus more on these cognitive aspects and cited our involvement in the South China Sea and Crimea as evidence.

Introduction Panel

Panel Members:
Dr. Allison Astorino-Courtois (NSI)
Dr. Spencer Meredith III (National Defense University)

For the introductory panel, Dr. Allison Astorino-Courtois and Dr. Spencer Meredith III presented a few questions and concepts to consider throughout the duration of the conference. Dr. Meredith began by postulating that all of these new technologies are not "making us anti-social;" as we have behaved similarly for a long time. Dr. Astorino-Courtois proceeded to elaborate on this perception that we are living in a period of unprecedented change and directed her remarks towards how people access information. She explained that is possible to easily identify technologies that have had profound impacts on humanity and society and these inventions change how people interact with one another, who they interact with, and where they interact. She then posed the following questions: Are things really different today? Is this really a period of unprecedented change? She concluded that the rate of technological change has been constantly accelerating, so this current era of rapid technological advancement may not be as unique as we tend to think.

Dr. Meredith began with the notion that we are attempting to ride a tidal wave of information and that what distinguishes our era from others is not the type of information itself, but rather our ability to access information. He then made the assertion that faster processing abilities and accessibility to a near-infinite amount of information has the potential to impact individuals in a negative way as well. He discussed how there has been a gradual loss of taboo as traditions are challenged, lost, and replaced, and that individuals now feel the need to speak in a louder yet narrow fashion—meaning to communicate to those who they agree with and ignore those who they don't. He added that as our brains become so overwhelmed with the ever-increasing volume of information available to us, our capacity to process this information is reduced, and our decision fatigue is magnified. He then went on to discuss the social implications of information overload, including the pushback against cosmopolitan ideas, the fight between localism and globalism in education, and the national security implications. Dr. Meredith concluded by posing the following questions: Although the manipulation of information and perception of reality are not new, what would a world of *persistent* manipulation and engagement look like? If everything is deemed a crisis, how do we prioritize things? Have we entered an information arms race? Do people have control over their own logic? Can information deterrence rely on threats that are credible and discernable? Can we have assassination of character that crosses perception of influence? Could China's unity of thought, unity of rule, unity of action, and unity of society principle become the imperative for states in the future?

To wrap up the panel discussion, Dr. Astorino-Courtois and Dr. Meredith jointly posed the following questions to consider throughout the conference: Is the US at a disadvantage in the information arms race and can we put this genie back into the bottle? Given our democratic identity, if we can't put the genie back into the bottle, can we manage this? Or if we tried, would the effort itself make us more vulnerable? What does all of this mean for liberty and the pursuit of happiness, and for morale?

Panel 1 "War and the Cognitive Capabilities Agenda: Will Humans Continue to Matter More Than Hardware?"

Panel Members:
Moderator: Dr. Allison Astorino-Courtois (NSI)

- Mr. Robert Jones (USSOCOM)
- Dr. Spencer Meredith III (National Defense University)
- Mr. Randy Munch (TRADOC)
- Dr. Robert Toguchi (USASOC)
- COL Scott Thomson (OUSD-P)

This panel explored how US defense strategy is being challenged or outdated by the evolving technological landscape. More specifically, how can the US balance kinetic, technological, and cognitive capabilities in the future security environment and effectively influence governments and populations in the modern, hyper-connected world. Panelists discussed the propensity of the US to win battles but fail strategic objectives, and then offered critiques of the US defense mindset; supplemental to these topics were conjecture on how technology will influence and is influencing warfare.

Mr. Jones began the panel by fundamentally challenging the US approach to and understanding of post-Cold War conflicts; he argued that the US is not a nation at war, not a colonial power, nor is it using a containment strategy, even while acting as if they are. Mr. Jones' central notion was that the US is failing to understand that while nature of warfare hasn't changed, the character of it is changing and our

perception of internal revolutionary conflict embodies this misunderstanding. Mr. Munch continued this line of thought with the contention that the US has consistently engaged in conflict without an effective understanding of the human domain, and American strategy in the Grey Zone exemplifies this. He cited the ability to influence the most influential actors in the operating environment as the key to achieve enduring strategic objectives; but listed the misperceptions that (a) other populations want to behave as the US does, and (b) technical solutions will always be decisive.

COL Thomson agreed with the major points of the other panelists but highlighted that the DOD will be slow to implement a systemic redesign that includes doctrinal and updates to planning processes. These evolutions will be centered around reprioritizing the organization of the Joint Force's capabilities to optimize influencing behavior rather than a near-exclusive focus on lethality, which COL Thomson stresses is the real strategic objective. Dr. Toguchi agreed that the character of warfare is going to change, but emphasized the "new electricity" of artificial intelligence and machine learning and that the USG must anticipate the shift in adversary strategies toward employing a more dynamic application of the cognitive aspects of waging warfare. Dr. Meredith used the example of the PRC (People's Republic of China) "hyperstate" (survival of the state being the supreme prerogative) strategic control of resources and access to resources to maintain domestic control and the hegemony of the CCP (Chinese Communist Party). He contended that the PRC is effectively using information and technology to take advantage of the cognitive domain and implement state imperatives.

Panel 2 "Systems Considerations 101"

Panel Members:
Moderator: Dr. Val Sitterle (Georgia Tech Research Institute)

- Dr. Claudio Cioffi (George Mason University)
- Mr. Vinh Nguyen (ODNI)
- LTC Tom Pike (George Mason University)
- Dr. Gwyneth Sutherlin (Geographic Services)

This panel focused on the complexity of data, systems, and models involved in finding solutions to national security problems. Due to this complexity, analysts and others must wade through multi-layer problems, sifting through tons of data and using complex analytic methods to provide insightful recommendations for decision makers. There was consensus among the panelists that analysts should avoid getting bogged down in the complexity of problems and not lose sight of strategic objectives. In short, it is important to ensure that analysis has an impact on outcomes rather than falling into the trap of doing analysis for its own sake. Panelists also discussed the need to look at problems using a variety of different perspectives, including physics, data science, social science, the intelligence community, and the operational community. This panel sought to address how we handle complexity in analyses through a set of structured questions posed by Dr. Sitterle. Below is a summary of the panel's insights:

What are the most challenging characteristics of complexity in terms of national defense?

- We need to develop the foundations that allow us to understand how to conceptualize the environment to impact the landscape. We can gestate many complex issues, but the question is whether or not it will have the intended impact?

- We must develop the ability to summarize in terms of the outcomes we are trying to achieve. It is important to step back from problem and minimalize it as much as possible (which is not the same as overly simplifying). We should take care to imbue our analyses with complex aspects that we can justify instead of trying to make them complex for the sake of being complex.
- We need to be better at the balancing act of understanding the context of the problem as well as the deadline (or shelf-life) for the analysis. This means efficiently deciphering when the findings must be briefed to still allow for an actionable decision, and how long analysts really have to present those findings to senior leaders. If decision makers require a condensed into 3-minute elevator speech, there is no point in delivering overly complex information; consider the audience.

How do these challenges regarding complexity impact the interpretation of data to answer questions?

- It is easy for people to take analysis and amplify it beyond the intended use—this is wrong—but it is also wrong to underestimate threats. To date, we do not have sufficient analytic tools that estimate the impact of cyber warfare, for example.
- We need to determine how we use cognitive tools for analyses that go beyond the cognitive capabilities of an individual. Perhaps we use too many tools/models, but nevertheless, the one that people use the most is agent-based modeling. We need to go from an us-vs-them mentality to understanding how we can influence the leaders and actors on the other side rather than treating "states" as homogenous entities.
- We need to ask what is the minimal amount of information needed to get to a strategic objective. On the topic of influence, we are not always talking about conflict, so making sure to ask the right questions and finding the questions that will best get us to our strategic objectives is vital.

A lot is spent on R&D efforts to build models based on complex situations where the landscape or situation changes. How do you view the development of analytical tools and the use of analytical tools?

- When you put an interface on top of code a lot can be lost; consider the capability of service members to leverage tools that are being used. Analysts are very smart people with a limited bandwidth. Tell them key variables (minimum information needed) and implications that are at stake. Don't mandate that they must use one tool or another because this a recipe for failure.
- We are dealing with non-stationary, continuously changing systems where there is frequently a mismatch between analytical and system timescales. This complicates what we need out of analysis tools and how long tool development timelines can be. Relatedly, as leaders paint narratives with new, complexity-based perspectives, this will begin to drive a different approach to data collection to support the analytical content and temporal characteristics.
- Many technological solutions designed to solve complex problems leave social science out of the equation. Much of the software development does not recognize the social science theories and assumptions that went into the process; users consequently might be blind to some factors the programs are trying to visualize. We need to bring more social scientists into the analysis.

What kinds of burdens are we placing on our analysts?

- There should be an interdependency between intelligence and tactics. Intelligence should filter down to the operator level and shape their tactics. Too often these two systems are stove-piped

and do not work together. It is important to look at the world as interdependent systems. However, in the cultural context, we always regress to checklists and stovepipes.

- Analysts in other countries do not seem get to get bogged down in complex systems to the point that they lose sight of strategic objectives. Yet in the US, we often spend too much time trying to align systems and tools and do complex things and lose sight of strategic objectives.
- The main challenge is to get analysts out of complexity and working toward an outcome. At the end of the day, we are seeking to translate all of the complex analysis into something that people can carry away and use.

Panel 3 "Global Environmental Systems and Futures: Fragility & Resilience?"

Panel Members:
Moderator: Mr. David Horwitz (USSOCOM)

- Dr. Richard Cincotta (Wilson Center/The Stimson Center)
- Dr. Gwyneth Sutherlin (Geographic Services)
- Dr. Ben Ruddell (Northern Arizona University)

As an introduction to the panel, Mr. Horwitz described the purpose of the discussion as "different pieces of the puzzle" to influence behavior or to prevent or resolve conflict. Water resources allocation in 2012 Afghanistan was used as an example, where integration and fusing of data would have potentially made efforts more effective. Dr. Cincotta then described a model that showed the relationships between age distributions and conflict, stability, and other variables of interest. Countries with a "youth skewing" population tended to be more unstable, whereas countries with an older population demonstrated a higher likelihood of being peaceful democracies. Dr. Cincotta then explained the development window achieve a placative democracy correlates with a decline in fertility and where populations achieve a median age of at least 35, risk of population (or violent regime change) declines. Dr. Cincotta then concluded with the disclaimer that these patterns are less clear for ethnic conflict. Dr. Sutherlin focused on technology and visualization tools that tie together social and physical data. Specifically, drivers of displacement were explored versus population resiliency, by looking at displacement patterns, family group locations, and resource availability. In the example shown, there was significant overlap between family or clan locations and locations of Internally Displaced Person (IDP) camps, indicating a higher potential resiliency. In addressing a follow-up question, Dr. Sutherlin explained that the approach could also be used to monitor changes over time. The final panelist, Dr. Ruddell, discussed how new developments in network theory can be used to map connections relating to a diverse set of topics of interest, including areas such as food, energy, or water systems, transportation, labor, environmental/resource factors, etc. He explained that once these are mapped, it is possible to determine which groups or locations would likely be impacted by different events; however, the challenge in using this tool in many countries is the lack of data.

Further Reading Recommendation:
Dr. Cincotta's suggestion:
Cincotta, R. (2017, June 12). 8 Rules of Political Demography That Help Forecast Tomorrow's World. (link)

Invited Speaker

MG Jim Kraft (USAOC)

USASOC's special operation forces (SOF) enterprise is currently deployed to some 72 countries around the world and consists of about 3,500 personnel, including Civil Affairs, PSYOP, Rangers, Special Ops Aviation Regiment and Green Berets.

USASOC's mission is to man, train, equip, educate, organize, sustain, and support forces to conduct special operations across the full range of military operations and spectrum of conflict in support of Joint Force Commanders and Interagency partners, to meet theater and national objectives. The centerpiece of USASOC's formation has been and will continue to be the operators.

ARSOF provides four Pillars of Army Special Operation Forces (ARSOF) Capability:

- **Indigenous Approach:** The indigenous approach is a means to address challenges to regional stability with and through populations and partner forces empowered by persistent ARSOF engagement. Through the approach, ARSOF leverage nascent capability within populations, transforming indigenous mass into combat power.
- **Precision Targeting:** Precision targeting operations involve direct action and counter-network activities enabled by SOF unique intelligence, targeting processes, and technology, such as ARSOF rotary wing capabilities and armed unmanned aerial systems. Precision targeting operations are employed against uniquely difficult target sets that may require operating in uncertain or hostile environments, careful and focused application of force, and significant intelligence and operational preparation.
- **Understand & Influence:** Developing understanding and wielding influence are essential aspects of the value ARSOF capabilities provide to joint force commanders and the nation. The SOF network of personnel, assets, and international partnerships represents the means to obtain early understanding of emerging local, regional, and transregional threats and where opportunities exist for advancing US objectives.
- **Crisis Response:** Crisis response, provided through CONUS and OCONUS stationed alert forces and persistently deployed and dispersed units, provides national decision makers with agile, tailorable, and rapidly employable special operations formations necessary to respond to emergencies.

Moving Forward: We will harness emerging technologies, capabilities and organizational designs for our advantage. We created 4th Battalions to get a better understanding of environments and give strategic options for our nation. We are doing a lot of work in artificial intelligence and big data, for example, to increase the speed and accuracy of our intelligence processes. We are also starting to use data robots to assess and better select the forces that we want. As part of the joint SOF force, ARSOF will deliver its capabilities to maintain a competitive advantage over our Nation's adversaries.

Question & Answer Session

(*Italics indicates questions from the audience.*)

How does the US as a nation, attempt to either stay apace with or get ahead of that understanding that occurs in certain dynamics?

All of this starts with having a deep understanding which comes from persistent engagement, cultural awareness, and Soldiers who can see, interpret, and explain the dynamics of a particular area.

Looking at the 'by, with, and through' that the Special Operations Forces have done in Syria, and the leadership by influence that they are exposed to with mission command as their enabling idea, how do we bring that back to the broader force so that as we look at force 2035, and the potential of future conflicts, we have mission command as a capability that is not just resident within a select specialized part of the force but more broadly held enabling the broader force?

Our ARCIC (Army Capabilities Integration Center) and TRADOC (Training and Doctrine Command) and our CTCs (Combat Training Centers) are working very closely with our Army to inject that into the scenarios. First and foremost, we have to get reps on this. That is number one. We have to practice and value this. Having said that, we as an Army can absolutely improve on this, but there is something to be said about our accessions process: it is different—it is not good versus bad, it is different. When we throw complexity at our personnel, it is just normal business because that is what they are trained in, day in and day out. I will say that mission command is something that we take extremely seriously. As a matter of fact, even though we look to high technology options, we are actually moving toward alternatives in environments where the higher technology equipment is denied or inappropriate. This illustrates the real business problem we have: how much do you invest in DARPA activity versus gray zone activity. Ultimately, you need a little of both. It has to be replicated in the CTCs.

The joint force recently added information as a joint function. Do you think this is a good idea? How will this change the way in which we operate? Who should be the proponent for it?

I think adding information as a joint function is a great idea. Codifying it and testing and evaluating it is important. We are in a war of ideas and most times we are not going to shoot our way out of any of these gray zone situations. The PSYOP community needs to be a critical actor in that war.

Can you speak about the Interagency and some of the points of friction that you have identified, as well as the successful measures you have taken or seen to overcome that friction to get the information you need?

This is a whole of government business that we are in. Frankly, in most of the 72 countries that I mentioned earlier, we are working for the Ambassador at his/her will. We are familiar with this and familiar with country team interaction. If you look at Syria as an example, it is very generous for the US Agency for International Development (USAID) and Department of State (DOS) to commit a full-time person on my team, and hugely beneficial. All of the various elements of government have to work together because sometimes the military alone does not have all of the necessary tools required for cognitive, virtual, or physical maneuver. We need diplomacy and engagement, and we need to articulate our role depending on what the situation is.

You mentioned the term "information as a weapons system" in terms of a more proactive way of using information. If you had to think about how to train information as a weapons system, how would you go about doing that?

It starts with deep understanding. I have to know what the bad guy is doing. I have to know what he is thinking. I have to know what his campaign is, what his strategy is, and what his ends, ways, and means

are so I can get after him and do a little analysis to start applying our means against it. That is first and foremost, to include getting the requisite authorities and permissions to do so.

Panel 4 "Societal Generational, and Economic Revolutions?"

Panel Members:
Moderator: Collin Agee (Army G2)

- Ms. Regina Joseph (New York University)
- Dr. Cathryn Downes (National Defense University)
- Dr. Anthony Vinci (NGA)
- Dr. James Giordano (Georgetown University Medical Center)

Mr. Agee introduced the panel with reference to Nikola Tesla's 1898 claim that radio controlled devices (analogous to the drones of today) would become so lethal that this technology would precipitate an end to warfare. Reflecting on how that technology failed to induce the change that Tesla predicted—but nevertheless led to a technological revolution—he then introduced the panelists. Ms. Joseph began the panel by delimiting three vectors that shape the "clash" between demography and economy: (1) gender, age, and national composition of domestic and international labor markets; (2) the relative share of the economy that is automated and/or digitized; and (3) the technological habits of the young adult and teenage generations. Dr. Downes detailed the Russian-influence campaign and warned that the US is vulnerable because we cannot distinguish between political campaigns, political warfare, and disinformation. Dr. Vinci then talked about the challenges of making correct inferences from critical historical turning points and lamented that it is easier to resort to the tried, tested, and successful method, and therefore refuse to seek new sources of innovation. He concluded by saying that a decision framework can help shape these change moments to our advantage. Dr. Giordano (filling in for Dr. John Shook) presented an overview of a novel cliodynamic approach to assessing and predicting large-scale generational patterns in socio-political trend activity. Dr. Giordano described how cliodynamic modeling predicted an era of considerable socio-political instability to begin around the year 2020. However, he noted that such predictive speculations must be assessed post-facto for their empirical accuracy and value, and are best considered if and when regarded concurrently with biopsychosocial and politico-economic data.

Further Reading Recommendation:
Ms. Joseph's suggestion:
Harris, K., Kimson, A., & Schwedel, A. (2018, February 7). Labor 2030: The Collision of Demographics, Automation and Inequality. Bain & Company.

Panel 5 "Human Cognition, Artificial intelligence, and Disruptive Neurotechnologies"

Panel Members:
Moderator: Dr. Diane DiEuliis (National Defense University)

- Dr. James Giordano (Georgetown University Medical Center)
- Dr. Nick Wright (University of Birmingham, UK)

- Dr. Jason Spitaletta (Johns Hopkins University Applied Physics Laboratory)
- Dr. William Casebeer (Lockheed Martin)

Panel speakers addressed national security implications and consideration for the convergence of artificial intelligence, deep learning, and disruptive neurotechnologies that could affect human cognition and behavior. Dr. Jason Spitaletta discussed how AI can be a powerful tool for enabling better decision-making at the tactical level, where actions nonetheless can have strategic effects. He emphasized that the DOD has the ethical obligation to service members to protect their long-term well-being while doing what is tactically prudent in the short-term. Dr. Bill Casebeer of Lockheed Martin laid out the moral obligation to build autonomous systems acting as an artificial conscience for service members, but with the caveat of having such systems under their ultimate control. He then discussed why we need such systems, concerns, and rejoinders, and to explore possible architectures. Dr. Nick Wright of the University of Birmingham discussed the intersection of human psychology with AI, providing three examples for illustration. He stressed the need to understand one another in the human decision-making process, emphasizing the role of confidence (e.g., noting how confident each team member is when making estimates). He concluded by noting the critical role of AI moving forward. Finally, Dr. James Giordano discussed emerging neurotechnologies that are being used to remotely sense and engage brain functions sub-serving cognition, emotion and behavior. He noted that the brain is increasingly being viewed as the 21st century battlespace, and described the "3A" approach—to *access, assess, and affect* the brain—as a means to evaluate and influence capability of national security, intelligence and defense operators–and key political and civilian targets alike. Dr. Giordano detailed the market growth of neurotechnology outside of the West, noting that such technologies can be—and are being—used as weapons of mass disruption, which can affect dynamics of power in asymmetrical engagements, and which will necessitate a stance of preparedness to identify, and mitigate specific security threats and risks.

Further Reading Recommendations:

Dr. Spitaletta's suggestions:

M. Reynolds & D. Lyle (Eds) (2013). *Topics for Operational Considerations: Insights from Neurobiology & Neuropsychology on Influence and Extremism—An Operational Perspective*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

D. DiEuliis, W. Casebeer, J. Giordano, N. Wright, & H. Cabayan (Eds) (2014). *White paper on Leveraging Neuroscientific and Neurotechnological (NeuroS&T) Developments with Focus on Influence and Deterrence in a Networked World*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

J. Giordano & D. DiEuliis (Eds) (2015). *White Paper on Social and Cognitive Neuroscience Underpinnings of ISIL Behavior and Implications for Strategic Communication, Messaging, and Influence*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

J. Giordano (Ed) (2016). *White Paper on Assessing and Anticipating Threats to US Security Interests: A Bio-Psycho-Social Science Approach for Understanding the Emergence of and Mitigating Violence and Terrorism*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

J. Spitaletta (Ed) (2016). *Bio-Psycho-Social Applications to Cognitive Engagement*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

M. Yaeger (Ed) (2018). *What do other think and how do we know what they are thinking*? Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

Keynote Speaker

General Joseph Votel (CDR USCENTCOM)

First, I would like to thank Doc Cabayan, Glenn Fogg, and Chuck Perkins who were very kind to me when I was a promotable Colonel assigned to the Pentagon. While there, I found myself dealing with the improvised explosive device (IED) defeat effort. These guys really helped me and introduced me to an area where I had no knowledge. I learned a lot. There was nothing in my military career that prepared me for what I was about to encounter: learning about money, bureaucracy, and the technical threat. These guys helped me a lot and introduced me to a lot of ideas. We were successful because we focused on both technological solutions as well as enhancing force training. I owe a lot to Doc in particular in helping us through that.

We had a lot of crazy ideas—including using swarms of bees for IED detection. While that did not work, it was illustrative of the innovation that went into the effort. Doc was focused on change detection, which was important. Even though this was 15 years ago, Doc continues to push innovation, and I really appreciate that.

While my staff has done a great job preparing a speech for today, I am going to go off script. What I want to do is talk about how we manage complexity in the CENTCOM area of responsibility (AOR). I want to talk about managing risk.

This is an area where SMA really plays a role. It is a key tool that we have come to rely on. Frankly, the work that has been done for CENTCOM for almost two years has really been key to what we are doing. I cannot tell you that any one of the dozens of reports have been a smoking gun, but it has helped fill in gaps in knowledge. SMA provides a granular level of knowledge that we need to fill in those gaps. It is greatly appreciated.

SMA has to continue to push in this regard. We need you to help us think differently about these problems because they are incredibly complex. Our new National Defense Strategy emphasizes great power competition, which is playing out in CENTCOM's AOR in major ways. I talk to the Russians multiple times a day and we have managed despite our political differences to have a fairly professional dialogue over activities, particularly in Syria.

The environment is changing. Information operations and cyber in particular are changing the environment. We see that in CENTCOM and this remains incredibly complicated.

I want to talk with you about how we lead and manage our way through the complexity that we see in this region. I want to talk about key skills that we think are important for our leaders to have. Then I want to talk about the methodology that I use with my commanders. This methodology has been informed by Secretary Mattis. I spent almost two years as his subordinate Joint Task Force commander and observed how he dealt with complexity. I want to share with you the insights on how we look at a complex region.

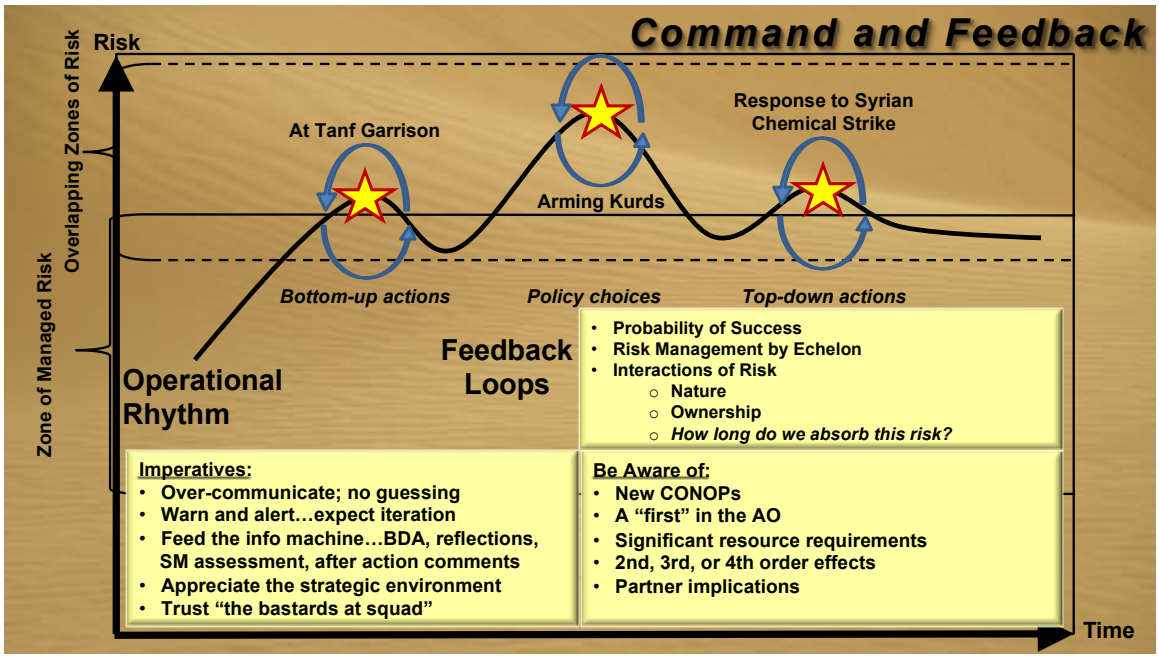
There are three key attributes for leader success: developing relationships, communicating effectively, and providing advice. These are basic things that we have to understand and master in this environment.

First, we have to be a relationship builder. We have to understand relationships. It has to be multilayered. It is not enough for me to have a relationship with my counterpart in Qatar; it has to go down through my Command. But it also means that we have to understand what it is they are telling us and understand things from their perspective. We have to listen first; being a relationship builder is important. Not all of these relationships are going to be positive. We have to work with difficult partners: the Russians for example. I would never characterize the relationship as positive, but it is professional. It requires us to understand their perspectives.

Second, we have to be effective communicators in dealing with complexity. Part of this is being proactive and embracing the idea of over communication. The key aspect that we do not want is people guessing what we are doing. They will get it wrong and it will work against us. We need to make sure people are not guessing and over-communicating is key to this. Part of this is that we have to understand different audiences: Coalition partners, regional actors, etc. And we have to understand how our own leaders receive information so we can best communicate with them. I have learned a lot about how to communicate with the Secretary of Defense. He is a voracious reader who reads everything we give him.

Finally, we have to enhance our ability to give advice. This is really a key attribute. It is the what and the how of providing advice. The "what" part is simpler than the "how." "What" is what you should do and the ramifications of that in terms of risk, resources, and second- (and third-) order effects. More important than that though, is "how." I spend a lot of time reading literature written on the decision to surge forces in 2009. It is an interesting way to understand how we communicate advice to leadership. There have been instances where advice had gotten outside the chain of command and limited options available to the decision-maker, which resulted in a lack of trust. How we provide advice through the chain of command is important. We cannot close the decision space. Advice helps align people between echelons. It is important to align what the low-level commander sees with what I see and what the president sees.

This is the backdrop for the question: How do we manage risk in an environment like CENTCOM that is rapidly changing all the time?



The concept in the slide above is called Command and Feedback, not command and control. We rarely have the ability to control things, so we emphasized the Commander's intent. The Feedback portion was designed to align and inform what is happening as we work through complex situations. The graph is designed to highlight the strategic consequences of risk that rise as you get to higher levels of risk taking over time.

First, what we are trying to do when we manage risk is to increase our chances of success. In the tasks we have been given, risk management does not exist at one level; it exists across multiple echelons. We have to understand the nature of risk we are experiencing. And we have to know how long we are willing to absorb certain levels of risk, particularly in complex regions like the CENTCOM AOR.

I want to build you a picture of risk management. Let us use the Defeat ISIS Campaign as an example of managed risk. The area marked "Zone of Managed Risk" in the slide above represents the space in which my Joint Task Force manager operates. It is determined by the authorities he has, the nature of the operation he is conducting, and maturation operations, as well as time and trust. If I were to draw you a picture of what the box looked like in 2014, it would be narrow. But over time we increased the area over which the commander can operate. Risk management is multi-echelon and overlapping. Then we have overlapping zones of risk (marked in the top third of the chart above). That is where I operate along with the Secretary of Defense and the President.

The idea is that risk management is multi-echelon and does not reside in a particular level. Let me share how we look at that. The squiggly line in the chart is "operational rhythm"—the day-to-day rhythm of activities that take place in a region. This can be driven by the nature of the conflict, time, and cumulative effect of the operation over time. How do we manage that?

Along that curve of operations, we have areas of anticipated and unanticipated risk where things are going to happen. Things we do and do not anticipate represent spikes in the environment. They are caused by a variety of things including bottom up decisions that have impacts at higher levels and higher level decision that have impacts on the bottom, as well as policy choices with implications for the environment.

Using Syria as an example of the impact of bottom up actions, there was an instance where a three star commander declared an exclusion zone around southern Syria. This was within his authority, but the ramifications in terms of defending that meant that we had to shoot down Iranian UAVs, engage with pro-regime forces, and shoot down a Syrian jet that entered the area. Low-level decisions can have ramifications at high levels.

For an example of a top down impact, last year, in response to the Syrian regime's use of chemical weapons, the president struck back within a couple of days. This decision had ramifications down into the organization on how we manage risk. In another example, there was a policy decision to arm the Kurds last summer, which was well debated. That is an example of a policy decision made at a high level that had impacts on the environment.

So how do we deal with that? We do it through feedback loops. This is where SMA really helped us in understanding enough to fill in the gaps of how we are managing risk. It will not solve the problem though. So these feedback loops attempt to get leaders at all levels aligned on particular problems.

There are key imperatives for alignment across leadership echelons. First, you have to over communicate. No guessing is allowed. Knowledge and information is really key. Moving it up and down the chain of command is vital. It puts the premium on warning and alert. I alert the Secretary of Defense to changes in the AOR. Then we expect and iterate about it. We will exchange questions and go back and forth. We will feed him information including battle assessments and after action reports. SMA helps us understand this area much better so we can anticipate what reactions will be.

Trust is really imperative. Army guys have heard this expression: "the bastards at squad" are holding us back. The implication is that we often blame our higher headquarters when things are not going our way. In reality, communication usually fixes this. None of this process works unless there is trust across all echelons of leadership.

We try to pay attention to new concepts of operation, second- and third-order effects, and things that have partner implications. This is how we manage risk in an area like CENTCOM's AOR. We are doing this all the time, every day. It is not just happening in Syria. It is happening everywhere. What it requires is the ability for leaders to establish feedback loops and fill in data as soon as we can so that we can fill in the gaps. SMA helps us fill in those gaps and is very important.

I am asking Doc and his team to continue to work in this area. But I want you to understand how we use it. We use it in this way to increase our chances for success. It is increasing opportunities for success in the mission and the tasks we were assigned.

Question & Answer Session

(*Italics indicates questions from the audience.*)

One of the themes we have been hearing about in the rapidly changing environment is how to deal with surprise. You have a lot of experience dealing with surprise. Do you have a framework for anticipating surprise?

I do not know that you can completely inoculate yourself against surprise. What I think we have to do is to anticipate second- and third-order effects. For example, in the decision to arm the Kurds, it should not have surprised us that the situation would become intolerable to the Turks. We knew that, but we did not

comprehend the nature and depth of it. If we better understand the ramifications and the granular viewpoints, we can better start to predict second- and third-order results. In order to predict where surprise may happen, I am not sure I can articulate a better model than what we have. We have to enhance the sharing of knowledge up and down the Command as soon as we have it to attack the problem from a common standpoint. It is a relatively simple framework, but in practice, it is much more difficult than you can imagine. No one wants to share bad news. No one wants to communicate that things are going out of control, but we have to do so.

Could you talk about how you extend Command and Feedback to working with partners in the area?

There is no magic to this. One challenge we have in working with Coalition partners is sharing information. CENTCOM has representatives from 49 nations that live and work at our headquarters, so we have a leg up. We have developed mechanisms to interact with our Coalition partners to make sure we are sharing information back and forth. In dealing with Syria, we have a core number of nations that really contribute hard military capability to the Coalition. So what we have is a forum to call together my counterparts from 15 nations. We can do a video teleconference (VTC) quickly. We have to have mechanisms in place to communicate. In term of interagency groups, we bring agencies into our headquarters as well. We have to support interactions like that so people across the USG and our partners understand what is happening. This is a structural solution, but none of that works if leaders do not buy in and support it.

I understand that SMA has done a lot of incredible work on ISIS. In terms of complex adaptive thinking, what kind of metric do you use to assess whether a group like ISIS has been defeated? In terms of complex adaptive thinking, what kind of metric could be used to assess that?

I think we have had a lot of success in that particular problem set. We have liberated over 90% of the terrain, and the fight continues against them. We have consolidated our gains, are conducting stability operations, and are conducting follow-on military operations designed to root out the remnants. We lost a couple of Coalition soldiers to ISIS in an area where we had established a level of security. It is a keen reminder that the threat exists out there.

Ultimately, what we want to do is turn over the environment to indigenous partners to handle the security situation on their own. This is easier in Iraq with its recognized army, Ministry of Defense, etc. that we can turn things over to. When we look at the operations they have conducted, they have done 75% without our support. The metric we are looking for is how dependent they are on our support for their security. That is how we know we have reached the end state. This is more difficult in Syria because we are not working with a state but an indigenous force. After we largely end the fight against the physical caliphate and move towards a longer-term security structure in Syria, it will take some time to establish an independent security force. The basic answer is the metric we are looking for is whether our partners can handle the security situation on their own.

Information has just been instituted as the 7th Joint Function. Can you talk about things you have seen changed as the information is integrated in other Joint Functions due to its raised profile?

I really support the integration of information as the 7th Joint Function. This is an important aspect and has been critical to how we have done strategic information operations and messaging. We have got a way to go in implementing this across the government. This is an area where we have to pay attention. The current budget for the State Department's Global Engagement Center is $40-50 million a year. Russia, China, and Iran are spending far more than that. It illustrates the important in which they view information

operations. This should not just be an investment in money, but organizationally as well. Many are aware of the United States Information Agency (USIA), which was a key player in the Cold War. It was used as a way to synchronize and coalesce messages across the USG. The agency no longer exists.

As we look at tactical operations and web operations, I think we have been fairly effective. As we began to deal with the threat in Iraq and Syria, we learned to quickly overtake ISIS with our own capability in the Twitter sphere. We are adept at amplifying messages that we have been authorized to emphasize. For example, recently with our military demonstrations and key leader engagements, we have been able to cause things to happen that we have not been able to do in the past—especially in a compressed period of time. We have used information operations very effectively to buy us physical time and space in a changing environment. I think we are becoming very adept at this. However, I am concerned about how we are applying it at the strategic level.

One panelist today said that in the past 50 years, the US has failed to achieve its strategic objectives. I know you have invested in this personally. We all study campaign design and the end state is important and elusive. What is achievable on your watch at CENTCOM?

What is achievable on my watch is implementing effectively by, with, and through strategy with our partners. As I look at our experience in Iraq and Syria, it is a key lesson learned. It is something we can do immediately. We used this approach in Iraq and Syria when implementing military components of our strategy. I think this is an achievable goal that we can move forward with. We need to develop relationships and provide enabling capabilities to begin to address problems and develop local solutions. At CENTCOM, we have bought into that as our preferred approach. As we went into a recent South Asia strategy review, we asked ourselves why we have not been successful there with hundreds of troops and billions of dollars. The idea of understanding failure analysis is an important aspect. We are not just looking at what has failed, however, we are looking at what has succeeded in other ways. These two efforts described above are achievable and something we can imprint on the region.

Could you speak to the complexity of a multipolar Middle East as we see increasing emergence of great power presence in the region? Could you also talk about the complexity of building a successful partnership?

Excellent questions. This is something I stay awake and worry about at night. In my testimony to Congress, I characterized Russia's role as being both an arsonist and a firefighter. What they do is stoke tensions while positioning themselves to relieve the tensions they have created. It is a dynamic that is difficult to get your head around and to be able to effectively operate around. When we make decisions to get involved in these kinds of things, we have to understand our end state and recognize that we have to be in it and sustain it. The challenge of by, with, and through is that you have to stay with your partners and accept that they will drive the pace on their own timeline. They will make decisions that we would not make, and we have to live with that. It will take longer to bring our partners in, but when we do, they own the problem too, which is important. What we have to understand is what various actors are seeking and what leverage points they have. So looking at Russia, what are they trying to achieve? They want to have access and influence in the region. They have already achieved their objectives, so we have to work our way through this. We have to recognize that it will take time to achieve our objectives.

How will China's One Belt One Road (OBOR) initiative affect your command in the future?

We see Russia and China acting in different ways in the CENTCOM AOR. Russia is focused on influence and reasserting itself in the Soviet model. The Chinese are focused on economic objectives. If you look at the China Pakistan Economic Corridor (CPEC), it literally bisects the country from north to south and connects to the waters of the Middle East. It is significant. My personal view is that CPEC could be positive for the region; however, I do not think the Chinese are pursuing it in that way. Its focus is on not on creating regional stability, jobs, and economic opportunity; it is about economic opportunity for China. They have not reached out to other countries to be part of that and that is a mistake. They are doing something that could create stability but will instead will create instability. We are concerned about that. We have also seen more maritime activity from China. They have major control over ports in Djibouti. These things are all connected. OBOR is not just a dream, it is becoming a reality, so we have to recognize that. There are cultural aspects at play as well. The Chinese do not have a lot in common with Pakistan, but are relying on them to protect them. I think this is ultimately going to have a destabilizing impact, but it could have a more positive impact if pursued in a different way.

You mentioned the significance of relationship building. In Steve Cole's book on Afghanistan, there was a tale and a chronology of limited tours for everyone there. Has that made you change your perception of the value of longer tours in the region?

General Nicholson just started his third year in Afghanistan. It is clear that we emphasize the importance of that particular relationship. Trust is important; we do recognize the importance of that. We do attempt to ensure stability in key positions for as long as we can. That said, after 16-17 years in Afghanistan, we have many people who have rotated through the region and do have relationships. They can come into the environment with those. The fundamental change we are seeing now in Afghanistan is that we now have a national security force that is increasing its competence. It has been in the lead, doing more fighting itself. Our approach can be different now. This is a fundamental difference in how to approach things.

Given all the lessons learned, what investments should we make to increase our influence posture?

We need investments in national strategic information and messaging capabilities. Russia is an extraordinary actor in this area. In many ways, we do not compete. We also need to commit more effort to the gray zone. We want to compete, but we do not want to go to war. We look at actors like Iran, Russia, and China who compete in this environment between normal and peacetime competitions all the time. We have to continue to make investments and look for ways to operate more effectively. We have done lots of work in that area. It is a space that we will be dealing with for a long time. Finally, I am concerned about our ability to detect and deal with rapidly evolving nature of technology that our partners are developing and the pace at which Iran is pursuing ballistic missile capability. Iran's ability to move their missiles and our inability to spot it is concerning. This is an area we have to pay more attention to. We have to pay attention to the capabilities that our competitors have and are developing, and we have to keep pace with it.

Panel 6 "Global Information Systems and Futures: State of the world and where we Are Headed?"

Panel Members:
Moderator: Mr. Matt Chessen (Department of State)

- Mr. James P Farwell (King's College)
- Dr. Laura Steckman (The MITRE Corporation)
- Dr. Spencer Meredith III (National Defense University)
- Dr. Ian McCulloh (Johns Hopkins University Applied Physics Laboratory)

Mr. Matt Chessen structured the panel session around four key questions. The first question was a broad picture analysis of the impact augmented reality will have on the future of the information environment. Mr. Farwell addressed this question, noting that current developments in augmented reality provide a 360-degree immersion into a virtual world which, if harnessed by adversaries would provide an unprecedented ability to fool us, but that could also provide extremely realistic training and planning abilities to our forces before they deploy. The second question concerned the implications of digital tools that are being innovated outside of the US. Dr. Steckman responded by noting that in Africa and Asia, people find that our technology is not suiting their needs and they lack our traditional communications infrastructure. Consequently, they are adapting by going right to contemporary mobile technologies and developing new applications of their own that do not necessarily fit our platforms. The third question was, "how will new tools power and constrain individuals?" Dr. Meredith addressed this question by explaining that new technologies have radically sped up the pace at which social movements begin, develop and end, thereby short-circuiting the normal lifecycles of organizations. This phenomenon is very disruptive since states seek "hyperstate" status through attempts to harness new technologies and grass-root movements respond by seeking to confront those states. Dr. Meredith concluded that we live in a state where, "If anyone can be mobilized, everyone can be mobilized." The final question was, "are soldiers and leadership prepared for new information environment?" Dr. McCulloh answered by asking a rhetorical question, "Could Bill Gates effectively command an infantry division?" The point being that, in reverse, our adversaries militaries' are accomplishing such by effectively moving into the online domain. He noted that the US military is not innovating in this way. He broke down the essential components of innovation into: (1) cognitive diversity, which we do not have among our current military leadership; (2) inclusion of new ideas, which our rank structure hampers; (3) time, of which we do not have enough; and (4) problems to solve, of which we have too many. He noted that our military is structured for efficient command and not for innovation. Dr. McCulloh concluded by stressing the need to invest in strategic education for our leadership, and not in tools to overcome our current obstacles to innovation.

Invited Speaker

Dr. Suzanne Fry (DNI/NIC)

Thank you for inviting the National Intelligence Council (NIC) to be a part of the conversation at this conference. At the NIC, I run the long-range and global issues program, which includes preparation and research of the Global Trends Report. This iteration of the Global Trends Report was released more than a year ago, in January 2017. Since then, the NIC has had a terrific year of supporting the development of the National Security Strategy and the National Defense Strategy, and you can see the tracks of our work in both of those publications as well as in other statements of strategy and doctrine that are emerging across the USG.

What I thought I would do for our conversation today is drill down on the core elements of the strategic landscape and strategic context of the near future that we find to be most useful in terms of organizing the threat picture around us. I am going to leap past a lot of the granularity of what you will find in the report itself, and instead focus on the bare bones of the argument and provide some implications for the threat picture to come.

In *Global Trends Paradox of Progress*, we canvassed and surveyed the key trends and uncertainties shaping the strategic landscape of the near and more distant futures, looking out 5 and 20 years. These trends, we argue (particularly those concerning technology and economics), are converging in a way that is fundamentally changing the strategic landscape. Four key elements emerge. First, it is proliferating and increasing the speed and complexity of the set of issues that are confronting governments. The issue space before government has expanded and will continue to do so. Second, it has expanded the number of geopolitically consequential actors in the international system. We simply do not talk about the P5 anymore. In the same breath that we think about China, Russia, and the US as major powers, we also have our eyes on emerging powers that could be a part of that conversation in the very near future, whether it be India, Turkey, or others throughout the world. The point is that we have many more actors that are geopolitically consequential at the state level. Third, we also have this same phenomenon occurring at the sub-state level with multi-national corporations, terrorist organizations, organized crime organizations, etc., which are, in themselves, geopolitically consequential actors. What we have here is many more actors and types of actors on the international stage. Fourth, the information environment is fractured.

When we put these elements together (the increasing number of issues before governments, many more actors in the international domain, and a fractured information environment), we see right away that we have a fundamental collective action problem. We also have some capacity issues in terms of governments managing this problem. Two familiar qualities will really impend in the near future: the collapsing of the long-term and short-term phenomenon, and the collapsing or increasing inseparability of domestic and international politics. These four effects of this altered strategic landscape are producing a situation where it is much more difficult for governments to govern (i.e., creation of political order within countries is more difficult). Meanwhile, international cooperation, guidelines, and rules that govern relations between states are also coming under pressure because of this proliferation of issues and actors and the fractured information environment. This impedes our ability to get consensus on a way forward. Ultimately, these are the core qualities of the strategic landscape to come.

I want to highlight what this means in the near future, i.e., looking out 5 years geopolitically. We are likely to see—and are living through—increasing tensions within societies. My background is political science

and I worked for the CIA for many years trying to forecast instability events around the world. When I was at the CIA, two-thirds of the planet was my problem. This is no longer the case for my successors that are doing global instability and governance work—the entire planet is now their problem. This is because the increasing challenge of governance is affecting the advanced industrial West. The creation of political order within the US, Europe, and the OECD is becoming increasingly difficult because of trends in populism, reactions to shifts in the global economy, the rise of technology and information in wealth creation, as well as decreasing demands for labor. These trends are putting a lot of political pressure on the governments and societies that we used to think of as being stable. When we look out into the future, increasing tensions within countries is very much an issue for most of the planet. This makes for a fundamentally more complex security picture. We have to think very carefully about the implications of governance changes within the advanced industrial West, and consider what that portends for inter-state relations.

In this context, where we have increasing political and economic pressure on governments in the developed world, we effectively have the West that is starting to turn inward, focusing on tending to issues of a hollowed out middle class and trying to figure out opportunities for wealth creation and employment for these middle classes. This is now occupying most of the political attention of many of the governments of the West. This is creating a strategic opportunity for traditional adversaries, and we are seeing this at the same moment as a resurgence of great power competition. As China and Russia perceive an inward US and West, they are exploiting this moment to assert their geopolitical prerogatives—China and Russia are trying to shape the ways of international politics in a fashion that suits their own particular futures, and they are using the tools of cyber, the tools of space, and other forms of advanced technology, many of which they have gleaned from our own society. Thinking back to a question from earlier about conscription and the implications for being ready for this new geopolitical context, it very much requires a whole-of-society understanding that the strategic competitions of the present and the future are taking place within our universities, corporations, etc. Fundamental questions about citizenship and national accountability really rise to the fore when we think that the key factor in determining advantage in these strategic competitions is technology and innovation. We are waking up to a moment in our post-Cold War reality that the great advances of the West are being exploited by core adversaries, and we have been slow to re-posture. China and Russia are taking advantage of this, but more importantly for the near-term security outlook, regional aggressors are absolutely exploiting this moment. The pressure that we are observing from North Korea, in terms of its desire to become and assert its prerogatives as a nuclear power, is very much a regional contingency that will force major power cooperation or confrontation. There is currently a great deal of concern within my community about the balance of this being more on the confrontation side at the moment.

If in the near future we are seeing rising tensions within societies, which are resulting in an inward West, as well as major power adversaries and regional aggressors trying to exploit these tensions to assert their advantages, then we come to the conclusion that the next 5 years exhibit greater risk of inter-state conflict—hot war conflict—than we have seen at any point since the end of the Cold War. This is ultimately the major headline judgment coming out of the Global Trends Report, and it has been carried through in Director Coats' most recent testimony to Congress about our annual threats. The North Korea contingency, of course, is the most proximate of these concerns.

Terrorism, meanwhile, is not going anywhere. As we cede changes to the conflict in the Levant, we are thinking about the future of terrorism as one that will diversify and expand as those fighters return home or disperse, as they will eventually do. We have seen this movie before. We saw Al Qaeda emerge out of the Mujahedeen of the 1980s-1990s. We saw ISIS emerge out of Al Qaeda and other Sunni extremist

movements. We are expecting similar innovation and emergence to occur. Thus, key questions in the future concern demobilization and reintegration of the people that share the aspirations of those fighters, as well as the fighters themselves.

This context of increasing geopolitical competition is very troubling, particularly for smaller states. It is troubling, obviously, from an American perspective, but it is also troubling for the nations of the post-WWII era that really benefitted from the norms and rules that came to govern that post-1945 period of astonishing and unprecedented wealth creation and geopolitical peace. Smaller states in the international system, whether in Europe or Central Asia or wherever they may be, have, in theory and in terms of international law, been guaranteed their equal sovereign rights to survival as states because of this post-1945 international system. In a reality in which we see ourselves trending toward a world of spheres of influence as major powers assert their prerogatives—particularly within their regions—major powers' tendencies and game plans to run roughshod over smaller states within their regions directly threatens that post-1945 suite of institutions, which served as the foundation for the unprecedented wealth creation that we have all benefitted from. The stakes here are pretty profound, both for small states and for members of the middle class or the advanced industrial West. The ingredients and foundations to that peace and prosperity are very much under challenge.

My colleague last year presented to you the 20-year futures that we provided in the Global Trends Report. In those futures, we presented three key uncertainties. I will highlight them quickly here. It is important to note that these key uncertainties are also policy choices before governments and societies globally. The first key uncertainty shaping the next 20 years is whether global economic integration will continue, or whether or not major players in the international economy will decide that they can do just fine without deepening global trade or economic relations between states. The second key uncertainty shaping the next 20 years concerns whether or not new patterns of international competition and cooperation will emerge to either shore up that post-1945 system, replace that post-1945 system, or something in between. One of the things that we at the NIC are looking very closely at is the nature of the US-China relationship moving forward, and whether or not new guardrails emerge akin to what we saw during the Cold War in terms of guiding Soviet-American relations to include confidence building measures and mechanisms to de-escalate conflict. A key feature of this will be how quick or how long it takes to develop those guardrails and mechanisms. The third key uncertainty shaping the next 20 years concerns the relationship between governments and societies. As societies and publics are becoming more empowered with the great historical wealth creation that is reducing poverty for much of the world while also straining the middle class in the West, we have two very different sets of demands for political participation on governments. Governments are going to have to think about how they govern and what they will provide to their people in a pretty brass tax-accountant kind of way. Fiscal limits are impeding our ability to be responsive to all of the demands that publics are putting forward, so some new arrangement in terms of to whom is owed what is likely to emerge. But this period is going to be very messy. This brings us back to where I started with the near-term forecast of increasing tensions within societies.

As you think about what you have been hearing throughout this conference, particularly discussions regarding anticipating the future of conflict and where we must innovate as warfighters and national security specialists, it is important to have the strategic context in mind. Please argue with it. We at the NIC find that it is more useful to provide a picture that may be incomplete or incorrect or easy to criticize, rather than simply laying a bunch of discrete trends before you and then handing it over to you to make sense of. In short, it is a future of increasing tensions within and between countries, the risk of interstate conflict is greater in the next 5 years than at any point since the end of the Cold War and probably rivals periods during the Cold War, and we have some very important political choices before us.

I will quickly note what we think makes for a situation where governments, organizations, and individuals are likely to thrive in the future. In a nutshell, this would consist of investments in resilience in terms of infrastructure, both physical and human. The importance of education and having the cognitive and intellectual flexibility to be able to respond to the challenges of the future is very much a priority takeaway of our work. Resilience in relationships is also key. Because the scope of issues is so overwhelming, it is impossible for any single organization or government to be able to handle them all alone.

Again, we offer all of this as a bit of a framework or heuristic on which to make sense of the discrete trends and uncertainties that you all are no doubt wrestling with both here at this conference but also in your day jobs.

Question & Answer Session
(*Italics indicates questions from the audience*.)

If I could pull together a couple of thoughts that have been presented throughout the conference. One speaker highlighted the construct of current thinking within the department and offered up some potential solutions that would be game changers. Another speaker raised the issue of our current phasing construct, and whether it is appropriate given that we have near-peer competitors operating online and firing information rounds at us on a daily basis, which creates a disconnect because these competitors are perhaps operating at a phase 2 or phase 3 construct while we would consider it to be phase 0. So, when we think through things like force protection and our FPCON (Force Protection Condition), how does that take in to account our cognitive security from a DOD perspective? DHS has a model that it uses for our terrorism threat levels as well, and there are other tools for warning conditions. How do we take in to account those aspects of information fights that we are in, and when we think through our INFOCON (Information Operations Condition), how do we take in to account the information power pieces to that? Given these current models, how do we modify them, and does it warrant a conversation about creating a new framework or model that is both defensive for our own personnel and offensive for looking at how our adversaries are attacking the cognitive and informational aspects of our society?

Frankly, there are many more experts in the room that can better answer your question about how to modify force posture and our general models for defensive and offensive operations. From a strategic perspective, I think it is important to recognize that our core competitors and adversaries effectively have been at war with the US and its allies for some time. We, collectively, have been oblivious to this. So, the first step forward here is recognition of the strategic competitions that we find ourselves in. There is a whole of society education process that I think would go a long way to backstopping and providing a foundation for what you all are thinking about in terms of force readiness and how our forces should engage with adversaries. That is the first thing: recognizing that our strategic competitors have been at war with us for some time. Truthfully, we have been slow to wake up to this.

The second dimension to recognize is that there are some countervailing tensions here. The State is back. One has to look no further than Russia, China, East Asia, Russia's near abroad, etc. The geography of these conflicts and competitions matter deeply; however, there are some aspects of these competitions that defy geography: namely, cyber and space. Wrapping our heads around those polar tensions would be a good starting point. These are questions that doctrine and force posture must respond to.

Ultimately, many Americans do not recognize that we are in the midst of a strategic competition, and a set of pretty severe competitions at that.

My question concerns the replacement of labor by AI and automation. Forecasts about this have been all over the map. I am wondering, what does this mean for the youth bulge areas of the Middle East, North Africa, Sub-Saharan Africa, and South Asia if there are no entry level jobs and a bifurcated workforce? We saw a million refugees overwhelm the European political system in 2015. Where are your thoughts on replacements for this loss of employment opportunity, and what does it mean from a security perspective?

That is a fantastic question and one that is at the top of our list as we investigate and research the next Global Trends Report. When we traveled to South Asia, particularly India and Bangladesh, we would often meet with leaders of government and industry. We came away from those conversations really quite alarmed at the views and assumptions that countries such as these would have the comparative advantage of an endless supply of cheap labor, and the assumption that this would continue to be a key component of their economic activity and growth for the future. We really did not see a lot of awareness of the impending shocks from automation, robotics, and AI, let alone changes in supply chain issues and things like that. In the near-term, we are likely to see some pretty significant shocks from those technologies in the absence of different policy and business choices about how to structure industry in those societies. Some initial research on India, however, does present some inklings that we are starting to see changes. I am actually anxious to get back to the sub-continent and continue with the interviews to see what people are saying.

You are absolutely right that the forecasts for AI and advanced technology on labor are all over the map. In the near future, in both the developed and developing world, we see that there will be a lagged reaction. The first phase of the impact will probably have a class of workers that get hit and displaced quickly. These workers will probably be unable to recover because they do not have the education, critical thinking skills, or flexibility within their workplaces to retool. So, again, this goes back to how we think about resilience for the future, particularly investing in education capabilities that allow for continued education and learning and encouraging adaptation on the front lines.

To push back on a comment from one of the speakers from the previous discussion, I do not think we have the luxury of picking and choosing to whom we give these educational skills. People are going to get these capabilities, irrespective of their rank within our organizations. So the trick here is how to lead these organizations so that we are swimming with the flow of history and modernity and taking advantage of this native curiosity and dexterity that our young people have with technology, and then channeling this in a way that is constructive. This is where the education piece comes in. But the notion that only some segments of society will have certain skills (while I think that is true at the extreme when talking about fighter pilots and mechanics who work on exquisite forms of technology), for the rest of us who are dealing with the societal and economic implications of technological change, this is overwhelming everyone. So, I think it behooves us to invest in core critical thinking and citizen education. For example, something like being able to know the difference between human generated content and bot generated content online is a really important and teachable thing.

Panel 7 "The Third Offset: Potential Implications of the "New Faces of Terror"

Panel Members:
Moderator: Ms. Gia Harrigan (DHS)

- Dr. Gina Ligon (University of Nebraska Omaha)
- Mr. Paul Scharre (Center for a New American Security)
- Dr. Kathleen M. Carley (Carnegie Mellon University)
- Ms. Rebecca Earnhardt (University of Maryland)
- Dr. James Caverlee (Texas A&M University)
- Dr. Robert McCreight (George Mason University)

This panel discussed new technologies and other form of relevant innovations and their implications for counterterrorism operations and national security. Namely emerging developments in artificial intelligence (AI), robotics, and autonomous systems; and was also framed in the context of the 2014 Defense Innovation Initiative, which included the Third Offset Strategy and contains five core-building blocks:

- Autonomous Deep Learning Systems
- Human-Machine Collaborative Decision Making
- Assisted Human Operations
- Advanced Manned-Unmanned System Operations
- Network-Enable, Semi-Autonomous Weapons Hardened to Operate in a Future Cyber/EW Environment

Looking at the motivations for adopting new technologies, Ms. Earnhardt noted that technology provides an additional asymmetric advantage to terrorists, while greater technological interconnectedness also makes the US more vulnerable. Dr. Ligon discussed the willingness and ability of such groups to innovate within their organizational structure. Referencing the LEADIR (Leadership of the Extreme And Dangerous Innovative Results) data project, which seeks to understand how terrorist groups inspire innovation, she suggests that the leadership style of a terrorist organization influences their ability to innovate. Specifically, leaders who are "power seekers" or "purists" are less innovative. Power seekers because they are more concerned over their own rise than the good of the organization, and purists because they are constrained by ideology. Dr. Carley discussed the use of social media by terrorist groups and contends that "we are in a social media arms race and we don't have effective tools to fight." Terrorist groups are becoming increasingly sophisticated in their manipulation of social media through the use of bots and satire sites, and that as it becomes easier to create and manipulate voice and image this is going to become worse. Looking at technology more broadly, Mr. Scharre argued that evolving technologies have "lowered the bar" for effective use of technology and made individuals more effective. Dr. Caverlee brought together many of the prior participant's observations but focused on ubiquitous platforms and the "Internet of Things" in particular. He explained that all these combine with both the access to software and big computing power, as well as the decreasing level of expertise needed to use evolving technologies, make it increasingly easy for terrorists and VNSAs (Violent Non State Actors) to use technology. Dr. McCreight explained that convergent technologies not only usher in potential a wave of unexpected weapons of mass destruction (WMD) and weapons systems threats, but also present serious strategic challenges—suggesting a 4th offset challenge. He also contended that the amalgamation of advanced

dual-use technologies of the mid-21st century, pose enormous strategic (i.e., 4th offset) challenges to US national and homeland security.

Several of the participants also discussed various approaches to countering this problem. Ms. Earnhardt suggested that understanding the process by which VSNAs become aware of and acquire new technologies, including technology transfers from states to VSNAs is critical to defending against this threat. She referenced a START project that examines technology transfers as a first step in systematically understanding the scope and nature of this issues as well as deriving indicators of impending transfers. Dr. Carley suggests that there are things we can do to combat terrorist groups' use of social media; such as bot competition, forcing platforms to protect themselves, requiring populations to change social media platforms every six months), but noted that they are all difficult to institute effectively. Dr. Caverlee noted that the US needs to invest more in AI and deep learning to retain its competitive advantage and should look for opportunities for partnerships. Dr. McCreight agreed that we need to think more about cooperation with partner nations but suggested that the "silver bullet" to this problem more generally, however, is education.

Further Reading Recommendations:
Dr. Carley's suggestions:
Benigni, M. C., Joseph, K., & Carley, K. M. (2017). Online extremism and the communities that sustain it: Detecting the ISIS supporting community on Twitter. *PLOS ONE*, *12*(12), e0181405.
Kathleen M. Carley, Guido Cervone, Nitin Agarwal, Huan Liu, 2018, "Social Cyber-Security," In Proceedings of the International Conference SBP-BRiMS 2018, Halil Bisgin, Ayaz Hyder, Chris Dancy, and Robert Thomson (Eds.) July 10-13, 2018 Washington DC, Springer.

Dr. McCreight suggestions:
McCreight, R. (2013). Convergent Technologies and Future Strategic Security Threats. *Strategic Studies Quarterly*, *7*(4), 11–19.
McCreight, R. (2014). Brain Brinksmanship: Devising Neuroweapons Looking at Battlespace, Doctrine, and Strategy. *Advances in Neurotechnology: Ethical, Legal, and Social Issues*, 115–132.

Panel 8 "New Strategies for Modeling Complex Interactions in the New Information Environment: A DOD Perspective"

Panel Members:
Moderator: Dr. Elizabeth Bowman (Army Research Lab)

- Dr. Rebecca Goolsby (ONR)
- Dr. Jonathon Pfautz (DARPA)
- Mr. Stephen Jameson (DARPA)
- Dr. Aaron Frank (RAND Corporation)

Dr. Goolsby began the panel by discussing how the development and proliferation of information technology has rendered what were once instruments of power, into the actual environment where power operates. She then articulated several examples of how social media and other forms of mass communication have been instrumental in shaping consequential political movements the world over. In terms of US strategy in the chaotic environment. Dr. Goolsby defined the difference between operational mastery of the environment and the idea of command and control of the information environment. She defined operational mastery as the ability of legitimate authorities to define and deliver their own

narratives and to frustrate and counter attempts to manipulate audiences. Command and control of the information environment, the capability to control all aspects of the information environment, is less feasible given the global social, cultural, and political dynamics that are in play, especially during crisis. Mr. Jameson stressed the complexity and multipolarity of modern operational environments and went on to explain that in such a chaotic landscape, unclear military objectives may lead to failure, despite the highly capable personnel, operational procedures and military doctrine that the US possesses. He noted the inherent challenges in updating systemic planning processes to accurately assess the modern information environment. Mr. Jameson ended by emphasizing the need to focus on building tools to help create information bases; as well as providing information that will allow planners to form their decisions because "the plan is nothing, the planning is everything." Dr. Pfautz continued Mr. Jameson's discussion of DARPA initiatives and shared additional challenges that arise in applying the social and behavioral sciences in operational environments. He highlighted the need to pursue not only basic research, but also to address pragmatic issues. Namely, how to best integrate traditional ISR (Intelligence, Surveillance, and Reconnaissance) with other types of increasingly available data that might provide additional insights into human behavior (e.g., online narratives, social media)—with the ultimate goal of enabling the construction and evaluation of increasingly accurate computational models. Dr. Frank concluded the panel by voicing concern over the processes and posing the questions of how do we make models of social systems better? And how do we make models that are useful for the user? These concerns covered the convergence and divergence of policy and politics, and the lack of efficient and integrative feedback between model design and research and the operation of models. He ended with the two notions: that (1) that the center of human analysis is choice, and we must take a practical standpoint and assume that individual choices matter; and (2) the metaphorical graveyard of failed models can be just as educational as the successful ones.

Further Reading Recommendations:
Dr. Aaron's suggestions:
Joshua M. Epstein and Robert Axtell, Growing Artificial Societies: Social Science from the Bottom-Up, Brookings and MIT Press, 1996.

Robert J. Lempert, Steven W. Popper and Steven C. Bankes, Shaping the Next One-Hundred Years: New Methods for Long-Term Policy Analysis, RAND Corporation, 2003.
Nancy Cartwright and Jeremy Hardie, Evidence-Based Policy: A Practical Guide for Doing It Better, Oxford University Press, 2012.

Panel 9 "The Middle East and North Africa: Dystopian Future in Front of Our Eyes?"

Panel Members:
Moderator: Ms. Patricia DeGennaro (US Army TRADOC G-2)

- Dr. Barnett Koven (Univ. of Maryland/START)
- Dr. Diane Maye (Embry Riddle Aeronautical Univ.)
- Dr. Kay Mereish (DHS)
- Dr. Vera Mironova (Belfer Center, Harvard Kennedy School)

Dr. Mereish began the panel with a reflection on the Westphalian structure that has governed international relations for around 400 years, and its relevancy and application in the Middle East today. She pointed out similarities between the environment preceding the Congress of Vienna and the region

today, and noted that Westphalian structure has not experienced a successful application to the Middle East. Dr. Maye echoed this point and suggested that the dominant paradigm in the region has been the existence of spheres of influence. She explained that such a system persists today in a region where state borders have never been rigid; pointing to the examples of a transnational Kurdish population and the fact that Iraq had long considered Kuwait to be a part of Iraq, despite the latter's independence. Dr. Vera Mironova presenting her findings from a survey conducted in areas in Iraq's Diyala governorate that partially fell under ISIS control. Dr. Mironova found that locals had mixed views on ISIS' activities; and on issues of governance, things were said to have gotten better under ISIS control. Conversely, on economic issues, ISIS was said to have made the situation much worse in every metric measured. Dr. Koven ended by explaining threats to the Westphalian system in the region. He noted a number of these threats, including trans-regional jihadism, massive cross border flows of people and goods, and a degradation of border security. The practical challenge, he noted, was for policymakers to operate in a statist context despite the aforementioned threats to the Westphalian system.

Further Reading Recommendations:
Dr. Koven's suggestions:
Fishman, B. H. (2016). *The Master Plan ISIS, al-Qaeda, and the Jihadi Strategy for Final Victory*.

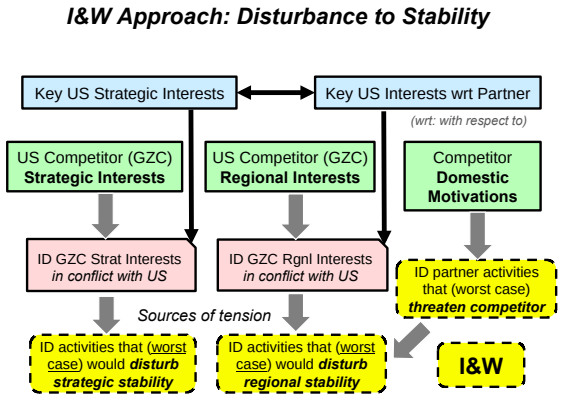
Panel 10 "Operations"

Panel Members:
Moderator: LTC(P) Brad Burris (Joint Staff)

- Lt Gen (ret) Dr. Bob Elder (George Mason University)
- RDML (sel) Joseph DiGuardo (Joint Staff/J-39)
- COL Brandt Deck (USSOCOM)
- COL Eero Keravuori (CENTCOM)

LTC(P) Brad Burris
Every year, the SMA Conference hosts an operations panel to elicit the key concerns, requirements, and thoughts from representatives of the operations community. LTC(P) Burris began this panel by asking the panelists to discuss what the operational community can do with the information challenges and opportunities discussed during the conference.

Lt Gen (ret) Dr. Bob Elder, George Mason University



Many conference participants, including GEN Votel, spoke about the need for deeper analytic thought about the complex issues facing the USG. One way to identify where stability disturbances are likely is to identify for a given area of competition where US global interests, US regional interests, US partner interests, and competitor interests diverge. The approach is depicted in the accompanying figure and uses areas where interests diverge to serve as warnings and indicators of possible disturbances. GEN Votel's notion of Command and Feedback is important because it recognizes that the US military does not get to control our partners' or even other US agencies' actions even though we share the same objective. This means that to synchronize our efforts,

we must establish and agree on clear strategic objectives, collaborate on our operational courses of action, and coordinate our individual (tactical-level) activities as we plan and execute our parallel strategies. One thing SMA can do to support this approach is to help institutionalize the Command and Feedback approach which GEN Votel offered, and leverage his Unified Action approach across the DOD.

RDML(sel) Joseph DiGuardo, Joint Staff/J-39
Investment in strategic communications and investment in the cognitive domain is insufficient to meet our needs. As we look at the current and future operational environment, our technical overmatch is quickly dwindling. One area where we can really exert ourselves is in creatively building weapons, payloads, and platforms that we can use in the competitive space. These tools need to be nuanced and sophisticated to influence adversarial decision-making in the gray zone. These tools must be supported by efforts—like SMA—to achieve near understanding of the cognitive process of our adversaries in any situation. We must understand our adversaries' actions, behaviors, and consequences (ABC's). This understanding is essential for creating messages that resonate deeply with our target audience. Big data, machine learning, and other technological innovations will help us harness the information, patterns, and knowledge we need to understand, influence, and operate in competitive environments.

COL Brandt Deck, USSOCOM
There has been a lot of talk about sustained great power competition as outlined in the National Defense Strategy. While we must prepare ourselves to win in the competition space—not just compete better, but win—we also have to be prepared if we cannot win. How do we win? First, we need to demand more of our senior leaders, particularly our elected and appointed leaders. We need a clearer annunciation of strategic objectives for each of our competitors and partners. We must also be more effective. SOCOM tends to talk about getting to the desired state not the desired *end* state. An end state implies permanence and sustainability, but a desired state can be a range of options. Second, we need to understand and become masters of the human cognition domain. A majority of our forces are so entangled with lethality that we have to refocus on how to conduct influence operations. The human domain is in the cognitive space. This is not just a SOF problem; the entire Joint Force has to operate there. The creation of the 7th joint warfighting function, Information, is a positive step, but there is no Joint publication to clearly articulate what it encompasses and how we use it. To be better operators within the human domain, we need to do more thinking, writing, and education over this new warfighting domain.

COL Eero Keravuori, CENTCOM
SMA helps to bring understanding and awareness of divergent views to CENTCOM. Understanding these alternative perspectives helps senior leaders accept higher levels of acceptable risk. There is a difference between risk by ignorance and risk by information in decision-making. SMA helps with that calculation. One thing CENTCOM struggles with is determining attribution. Our competitors are looking for influence, not blame. However, in the CENTCOM AOR, we have to work with our competitors. We do not have to be friends with our partners, but we must exploit common interests—even temporary ones—to advance our objectives. Our "by, with, and through" efforts are not targeted at winning local populations over, but at helping our local partners win their population over. Once we make gains in difficult environments, we must consolidate them by excelling in the human and cognitive domain, which often requires efforts to enhance partner legitimacy. Conveying messages effectively requires that we have deep knowledge of our audience, anticipate counter arguments, and have a way to respond quickly. We have to build relationships, not tear them down. SMA helps with these problem sets by advising up. It gives decision makers the ability to anticipate how key stakeholders, whether friendly, difficult, or competitive, might behave. SMA also helps the commander to share information concerns and contributions down to other commanders and across to partners.

Further Reading Recommendations:
Lt Gen (ret) Dr. Elder's suggestion:
Corrin, B. A., & Aug 19, 2009. "Command and control must become command and feedback, says NATO commander.

COL Deck's suggestion:
The Joint Staff. (2016, October 19). Joint Concept for Human Aspects of Military Operations. NSI Inc.

Panel 11 "Continuities and Discontinuities Within and Between Generations: Millennial Perspectives on Information, Technology and People Power"

Panel Members:
Moderator: Dr. John Stevenson (NSI)

- Ms. Nicole Peterson (NSI)
- Ms. Michaela Braun (Monterey Institute of International Studies)
- Ms. Clara Braun (Univ. of Nebraska-Omaha)
- Mr. Weston Aviles (NSI)

Dr. Stevenson introduced the panel by defining the term millennial, and called attention to four millennial characteristics: (1) status as digital natives, (2) participation in protest movements, (3) habits as related to accessing information, and (4) communitarian value set. Dr. Stevenson used both his introduction and the entirety of the conference as a base for the panelists (all of whom are millennials) to reflect upon. Ms. Peterson offered her thoughts on the integration of technology into the lives of millennials and noted that one of the core competencies of extremist groups today is the ability to use technology to appeal to younger people. She also stressed the need for US government officials to be familiarized with these modern technologies in order to more effectively combat extremist groups. Ms. Michaela Braun followed by highlighting her research in West Africa, where she focused on female suicide bombers. She noted the distinction between child terrorists, who often come from a family structure in which an ideology is taught, and child soldiers, who have their families wiped out, and replaced with a unit. Following her was Ms. Clara Braun followed and presented her work on the digital lifestyles of homegrown violent extremists in the United States. She emphasized that millennials are more likely to create original content on behalf of violent extremist organizations, assisting in the groups' resiliency to dissolution and fragmentation. Mr. Aviles concluded the panel by criticizing the millennial generation and discussing social media as an addictive activity. He explained the millennial propensity to subscribe to polarized social movements that are antithetical to free and open debate and also argued that while millennials have access to unprecedented levels of information and communication, they remain alarmingly secluded to ideological ignorance.

List of Acronyms

AI	Artificial Intelligence
ARCIC	Army Capabilities Integration Center
ARSOF	Army Special Operations Forces
CCP	Chinese Communist Party
CONUS	The 48 Contiguous States and the District of Columbia
CTC	Combat Training Center
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOS	Department of State
FPCON	Force Protection Condition
IDP	Internally Displaced Person
INFOCON	Information Operations Condition
ISR	Intelligence, Surveillance, and Reconnaissance
NCTC	National Counterterrorism Center
NDS	National Defense Strategy
NDU	National Defense University
NGA	National Geospatial Agency
NIC	National Intelligence Council
NSI	National Security Innovations Inc
OCONUS	Outside Continental United States
ODNI	Office of the Director of National Intelligence
OECD	Organization for Economic Cooperation and Development
ONR	Office of Naval Research
OSD	Office of the Secretary of Defense
OUSD-P	Office of the Under Secretary of Defense, Policy
PRC	People's Republic of China
PSYOP	Psychological Operations
SMA	Strategic Multilayer Assessment
SOF	Special Operation Forces
TRADOC	Training & Doctrine Command (US Army)
USAID	United States Agency for International Development
USASOC	United States Army Special Operations Command
USG	US Government
USCENTCOM	United States Central Command
USSOCOM	United States Special Operations Command
VNSAs	Violent Non State Actors
VNSAs	Violent Non State Actors