8th Annual Strategic Multi-Layer Assessment (SMA) Conference

28-29 October 2014

A New Information Paradigm? From Genes to "Big Data" and Instagram to Persistent Surveillance…Implications for National Security

Joint Base Andrews

Prepared by
NSI
Sarah Canna & George Popp
scanna@nsiteam.com
301.466.2265

This report represents the views and opinions of the conference participants. The report does not represent official USG policy or position.

Table of Contents

Executive Summary

We live in an age characterized by the reshaping of society through the presence of information and networks. The proliferation of information technologies from the micro and instantaneous to the insights hidden in "big data" has generated a range of new issues with implications for global transformation and political power shifts, patterns of conflict and warfare, and potential opportunities for enhancing global stability. The time is right for a thorough consideration of the implications of this "age" on US national security issues. How can we best understand the near-term and long-term consequences of these changes? What adaptations to our current intellectual frameworks, intelligence processes, organizational structures, command and control practices and planning approaches may be necessary? In short, how can the United States Government (USG) and its allies recognize the risks as well as the opportunities for enhanced global security presented by fuller realization of the "information age"?

The intent of the Conference was to examine the implications of the information/network age. What are its key dynamics? What impact do these dynamics have on national security-related topics? And, what changes in USG modes of planning, operation, policy development, and military capabilities are needed to mitigate information age risks while simultaneously recognizing and seizing opportunities?

The 2014 Strategic Multilayer Assessment (SMA)[1] Conference focused on these opportunities and challenges from various perspectives and disciplines including neuroscience, behavioral and social sciences, and operational strategy. Emphasis was placed on the need to interweave these various disciplines and perspectives.

As in previous years, the conference sought to address the needs of the Geographical Commands. Representatives from the Commands discussed their pressing needs and key operational requirements. SMA's wide network of experts as well as conference participants assisted in identifying and discussing capabilities that could match these needs.

Opening Session

CAPT Todd Veazie, NCTC, opened the conference. He stated that SMA's objective is to provide deep contextual orientation and decision quality assessment to warfighting commanders on intractable problems. Brig. Gen. David Béen, JS/J-39, added that SMA's multi-disciplinary, multi-agency approach does not exist

[1] Strategic Multi-Layer Assessment (SMA) provides planning support to Commands with complex operational imperatives requiring multi-agency, multi-disciplinary solutions that are NOT within core Service/Agency competency. Solutions and participants are sought across USG and beyond. SMA is accepted and synchronized by Joint Staff/J-39 DDGO and executed by ASD (EC&P).

anywhere else in the Department of Defense (DoD). We are living in challenging times, and we need multidisciplinary expertise from across industry, academia, think tanks, and others.

Mr. Ben Riley, PD DASD (EC&P), then questioned whether we are in a different or unique era compared to any other time in history. The Naval Postgraduate School (NPS) studied this question and determined that today is similar to the pre-World War I era in terms of a recent revolution (industrial and information respectively), rise of great powers, struggle of traditional nation states, and global communications advances. He emphasized that it is critical that we understand that global events arise from previous conflict, conditions, and events.

Keynote Speaker: LTG Ed Cardon, US ARMY Cyber Command

LTG Cardon stated that he believes we are in a new global paradigm brought about by the information/technical revolution. Due to this, threats and vulnerabilities are increasing, often in highly complex ways. The US military is dominant in the operational environment, but is losing strategically because we struggle in the information environment. We are in a political struggle and cyber operations are key to success in this area. Cyber operations could be used in all phases of conflict, but particularly in phase 0 and phase 1. He hoped that organizations like SMA could help bridge the gap between the operational and information environments.

Keynote Speaker: Admiral Michael Rogers, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service

ADM Rogers stated that in the digital age, the DoD has to be an agile organization that is capable of quickly building communities of interest in response to wide-ranging, unanticipated crises (such as Ebola). Big data provide new opportunities to distill critical information from the noise to generate insight and knowledge. However, in order to harness the power of information, we have to create partnerships with individuals and organizations we have never worked with before from the private sector, industry, academia, NGOs, think tanks, individuals, and others. That is why the tools and methodologies developed by the SMA community are so important.

Panels

Panel One examined complexity, interdependence, and emergence in an interconnected information age. The demographic/age change we are experiencing is the central issue facing the United States today because of newly emerging threats and opportunities that are arising and will continue to do so. It is essential to understand the nature and character as well as the dynamics of the information age. There is an incredible amount of data constantly being collected in the world today because of the information boom, but the ultimate challenge is figuring out how to make sense of the signal in all of that noise to help better understand the emerging

threats and opportunities. The world today consists of a very complex and uncertain environment characterized through interconnectedness and increased competition over resources. Thus, it is time to shift our focus beyond predictability and instead focus more on sense making. We are overwhelmed with data and we need new tools and methodologies to use this data to make sense of an uncertain environment. The United States must start focusing on opportunities to shape the rapidly changing environment and ultimately become more strategic and adaptive in its planning. With the world today being in an age of transition, from the past we learn that the most important factor in determining the success or failure of world systems during times of transition is the system's willingness or resistance to accept change. However, in reality, today we are rather conservative and overall resistant to change.

Panel Two discussed the information age, networks, and national security. In this new information age, which is defined by huge amounts of data, an abundance of information does not equal power. Instead, power is the ability to use information to define reality. Thus, communication plays a central role power. Using communication to define reality requires creative thinking—something that the intelligence community (IC) struggles with. Historically, the IC has been strong when it comes to critical thinking, but the IC and the US government as a whole often struggle when it comes to creative thinking. When trying to use information to define reality it is important to remember that different cultures use social media differently. If we are going to analyze social media, we must also understand how people in different parts of the world use and understand social media.

Panel Three explored patterns of conflict and warfare in the information age. Information technologies are changing the character of warfare due to advancements in networking, robotics, command and control, etc. This panel also explored how potential US adversaries might employ information technology to create narratives that develop sympathy for their cause and hinder US involvement and decision-making during a crisis. The panel found that the information age has made the world more transparent, which consequently makes the world more lethal for US forces. The panel also concluded that the information age has made political warfare (phase 0) more relevant. Russia and China are both engaged in political warfare with the United States.

Panel Four asked representatives from the Joint Staff and Commanders to discuss how the information revolution is shaping their worlds. They found a correlation of information environment to the national security environment. The same freedoms the USG seeks to protect are being used in an agile manner by adversaries and potential adversaries to US disadvantage. Information is a combat multiplier but we are moving into an age where user-generated content allows adversaries the ability to employ the ever-growing list of social media that nation-states cannot match. How do we account for this trend? The panel found that when the USG tries to do information operations, it is sprinkled into the operational plan at the very end. It has to be baked in from the beginning to be effective. Additionally, panel members

found that the answers to many of the challenges we face are hidden in the data and are only seen in hindsight. We need to move the identification of key factors closer to the decision-making calculus. Finally, panel members encouraged the DoD to find creative methods to better share information with partners and allies to achieve common objectives.

Panel Five discussed the intersections of big data, neuroscience, and national security. Big data helps allow for neuroscience insights to become operational. Linking big data to neuroscience is crucial in allowing for the use of neuroscience to provide utility in an operational environment. However, while significant advances are being made in the field of neuroscience (specifically in terms of big data collection), significant technology gaps exist. Furthermore, when operationalizing neuroscience it is important to realize there are a number of ethical and legal issues.

Panel Six examined how to understand social systems in phase 0 through human geography, big data, micro information, and the reconnaissance, surveillance, intelligence (RSI) paradigm. When analyzing a problem, it is crucial to begin by defining the purpose, perspective, and process to make the best use of available information and have effective intelligence. The distinction between what problem you are trying to solve and why it is important to you drives what kind of intelligence is needed, why it is needed, and who needs it. While data can come in various forms and provide important insights into factors like location, place, region, movement, and human-environment interaction, to actually make use of the data, it is essential that the problem set is well defined in the beginning. Data can come in many different ways, but it is important that something like metadata, leveraged crowd sourced verification, etc. is provided along with the data to illustrate trustworthiness confidence levels, etc. Furthermore, in addition to understanding confidence levels, it is important to understand that very good data can sometimes be at a scale that is inappropriate for a given analysis and if this is the case the data may not be applicable.

Panel Seven explored the implications for US influence and deterrence capability of the nearly instantaneous availability of both large and micro data. The panel used the example of attempts to deter Islamic State of Iraq and the Levant (ISIL) activities to begin its discussion of the impact of immediate, global communications on the effectiveness of US deterrence messages. The panel suggested that a strategic imperative for the US is to make sure that our messages, whether kinetic or informational, do not embolden or inadvertently strengthen potential adversaries. Although some argue that we need to respond quickly to opportunities to discredit or challenge adversary narratives, the USG has extremely limited capacity to change the worldviews of people in different culture and environments. There is some academic research and analysis describing countering specific adversary messages as a means of deterring unfavorable behaviors but very little that supports the notion of changing basic narratives. These research efforts need to be better operationalized for the DoD community. Furthermore, US words and deeds must be synchronized, as they are both forms of communication.

Panel Eight discussed what is in store for the Pacific Region and specifically U.S.-China relations amidst the information revolution. Over half of the world's population resides in USPACOM's area of responsibility (AOR), which consists of 36 nations and offers a number of unique characteristics and challenges. As two global superpowers, the U.S.-China relationship will shape the Pacific Region going forward. In order to build trust and improve security within the U.S.-China relationship and throughout the Pacific Region overall amidst the ongoing information revolution, we must understand and improve connectivity, communication/language, cultural understanding, confidence/confidentiality, collaboration, coordination, and cooperation. The information revolution has provided us with new methods of communication as well as the ability to better assess our effectiveness in our relationship with China. For the first time, we have the opportunity to fully understand communications with China. The next step will be to use communication as a means to deter and drive a specific outcome. China and the U.S. diverge on some aspects of the Internet including desired regulation levels and hacking and cyber-crime concerns and activities, all of which will influence the U.S.-China relationship going forward.

Panel Nine asked representatives from the Commands to discuss what they have learned at the conference, what they will be taking back from the conference, and where they anticipate needing further assistance. One takeaway was that the USG is not clearly messaging its own narrative. We need to focus on strengthening our own narrative in the information age. A second takeaway was the main targets of insight of many discussions were political officials. If these topics are not raised to these decision makers, we risk talking to ourselves. A third takeaway was that the information revolution is unlike other revolutions that were based on breakthrough inventions; the IT revolution continues to advance and expand. The thing we must manage is not the technology itself, but rather the evolution of that technology. A fourth takeaway is that operating in this new world requires building partnership and communities with unconventional partners within and outside of the USG. But progress in this area is impeded by an overly burdensome classification system. Finally, open source information is underutilized, particularly as non-kinetic (political) warfare become more prominent.

Introduction: CAPT Todd Veazie, NCTC

CAPT Veazie welcomed the participants. He noted that this was the 8th annual SMA Conference. Anything that has lasted eight years in Washington is a significant achievement. SMA draws a vibrant community and the brightest minds.

Eight years ago, CAPT Veazie and Dr. Hriar Cabayan planned the first annual SMA conference. SMA's objective was to provide deep contextual orientation and decision quality assessment to warfighting commanders on intractable problems—problems they could not solve with organizational assets and human capacity within their direct control. There was no single agency to turn to for these kinds of analytic

capabilities. They turned to SMA, which reached out to the community to put the best minds against the toughest challenges. SMA is multi-disciplinary—it relies on no single method to provide the right answer. It is both multi-layered and multi-agency. SMA's success can be measured in the quality and number of products transitioned and adapted to action by the combatant commanders. By this metric, SMA has a storied record of success and added value.

He noted that the conference attendees were all here for love of country. As we navigate the shoal waters of national security, we often need help—especially from those who attended the conference. He thanked participants for their sense of patriotism and for volunteering to help. Everyone attending the conference is part of Dr. Cabayan's network, who has been an inspiration and mentor to CAPT Veazie for 10 years. SMA lives because of his incredible energy.

Opening Session

Brig. Gen. David Béen, Deputy Director, Global Operations (J-39)

Brig. Gen. Béen welcomed the conference attendees. He recognized the hard work of the SMA staff in putting together this conference as well as Mr. Ben Riley's team at AT&L, which is responsible for synchronizing efforts from combatant commands. Right now, SMA has efforts in PACOM, AFRICOM, SOCCENT, and USSC.

The 8th Annual SMA Conference has brought together the brightest minds to discuss the new information paradigm and its implications for national security, which is extremely relevant to the Joint Staff and the COCOMs.

This has been particularly relevant with the emergence of the so-called Islamic State of Iraq and the Levant. How did the USG get caught so off guard? What makes the group so appealing to foreign fighters? In another part of the world, Vladimir Putin put on an information operations clinic last spring by annexing Crimea without firing a shot.

These are definitely challenging times. The Department of Defense (DoD) and the USG need the expertise from think tanks, academia, private industry, inter-agency, etc. SMA was established to bring to bear such a multi-agency, multi-disciplinary approach—one that does not exist in any one service.

Brig. Gen. Béen asked the participants to engage in an open dialogue, ask pressing questions, and propose innovative solutions. What the group accomplishes over the next two days, and in coming months, will most likely be relevant for planners in the field and their senior leaders.

Mr. Ben Riley (PD DASD (EC&P))

Mr. Riley noted that ten years ago, we were talking about theories regarding the insurgency in Iraq. CAPT Veazie said that all these people wanted was a job, a

girlfriend, and a place to live. That holds true today. When we started this conference eight years ago, a new "information paradigm" was not on anyone's tongue. Neither was ISIL, USSC, or the term "megacity." There was no such thing as AFRICOM. It is representative of the velocity of change in the world.

Last year, he asked his staff a question, "Is the current era different than any other time?" The Naval Postgraduate School concluded that yes, it is similar to a previous era: pre-World War I. NPS scholars referenced the start of the industrial age, the rise of great powers, the struggle of traditional nation-states, global communications advances, the introduction of the steam age, and the advent of aircraft wireless communication and battleships. Often, historical studies tell us what happened, but not necessarily why. If you replace the industrial age with the information age, we are in for quite a ride the next 100 years. The rate of change is very high; we are not sure we can keep up with it. The information age will drive us to places we cannot currently imagine.

A book written by John Arquilla and John Ronfeldt (1997) called "In Athena's Camp: Preparing for Conflict in the Information Age"[2] is prescient.

> *"Look Around. No 'good old-fashioned war' is in sight…For most of the world, the daily reality remains otherwise. Irregular conflicts abound….Bands of Chechen ethno-nationalists, organized more like clans than corps, have repelled the clanking Cold War-era Russian army in bitter murderous fighting; Hamas terrorists, disdainful of [PLO] leaders continue to hit Israeli targets….Criminal networks…become the covert arms of states aiming to pursue "strategic crime and criminal mercantilism….The world is entering – indeed it has already entered – a new epoch of conflict (and crime). This epoch will be defined not so much by whether there is more or less conflict than before, but by new dynamics and attributes of conflict."*

Conflict in the information age is extremely complex and difficult to understand. SMA tries to make sense of it by bringing together many perspectives.

As a community, we tend to study these groups as separate entities and not include global events that drive them. ISIL did not come out of nowhere. It represents a struggle within the global Muslim community. We need to understand the push and pull of factors. In 15 years, we may have another phenomena like ISIL—perhaps in Africa. Boko Haram is the latest development there, but Nigeria has a long history that drove the problem. He encouraged the participants to take a global overlay, strategic look at where these sources of conflict emerge from and how they drive phenomena.

[2] "in Athena's Camp. Preparing for Conflict in the Information Age," John Arquilla & John Ronfeldt, RAND, 1997, pp 1-3

Key Note Speaker: LTG Ed Cardon, US ARMY Cyber Command

LTG Cardon stated that he has been looking forward to this conference. He is leading Army Cyber Command, but he is not a cyber person. In fact, he was surprised to be selected to run Army Cyber Command. He was selected to operationalize the space: organize, train, and equip the Army to take advantage of the cyberspace domain's opportunities. He spends a lot of time thinking about information and how to use information to gain a competitive advantage in cyberspace. We are in a new paradigm. LTG Cardon stated, "We are in the middle of an information technology revolution driven by cloud technology, data analytics, big data, wireless and mobile technologies, and advanced computing."

LTG Cardon visited Google recently and asked them what the computing environment would be like in three years. They were unable to answer because the speed of change in technology makes it impossible to project that far ahead.

Often, when he talks about the cyberspace environment (threats, vulnerabilities, and complexity are all increasing), he describes it as a math problem. "If you have 2^{1000} and add one more zero, that is not linear change; it is exponential."

Think about what happens on the Internet in one minute: 639,000 gigabytes of data transfers, 277,000 Facebook logins, 6 million views, 30 hours of video uploaded, etc. Those figures are global. The United States is a relatively small actor in this space.

If one look at the information component of DIME,[3] LTG Cardon would argue that the USG is dominant on the ground but is losing strategically because it struggles with the information environment. Look at Joint doctrine. It describes the operational environment. The USG dominates the operational environment and can adapt rapidly. But the USG struggles in the information environment.

He noted, "Perhaps we are looking at the information environment the wrong way. The USG is in a political struggle. It needs operations to support political narratives. This viewpoint changes how we assess things, how we measure how well we are doing. Measuring the number of patrols is meaningless. What has more meaning are the phone numbers and names collected during patrols or knowing how individuals or units changed the environment while they were out. If you have that information, then you start gaining energy."

Information operations have changed due to social media. The USG is struggling to understand information operations and information warfare. The DoD has electronic warfare capabilities down to the individual soldier. The implications of this are enormous.

[3] DIME stands for Diplomatic, Information, Military, Economic

LTG Cardon noted, "We can more easily describe land, sea, and air power than information or cyber power. How can the USG really adapt to this new world? For example, the traditional way of looking at a map shows you streets, intersections, buildings, etc. In the information age, we need to transform that. Instead of a street, we will have communication pathways of some kind. Every intersection is built around a switch. A building is a device. We would have to figure out how to start at one end of the city and navigate to the other side. Soon, you begin to realize that all US doctrine that talks about movement absolutely applies. The same principles of maneuver, firepower, and protection apply. You need intelligence to maneuver in cyberspace as well."

LTG Cardon stated that his biggest challenge is trying to determine what commanders need from a cyber perspective. "In our current model of cyberspace, there is a geographic layer, a logic layer (networks), and a persona layer. The challenge is that the logic layer has no boundaries. Information may start in a red space, go through grey, and end up in blue. It goes through layers and tiers (national to local). Think of the way we divide the world in the DoD. We have geographical boundaries in the other domains, and we struggle with boundaries in cyberspace just within the US—between DoD, State, Commerce, DHS, etc., for example. Then we have legal authority boundaries and presidential directives. Cyberspace has no boundaries. Cyber adversaries using social media across cyberspace do not ask for passports or visas."

It is not clear if we can operate at the speed of cyber in cyberspace. We have multiple countries, combatant commands, authorities, and the public and private sector that we have to coordinate with. Does this give us the speed we need to operate in the information age?

Cyber Command faces many challenges. For example, some would like us to do something about ISIL's [Islamic State of Iraq and the Levant] use of social media. However, the minute people in the United States become involved, a different set of rules kicks in. We are bound by the rule of law and our own fundamental beliefs about privacy and freedom of speech. How are we authorized to operate in the current environment? Cyber operations have been neglected because it was born out of the communications and sensor world, before the globalization of the Internet."

LTG Cardon stated that he hopes to provide clarity on what cyberspace operations are. "Cyberspace operations allow commanders to conduct activities in phase 0 and phase 1: de-escalate, prevent, and shape without creating lethal effects. Cyber can also be used to augment all phases of operations to achieve military effects."

Big data is going to give the USG incredible capability. But the DoD has to figure out how to leverage it. It can be used to leverage efficiencies, identify predictive patterns, etc., but it is so much bigger than that. In the private sector, people are using data in ways we have not even thought of yet. But it creates big problems.

How do we govern algorithms? The human side (neuroscience) is absolutely applicable. Often, humans infer causality from correlation, which is inappropriate. With big data, we have to pay attention to how people make decisions. This will cause problems if we assume causation. Is data worth money? Yes.

The USG needs innovation in how it collects and uses big data. It also has to think about how to get information on target populations for information operations. The North Korean government maintains a database on all of its citizens. That would be interesting to have if anything happened. We did not have that in Iraq. We did not understand the power of data.

There are privacy issues. Americans tend to have this idea that we can make ourselves anonymous. With big data, that is wrong. With enough data, we can figure out who someone is from the public domain.

With regard to the "Strategic Log of Failure," this is where people make what they think are perfectly good decisions and they fail stunningly. The problem is in how we make decisions.

The DoD also has to rethink how it does command and control (C2). It is interesting that for all the different mission sets, we have one form of C2. Is that valid? Do we need different models for different mission sets to allow different ways of using cyber and operational capabilities? In a way, when you look at C2, it is about controlling the distribution of information, controlling patterns of interaction, and allocating decision rights. This area requires further study.

LTG Cardon once took a course to learn how to be a task force commander. First, he learned to solve the right problem. That is being captured in doctrine and through operational design. Then, you have to get the C2 right. Third, you have to control the narrative, which is a form of influence. Fourth, you have to get outside help. You are not the expert in everything. "The cyber space is something all the COCOMs need help with. But you cannot have absolute control over it. You cannot control information entirely if you try, you will lose the battle."

"Once you lose the narrative, you can never go back and reclaim it. We have to have people thinking about cyber operations from the beginning. Cyber Command has to engage in operational research. We have to start evolving at a much faster rate, because the world is evolving around us. It is amazing the way data is being used to shape. What are the tools we need to be able to do this?"

Discussion

Do you think there is enough freedom within military institutions to start raising questions from bottom to top or is discussion still constrained by rank?

General Dempsey is working hard to prevent this. For example, LTG Cardon wrote an article about better developing homeland cyber security. He expected to get a phone call from his boss about it, but it did not happen. The USG needs to create a body of knowledge on this topic and start advancing it. He wants DoD personnel to be able to intern at Facebook and Twitter to better understand it. We have an idea what it is from the outside, but we do not understand it. We need relationships with these companies. It is a great time for intellectual debate, but we need resources to devote to innovation and exploration.

Are you working with international relations department in colleges to describe the problem set and ask them to adjust their curriculum to respond to it?

Not yet, but that is a good idea.

Could you comment on how Cyber Command does social media analysis? When operations and exercises are conducted, how do commanders know what is being said out there? Are we missing tools?

We are struggling with boundary issues. Social media trips across not only boundaries within the DoD, but with privacy, civil liberties, etc. It is not that we should not do it, but how do we do it properly? He has strongly supported the Army's legislative efforts to further cyber mission effectiveness at every chance.

How important is situational awareness of boundaries because they overlap in different dimensions? How do you visualize that?

Situational awareness in cyberspace is a critical need. It is important for commanders to understand the terrain in cyberspace just like a commander needs to understand the terrain in the land domain, or maintain situational awareness in any other domain. You need to be able to see both friendly and enemy forces in cyberspace and know where the .mil, .gov, .com space begins and ends. A commander needs to know what the "key terrain" is on the network and how to protect it and how what happens in cyberspace will affect warfighters across all the other domains.

With regard to the difficulties boundaries represent, no matter how good our cyber ability, there will always be obstacles. The NSA will always have a disadvantage. Does it make sense to pursue our adversaries symmetrically?

The greatest innovation of the Iraq war was when General Stanley McChrystal (Commander, Joint Special Operations Command) gave flexible authorities to brigades to target within a 24-hour window. At the time, McChrystal had more intelligence than capacity while brigades had more capacity than intelligence. McChrystal's actions allowed for smart brigades to leverage the target list to start turning the tide against the enemy. It allowed the brigade to leverage every capability. We need more things like this in our operational spaces. He does not

know what it will look like though. He is concerned about establishing C2 that operates at the speed of cyber.

You talked about McChrystal's Baghdad Fusion Cell and flattening. In the next three years, is there any way Cyber Command can flatten organizations to increase the level of Subject Matter Expert participation to enable us to better define the future? How are we prepared for this?

The biggest problem is linking capabilities to commanders. We are increasing our capability, but it is slow because of a lack of institutional training across the Services. We need three kinds of training. First, you have to have training in military schools across all the Services. Commanders have to know enough to know that they need a cyber plan and that they have to integrate it from the beginning. Then you need someone who really knows cyber operations (a cyber operator) we cannot train commanders at that level. Then, at the commander level, they need to know how to ask the right questions.

Keynote Speaker: ADM Michael Rogers, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service

ADM Rogers thanked Dr. Cabayan for inviting him. He is a big fan of SMA and remains impressed with the entire idea of SMA. He asked, how do you look at complex, multi-dimensional problems that have application far beyond one Command? How do you do it with a formal, data-driven methodology? This is not a strong DoD tradition. We talk about operational art and tend to scoff at data-driven traditions and go with our gut. SMA helps us challenge our assumptions. Another strength of the SMA methodology is that it brings together many people from outside of the DoD and the USG. The ultimate key to success is in creating partnerships and relationships to access information and insight.

In the digital age, we have to be an agile organization that is capable of quickly building communities of interest that, one month from now, we had no idea we would be interested in. For example, six months ago, ADM Rogers had no idea he would be spending time on Ebola.

As director of NSA, his job is to collect, assess, and assimilate huge data. How do we distill that data into information that in turn generates insight and knowledge? Our customers care about insight and knowledge. What generates value is insight and knowledge.

The information flow can be overwhelming, but the answer is not to shut ourselves off. So how do we increasingly assimilate levels of data that in the early parts of our career were not accessible to us? What generates value? What is worthy of our time? How do we assimilate and generate insights and knowledge? This is not unique to DoD.

As intelligence professionals, we tend to discount data that we did not generate. Therefore, we did not take advantage of insights from the social networking phenomena and mobile devices that generate the magnitudes of data. So how are we going to assimilate all of this?

This problem set will not go away. It requires us to get outside of our comfort box. To do this we will have to create partnerships.

Going back to Cyber Command, it has three primary missions: defense of DoD networks, operational employment of cyber forces, and, when directed by the President, to defend critical infrastructure (power, water, and aviation) in the US. To accomplish this mission, we have to figure out how to create partnerships and how to harness the power of information to generate insight and knowledge. We are going to do it with people we have seldom worked with before.

ADM Rogers stated that if you told him several years ago that he would be working with executives of power and water utilities as well as banks, he would not have believed it. Such is the interconnected world we live in today. As a military officer, he is accustomed to working with large problem sets. That is not unique to the DoD.

From the NSA side, ADM Rogers runs the largest intelligence agency in terms of people with the third largest budget. It is frequently in the news. This is not an insignificant challenge as a leader—stepping into an organization where he has to spend a good deal of time reaching out to citizens and the private sector about having a real dialogue about moving forward. The issues raised by Edward Snowden have been portrayed as an incredibly simplistic, inaccurate dialogue that does not get to the broader issues: what are we, as a nation, comfortable with in terms of the balance of security and individual rights? We should feel good that we live in a nation where we can have this dialogue.

If we have to compromise who we are or what we are in name of security, then our adversaries have won. We are trying to find a balance of risk. Do not forget, the closer one gets to crisis, the more risk one is willing to accept, which might be considered an error in hindsight. In 1941, the USG interred US citizens based on their ethnicity and race. At the time, we thought that was a reasonable action. Today, we do not understand how we could have done that. What seems normal during a crisis may not seem normal in the rear view mirror. There are many challenges, but methodologies like the ones SMA develops and uses are truly important.

ADM Rogers said he was honored to spend time with the SMA community. He has seen the benefit that this construct can bring to the table.

Discussion

How can we enhance our information sharing capacity with national partners and allies?

ADM Rogers responded that he hopes the USG can increase its information sharing capability. However, current laws and authorities are not currently aligned to make this easy. We are a polarized society. We are an angry and frustrated society. The sense of frustration is fueled by the perception that the mechanisms of government do not seem to be generating results and take on hard challenges. It is not an insignificant challenge. We are unable to generate the political will to address hard problems. It is very sad to consider that we chose to take the poison pill we designed for ourselves (sequestration) rather than deal with tough decisions. It is symptomatic of what it is going to take to generate a cohesive political will.

With regard to the information domain, ADM Rogers does not want to wait for another disaster to do things differently. When he was a senior intelligence officer, the thing that worried him most was decision-maker bandwidth in DC. We are structurally aligned to addresses crises in broad terms; long-term policy and

planning is difficult. We are linear, sequential, and crisis oriented. That is not a good long-term approach. There is no easy answer.

The public seems comfortable with the collection of personal information by Google, Facebook, etc., but is not happy with it being done by the government. What steps can the NSA take to alleviate that concern?

ADM Rogers stated that from his point of view, it is less that the US public is comfortable with what the private sector is doing; it is that they have no clue. If you had a Snowden from inside the corporate sector about what they do with our behaviors, they would be equally as upset. If you ever read those long disclaimers you have to agree to, you would be amazed at what is in there. We would be amazed at what we were yielding. We are focused on speed and expediency.

ADM Rogers stated that one of his frustrations over the last 15 months is that he would like to have a dialogue about what privacy means in the digital age. Is anonymity truly possible? What is acceptable? What is not? We are willing as a nation to accept video surveillance at a higher level than ever before.

Look at what the private sector does with data. People outside of our lives are collecting more data on what we are doing every day than in the history of the world. We have not had a conversation about whether we are comfortable or not. But the private sector is not interested in a dialogue on privacy right now. They push that on the NSA. The NSA should have this conversation too. NSA follows the law. The part you do not hear about with regard to the phone records is that the collection of that material was in accordance with a law passed by Congress twice. It was not something NSA made up. It was not an executive order. It was a law that was upheld. It will continue to be challenged, which is how it works.

As emotions die down, he expressed hope that, as a nation, we could have a broader dialogue. What does privacy truly mean in this world? It is not about good versus bad.

At the NSA, ADM Rogers tries to generate insights about what nations states would do to harm or gain advantage over the US. Companies use big data on behaviors to provide insights that generate better business outcomes. The objectives are not new, the tools are.

With the arrival of the information age, are you comfortable with the tools and analytic methods we have?

As a society, we ha e not come to grips with what the information age means. If we thought we were interconnected in the last 20 years, we have not seen anything yet. We have not come to grips with the 2nd and 3rd order effects of this interconnectedness. Unfortunately, at the rate we are going, we will not come to grips with it until we come to a crisis. He hoped it would not come to that.

Given the exponential increase in data, what challenges come with leveraging vast data and finding the right opportunities to present these challenges to decision makers in DC?

ADM Rogers qualified that he did not want to paint this as a bad picture. The tools we have allow us to make connections and generate insights that we never could have done in the past. That is a good thing. But the challenge will be that the government's use of big data is perceived to have a big brother element. There is a chill in academia of those willing to work with the government on big data issues right now. This is not good for our nation. This is not going away and it is not something we can ignore. We can, and have to, deal with it. We need to recognize the benefit of big data on a global scale. The tools allow us to take disparate dots and bring them into a coherent whole.

Operators increasingly try to obtain intelligence data before it has been processed. They want to get ahead of the decision cycle, which raises issues of misuse of unprocessed data.

There is no right answer here. There are those who believe we should push information as far forward as possible. In an interconnected world, what happens if connections are severed? Analysts often think that no one understands their requirements like they do. They doubt the ability of an external organization to understand both their needs and intent. Therefore, they want to move it forward.

Cyber is also driven by rules of engagement and authorities, which have not been pushed significantly forward. Therefore, we have to think like an enterprise. We have to fight our own culture in the uniformed world. From the commander's first day as a leader, he has to think about the mission. I tell them that what they need to control is the outcome; do not worry how the sausage is made. From an intelligence perspective, we integrate capabilities to the forward-most edge of the battlefield. We literally have integrated capacity to understand commanders' intent and discern who to maximize value. It is not either/or. We need to think like an enterprise.

How do we deal with blue data?

How accustomed have we become to analyzing blue data on our own forces? Right now, COCOMs are under pressure to make headquarters smaller while they are given more responsibilities. There is a mismatch here. ADM Roger's major concern is not maneuvering forces; it is cyber integration at the COCOM level. We are not providing them with manpower that understands cyber on the planning and operational levels. We cannot expect COCOMs to maximize cyber capabilities if we do not send them the right people to help with this.

Historically, basic maneuver elements were the easiest to generate. The hardest is expertise in headquarters. When you build something from the group up, it takes more effort to generate capability. We forget this lesson.

There are good guys and bad guys out there. One factor you may want to consider in calming the American public is how we deal with ethics inside intelligence. Have you considered setting up an Institutional Review Board (IRB) to inject ethics scrutiny before you launch a new data system?

In 2008, FISA told NSA it had a problem with controlling and protecting data. In 2009, his predecessor implemented an incredibly formalized systematic multilayer compliance mechanism that covers data and tools. That mechanism has been evaluated by two presidential reviews. Both reviews came back and said that the NSA has not tried to undermine rights of citizens and has a comprehensive compliance framework. Unfortunately, Snowden did not steal compliance mechanisms or insights on oversight and compliance. He stole insights on some amazing technical capabilities and said we were using them indiscriminately. We have amazing technical capabilities; we do not use them indiscriminately. We use them in compliance with the law.

We are close to the tipping point where we can have a dialogue without screaming. We have become a society where the louder you speak, the more righteous you feel. He encouraged a broader debate on compliance and oversight.

Regarding privacy, Presidential Policy Directive 28 talks about the extension of privacy and civil liberties regardless of nationality. It seems to be extended across the globe. In the National Security Council staff, that guidance is bleeding into other areas.

Should the US provide legal protection to every US person? We define person broadly in the US to include citizens and corporations. What are the implications of extending protections to persons around the globe? This will really slow us down. For example, would we need a warrant to collect on a non-US citizen abroad? Do we need that for every target in the world? We interpret PPD28 to mean that we need to comply with all laws and authorities, which we do. The next conversation is do you want to move beyond that to something else? It will involve tradeoffs. It has huge implications for national security. We could do it, but there would be tradeoffs.

Panel 1: Complexity, Interdependence, & Emergence in an Interconnected Information Age

The age change we are experiencing is the central issue facing the U.S. today—with all of its threats and opportunities. It is essential to understand the nature and character as well as the dynamics of the Information Age.

Panel Members:

- CAPT Todd Veazie (NCTC)
- Dr. Wayne Porter (Wikistrat)
- Dr. Mike Vlahos (Johns Hopkins University & U.S. Naval War College)

CAPT Todd Veazie, NCTC, moderated the panel. *Captain Veazie is assigned to the National Counterterrorism Center where he leads a team producing counterterrorism net assessments. Prior to this he served as the Executive Director of Joining Forces in the Office of the First Lady at the White House. He was born in Washington D.C. and earned a Bachelor of Science degree in Marine Science from the University of South Carolina and was commissioned in 1986. After commissioning he reported to Basic Underwater Demolition/SEAL training and graduated in Class 140. Veazie is a career Naval Special Warfare (NSW) SEAL officer and has served in east and west coast SEAL Teams and deployed to over fifty countries around the globe leading SEAL formations in execution of combat and peacetime special operations in Latin America, Europe, Africa, the Western Pacific, and the Middle East. Command tours include SEAL Team SEVEN in San Diego, Naval Special Warfare Unit THREE in Bahrain, as well as duty as Commodore, Naval Special Warfare Group FOUR in Virginia Beach. He has served in numerous staff assignments that include personnel policy at the Bureau of Naval Personnel, the Assistant Chief of Staff for Resources, Requirements, and Assessments for the Commander, Naval Special Warfare Command, and in the Operations Directorate (J3) on the Joint Staff at the Pentagon. Decorations include the Legion of Merit (3), the Bronze Star, Defense Meritorious Service Medal (2), Meritorious Service Medal (3), and various other awards. He is also a 2003 Graduate of the National War College earning a Master's Degree in National Security Strategy. Captain Veazie has been married to his bride Vanessa for 23 years. They live in Alexandria, VA.*

CAPT Veazie introduced the panel and noted that the information age transition is rapidly taking place and, as a result, a new set of rules are being developed that are creating new global commons. Age transitions are typically defined by dislocation as people try to begin accepting the rule changes that result from transition. Often times, instability and violence arise during these age transitions. Following the Cold War, a rise of networks underpinned by information technologies enabled the networks to do new wonderful, innovative things, but also provided them the opportunity to take a new destructive and violent path if desired.

CAPT Veazie added that in today's rapidly changing environment, we need new metaphors. The metaphors of the past are breaking down with the new, incredible complexities of the world today. Furthermore, there is an incredible amount of data

constantly being collected in the world today, but the ultimate challenge is figuring out how to make sense of the signal in all of that noise.

Dr. Wayne Porter, Wikistrat

Dr. Porter spoke about the *National Strategic Narrative*, which he helped to develop as a means of understanding the evolving United States role in a very new strategic environment. The basic idea of the *National Strategic Narrative* is that the United States needs a strategy to sustain its enduring national interests in a way that values and characterizes itself as American. It is pretty clear that over the last 20 years there has been a significant ethical shift in terms of certainty. The world today consists of a very complex and uncertain environment characterized through interconnectedness and increased competition over resources.

We are in the midst of the greatest epochal shift for civilization since the Age of the Enlightenment—or Age of Certainty as it came to be called. Just as the enlightenment era led to the industrial age, people are beginning to wonder what will follow the information age. This new age is characterized by digitization, exponential access to information, and cognitive innovation. As a result, it is time to shift our focus beyond predictability. In today's environment, it is hard to believe that we are able to predict anything. Instead, we need to focus more on sense making. The world today is overwhelmed with data and we need new tools and methodologies to use this data to make sense of an uncertain environment. We need to stop focusing on risks and threats, but instead start focusing on opportunities to shape the rapidly changing environment. We must start understanding the dynamic, non-linear feedback (i.e., time delays and effect) that is part of all complex systems so we can begin to overcome policy resistance as short term solutions to problems that only end up causing second and third order effects to the problems we are trying to solve.

Ultimately, the United States needs to become more strategic and adaptive in its planning. The only way to do this will be if we can transition away from the expert approach of trying to filter huge amounts of data through a small panel of experts, and instead create platforms that can help us leverage bounded crowdsourcing, which is a multidisciplinary approach utilizing people who can look at a large problem through diverse perspectives and present alternative outcomes to help us understand where we are going in the future and how we can adapt.

Dr. Mike Vlahos, John Hopkins University and U.S. Naval War College

Dr. Vlahos began by noting his belief that information itself represents an artifact—information is something that we make. The reason we use terms like "data" to describe information is because the term "data" has a clinical ring to it. Data is external—it has a validity of its own. On the other hand, information is something that we have created and shaped to our purpose. As a result, we use information as the brick and mortar of reality. If information is thought about as a human-crafted

reality artifact, then we can begin to see the importance in understanding the way in which we absorb information and then assemble and sculpt it. The key is in understanding what humans do with information. The ways in which we do things with information help to explain who we are. It will also help understand the limitations to which we understand actual reality. The competing needs of our reality tell us how we need to use information to tell ourselves the story we want to hear.

Our belief systems are shaped by how we want to put information together to tell a story. Therefore, it is critical to examine the nature of our own belief systems. However, analyzing things that we "know" to be true is something that Americans will never do. Questioning the belief systems that we have always known to be true is something that is not likely to happen. This creates a fundamental problem. It is crucial that analysts are able to find a sense of detachment, but it is extremely difficult to train someone to question their own belief systems. Thus, it is very difficult to develop a core of analysts who will stand back and be able to have a sense of detachment from tapping into their belief systems when analyzing a problem.

The world today is in an age of transition. Throughout the transition periods of the past, it is clear that the most important factor in determining the success or failure of world systems during times of transition is the system's willingness or resistance to accept change. In reality, today we are rather conservative and overall resistant to change. Even though the present system is in tremendous tension, it is still resistant to change. Historically, past systems have typically unraveled because the elites of the system were resistant to change and instead believed they could use force to remain in power. However, it has been observed that the use of force often comes to the detriment of those in power and the overall system.

Discussion

Has work been done on identifying attributes of resilient systems and the societies that can be used to characterize them?

Dr. Porter noted that he does not like talking in terms of resilience. Resilience can be characterized as the ability to overcome something and then keep going. Resilience is different from sustainability, which is the ability to move forward. A greater emphasis should be put on how systems interact with each other in a sustainable way going forward. It is often difficult to look backwards at previously resilient systems because the today's environment is incredibly different from what it was in the past.

Dr. Vlahos agreed with Dr. Porter's preference of using other descriptors than simply resilience. Additionally, when looking back, it is crucial to specifically frame how you define what is actually a lesson learned from the examination.

With respect to the process of change, with the billions of people on the world today it is farfetched to think that everyone can change. However, incentive systems within the United States and its institutions exist that seem inappropriate for our current world. Consideration should be put into thinking about how to alter some of these processes. Do you have any idea how to change incentive systems in these big institutions?

Dr. Porter responded that it is difficult to maintain the aura of entrepreneurial and intelligence dominance when the U.S. education system is in the shape that it is today. Our current system was developed when we were an agrarian nation and is currently out of date. It is important that we begin to understand that there are elements of critical thinking that need to be used to examine of our current internal systems and cultures. The United States should look at some of the more effective education systems in the world and try to map some of those within its own borders as test beds.

Dr. Vlahos added that one of the biggest problems that exist today is denial. For example, the tenure system that exists at universities in our country is a great example of this denial. Presently, we are observing an abusive hollowing out of the disciplines at the core of our culture. Part of the problem is that we have a society that is ruthless and wedded to a single standard of value.

Panel 2: Setting the Stage: The Information Age, Networks, and National Security

This panel provided a preliminary discussion and overview of issues surrounding the information age, networks, and national security. Furthermore, the panel offered thematic questions for subsequent panels. Key questions examined by this panel include the role of big data in the context of national security, the key dynamics shaping emerging geopolitical structures, and hoe the world is being shaped by the information age and connectedness.

Invited Speaker:

- Mr. Josh Kerbel (DIA)

Panel Members:

- Dr. Dana Eyre (SoSA)
- Dr. Randy Kluver (Texas A&M)
- Dr. Laura Steckman (WBB)
- Dr. Regan (Booz Allen Hamilton, EUCOM)

Dr. Dana Eyre, SoSA

Dr. Eyre introduced the panel and noted that the information age is both a reality and an ascendant rhetorical device for understanding. As a reality, the phrase describes a large number and variety of technical changes, ranging from sustained increases in processor and storage capacity, and volume of data, to the proliferation of networks, as well as a large number of other changes enabled by these technical capacities (e.g., the rise of web commerce and rapid delivery services, or the rise of "many to many" communications). As a complex rhetorical device, the idea of the information age at the same time enables us to see these changes, conceals other changes, and distorts our understanding of the changes. The label "information age" could have been applied in the era after Gutenberg's revolutionary achievements, or to the 19th century that witnessed the invention of standardized worldwide time keeping, the telegraph, and modern bureaucracy (itself an information storage and handling revolution). These technical developments resulted in massive social change, and robust growth in both state and corporate capacity, yet we don't think of them as "information" revolutions. Instead, our understanding of the 19th century, as well as our understanding of conflict and international relations inherited from that era (e.g., through the vocabularies of Clausewitz) is dominated by other metaphors of the era, particularly kinetic physics (e.g., friction, center of gravity, force) and rational choice (e.g., the state as a unitary actor, national interest). It is critical to be aware of the dual nature of the phrase "information age" because it is not only the technical changes that change the world, our beliefs, our anticipations and our fears about these changes, also change the world. Rhetorical devices such as "the information age" (both a metaphor and a synecdoche) both shape our understanding and in turn shape the world. The way we use these metaphors sinks into our thinking, their rhetorical nature is forgotten, and they

shape the world in which we live. The idea of the information age should highlight, not only technical changes, but also our increasing visibility into the psychological and sociological processes of perception, sense making, and social construction of reality. If we are to adapt, successfully, to this "information age" we must constantly interrogate the world, the technical and physical changes, and the ideas through which we understand the world. The talks in this panel do both – challenging our understanding of the information age, and how conscious we are of our understanding.

Mr. Josh Kerbel, DIA

Mr. Kerbel discussed complexity and simulation in the context of the intelligence community (IC). He asserted that the notion of "increasing complexity" is the great post-Cold War cliché of Washington DC—not because it is not real but because the government seems not to change that much. This is certainly the case in the intelligence community where many analysts have rebelled against the notion of increasing complexity. These analysts argue that the world is increasingly complex, but it has always been so. They are not entirely wrong. However, the last 30 years have seen complexity increase at an unprecedented rate and scale. In particular: 1) China became a fully integrated of the international system, 2) the USSR collapsed its remnants connected to the broader international system, and 3) the information technology (IT) revolution allowed people down to an individual level to not just "be reached" but "to reach" heretofore impossible numbers of others. Mr. Kerbel believes that these three factors in combination constitute a revolutionary—not just an evolutionary—change in the global strategic environment.

Often times the IC is somewhat in denial in thinking that all it needs to do is get better at things it has traditionally done. For the IC, this is critical thinking and there are numerous critical thinking classes offered throughout the IC. However, the IC has completely neglected creative thinking. Creative thinking is the hard part. Some wonder if creativity can even be taught? In reality, from an IC perspective, it is crucial that creativity is taught—or at least cultivated—because there is no way we can fully understand a complex system by simply critically breaking it down. We need to creatively think about how the system is put together-interconnected. Unfortunately, the IC is often creativity averse. The notion of creativity in the IC is often a no-go zone. Indeed, the USG as a whole has a creative thinking problem.

Within the IC, most analysts think according to four basic analytic rules: 1) the world is additive, 2) cause and effect is identifiable, 3) repeatability, and 4) input and output are proportional. These are reductive rules that underpin much of the thinking within the IC. As effective as this kind of rule-based-critical-thinking can be for understanding complicated challenges, it is often problematic when misapplied to highly interconnected, complex phenomena. Quite simply, complex issues tend to defy the behavioral conclusions that these rules promote. Indeed, complex phenomena can only be understood and anticipated via holistic, synthetic—creative!—perspectives that break these analytic rules.

There are many ways the IC might start to attack this excessively critical-anti-creative-mindset. However, for the purposes of this panel, one of the most powerful approaches would be to make the use of synthetic methodologies (gaming, simulation, red-teaming, and so on) mainstream-vice "alternative"-analytic activities. This, in turn, would allow for greater consideration of U.S. policy—something that is too often lacking in IC assessments, especially when the US is such an influential shaper of, and responder to, global developments.

In sum, creative thinking is now a vital-and fundamental-ability that needs to be carefully cultivated, incentivized, and valued by any organization that seeks to remain relevant in this evermore complex world. This is true for the IC and by extension the entire USG national security apparatus.

Dr. Randy Kluver, Texas A&M

Dr. Kluver discussed information in society. Information is nothing new. What is new, if anything, is the role of knowledge networks. In thinking about the theory of communication power, an abundance of information does not equal power—although access to information can be powerful. Moreover, having different information or better information does not necessarily equal power either. When thinking about power, it ultimately comes down to the ability to define reality. A communication power is a power that helps describe reality and drive metaphors central to communication.

Social networks have always been part of our reality. What is different today is that the smaller networks have begun to rival the power of the nation state in defining our reality. One of the critical components of this is the ability to facilitate information flow between networks. In addition to having more information, we are now operating in a world where logics have changed. A logic is a way in which we receive, process, transmit, and act upon information. There is logic to traditional media. There is a different logic to new media. There is a different logic to today's networks, and this is changing the geo-narrative of the world.

Communication is the key to the theory of power. Drawing upon Manuel Castells' Theory of Communication Power, there are two primary tools of influence. First is the power of switching. This includes the ability to create new networks, change network linkages, or disrupt network formation. Second is reprograming, or changing the values, skillsets, and knowledge sets within a network. Geopolitical power is thus grounded in these two techniques.

Dr. Laura Steckman, WBB

Dr. Steckman discussed social media as big data and whether or not we are looking for the right things in the right places. It is often difficult to define social media because social media is different for everyone. Social media is not a new concept—people have always communicated with each other in their networks. What is new, however, is the vast access to social media that now exists because of the Internet.

The Internet adds an extra level of complexity and rapidity to social networks and social media.

Twitter is the new phenomena of social media analysis, but it is important to always ask if Twitter is the right place to go to answer a specific question. Different cultures and societies use social media differently. They often prefer platforms that are unknown in the West and therefore overlooked for analytical purposes. If we are going to analyze the information that is available from social media, we should also understand how different people in different parts of the world use and understand social media. Such an understanding would permit us to map the information environment, which currently remains under-defined and opaque, and to derive conclusions that are more meaningful from analyses of the environment.

Dr. Regan, Booz Allen Hamilton & EUCOM

Dr. Damron discussed big data and open source information at EUCOM. Data becomes "big" when its structural characteristics (e.g., Douglas Laney's "volume, velocity, and variety") become issues themselves (storage, algorithmic efficiency, unstructured data management, etc.). Such data requires a paradigm shift from *data* sharing to *access* sharing because transferring such massive amounts of information is impractical; what is needed is the ability to query the data directly and run analytics on the germane subsets in as near to real-time as possible. Intelligence could learn much from the private sector in this regard. For example, data from classified programs with one-off tasking procedures are generally *not* available for aggregation and analysis that could provide insight into emerging or evolving trends. Big data is typically in two flavors: wholly unclassified or highly classified. EUCOM is looking at wholly unclassified big data primarily because (1) Snowden has created a need to increase trust through transparency and (2) unclassified information is broadly shareable (whether with NATO allies and partner nations or European Union institutions and law enforcement entities)—a must in light of limitations imposed by EUCOM's "by, with, and through" authorities.

Big data is generally best for automation of simple and/or formulaic tasks (e.g., recurring reports with updated data) and augmentation of analyst capabilities (e.g., sifting through massive amounts of information to help focus an analyst's scarce attention and time). However, big data is not currently good for automation of complex, adaptive, and/or high-stakes tasks (e.g., targeting) and replacement of human analysts or human reasoning (algorithms display no creativity, no ethics)—although it is certainly improving, concurrent with advances in artificial intelligence (AI) more broadly. Big data can be dangerous for at least two reasons. First, the use of normal statistical techniques without compensating for data "bigness" can yield erroneous results. With a large enough dataset, anything can be shown to be related to anything (statistical significance). Furthermore, results can be highly sensitive to variable definition (operationalization—an especially thorny issue in the social sciences). Second, results must be interpreted (substantive significance), which requires knowledge of context and contextually appropriate theory and training to

recognize and avoid fallacious reasoning. Bottom line: There is no substitute for clear thinking.

EUCOM is currently developing tools for looking at big data. Additionally, EUCOM is working on a development lab. The goal is to create a data and algorithm playground that can be used to test new ideas. EUCOM's Knowledge Commons tool is a big data open-source repository that ingests massive amounts of Web content and processes it via thematic and entity extraction coupled with document categorization and signal detection to provide environmental sensing and scanning to enable analysts to rapidly understand emerging and evolving topics and trends. EUCOM's Savanna tool provides an analyst workspace focusing on information synthesis and production. The tool focuses on relationships between items and explicitly represents analysts' thoughts in mind maps (an analytic best practice). All the data is "live," enabling changes in the data to propagate to all products that use that data, and the tool is highly visual and interactive.

EUCOM intends to share these tools with NATO allies and partner nations to create a Community of Practice in order to share information and insight, enable collaboration/coproduction on topics of mutual interest, develop and share analytic best practices, and ultimately to enhance NATO interoperability.

With an eye toward all of this, ECJ2 has begun leading an effort just in the last month to systematically: 1) understand, codify, and verify process/doctrine regarding the use of open source information; 2) assess the potential for collaboration and coproduction with NATO allies and partner nations in an open source environment; and 3) engage in a dialogue to convince others in the Intelligence establishment that open source information has intrinsic value—it is more than just another input to "all source analysis."

Panel 3: Geopolitics and National Security in the Context of the Information Age

Panel 3 explored patterns of conflict and warfare in the information age. Information technologies are changing the character of warfare due to advancements in networking, robotics, command and control, etc. This panel also explored how potential US adversaries might employ information technology to create a narrative that develops sympathy for their cause and hinders US involvement and decision-making during a crisis.

Panel Members:

- Mr. Dan Flynn, DNI/NIC, moderator
- Mr. Paul Scharre, Project Director for the "20YY Warfare Initiative" at the Center for New American Security

- Mr. Dean Cheng, Research Fellow at the Asia Studies Center at the Heritage Foundation
- Dr. Stephen Blank – Independent Consultant (formerly with the Army War College)

Mr. Dan Flynn, DNI/NIC

Mr. Dan Flynn encouraged the panelist to take the concepts presented earlier in the day to see how they play out in the national security environment. This panel also was asked to incorporate nonwestern perspectives on the use of information in conflict. The panel discussed how states might exploit the gap between wartime and peacetime—so called "grey zone conflicts"— to advance their interests.

Mr. Paul Scharre, Center for New American Security

Much of today's military technology—long range sensors, networks, precision-guided weapons, and stealth—were born out of the first stage of the information (microprocessor) revolution in the 1970s. At the time, the US Department of Defense was the lead in the information revolution. That is no longer the case. The bulk of innovation is occurring outside of the defense establishment. In the future, game-changing innovations may not come from secret military laboratories.

There are three big IT trends: transparency, connectivity, and intelligence. Large data and information flows freely within IT. It is nearly costless to copy and transmit information. There is a lot more information about the world available than in any other time before. Many physical objects are being endowed with more sophisticated intelligence—cars, aircraft, and refrigerators.

The advantages the US military had are now in the hands of nonstate actors and individuals. In the future, wherever US forces will go, it will be in a world with ubiquitous access to smartphones. Populations can transmit location of US forces in real time. The world is more transparent, more contested, and more lethal for US forces.

New technologies can be viewed through a series of competitions: hiding vs. finding, coordinating vs. disorganization, understanding vs. confusion, and offense vs. defense, etc.

With regard to hiding versus finding, adversaries switch to hiding to avoid precision weapons. But some advances in physical stealth are not following Moore's law, but finding is. We have the ability to sift through large amounts of data and draw passively from multiple angles through computer processing, such as multi-static radars and other sensing tools. The ability to fuse data makes it easier to sift out noise. In the future, hiding will be increasingly dependent on software-based means of stealth.

With regard to understanding versus confusion, we use a combination of human vs. machine cognition to shift through vast sources of information. We do not have Google for the military dimension to help us sift through information. Increasing

machine intelligence will help. But the best chess players in the world are neither humans nor machines; they are human/machine combination. They innovate better together than individually. The human brain is the most powerful computer on the planet; we need to enhance that.

Deception will be important. It is not a new development, but the advent of the information age allows new way to deceive enemies or intentionally decrease their confidence in their data. A key component of warfare is changing the information an enemy is presented with faster than he can process that information and respond, so that the battlefield is constantly shifting, inducing paralysis.
With regard to networking, coordination and disorganization is important. Those who can continue to fight as a network will have the advantage in this domain. Networks have been relatively uncontested; that is not likely to continue. To combat this, we need better doctrine and training. Operators need to learn how to operate in degraded conditions and to shift between them.

Space is a particular vulnerability. The US will no longer be uncontested there. The USG should develop the ability to conduct operations when space/cyber capabilities have been degraded or denied.

With regard to shooting vs. intercepting precision-guided weapons, we can use lasers, electromagnetic rail guns, and counter-swarms to stop swarms.

The USG needs to continue to learn how to shape key populations. There are an increasing number of actors in the space and many are not simply states.

With regard to speed of action versus speed of decision, there is a tension between the pace of military operations and the pace of decision-making. There are ways to build in time for decision makers. The Cold War showed us that we need to have second-strike capabilities. We need to respond in the time and place of our choosing.

Dr. Stephen Blank, Independent Consultant (formerly with the Army War College)

In the last 15 years, the US has waged two wars and lost. Russia is a backward, inferior actor, fought two wars, and won. The USG believes it is in phase 1 with Russia; Moscow believes itself to be in a permanent state of multidimensional conflict with the US. Russia believes it is under attack from the West—that the West is trying to destroy Russia systems of government and wants to establish unipolarity in the world. They are acting accordingly.

The Russians are engaged in unrestricted warfare. They have inherited Leninist ideology that a state of siege exists between east and west and the domestic economy is part of the west. Russia is using all instruments of power in the conflict and has been for years.

If you read Russian literature, about eight years ago, they began to think seriously about warfare with the US after its invasion of Iraq in 2003. They came to the conclusion that this is just a modern kind of warfare. For the Russian military and government, the threat is not just military; it is multidimensional and the key dimension is information.

Russians define information warfare in an antithetical way to us. Big data is only part of it. Russians see information warfare as essential and it includes degrading networks, cyber crime, hacking attempts targeting US industries. They see it as mass political warfare and manipulation. We see this in Ukraine, Europe, and US.

Military operations are designed not only to defeat the enemy physically, but to crush their moral—not just the troops but the people and their government, so does understand and using culturally specific features of the economy though exposure via media. The distinction between military and civilian is disappearing. We need joint civilian and military operations. The Chinese use their own terms for this, but they would buy every word.

The USG does not understand the Russia system. The government has systematically degraded intelligence capabilities over the years. Last October, Dr. Blank met with the Ukrainian opposition. He told them if they signed an agreement with the EU, Russia would invade. Russia thought we knew their decision calculus, but we did not. When the operation came, the USG was caught by surprise.

Information is not knowledge, it is not understanding, and does not give you strategic foresight. And even if you understand "counterunconventional warfare," building perfect bureaucratic architecture is not going to substitute for informed strategic understanding. Their strategic insight has been better than the USG's. The USG has to understand the way they think. They see the world in a state of siege—they presuppose conflict with everyone, even China. Information warfare is the main form of warfare, which is political at heart. Political warfare is the only kind of warfare the USG does not do.

The purpose of war is to manipulate political structures through deterrence or panoply of asymmetric measures.

Russia has retained a capability for biological warfare. They do exercises with chemical and biological warfare. They expect to see chemical and biological on the battlefield. They have talked about using information technology as a biological weapon to get in to users' heads.

Mr. Dean Cheng, Asia Studies Center, Heritage Foundation

China is using information in the context of its "Three Warfares" strategy: public opinion warfare, legal warfare, and psychological warfare. Clausewitz said that war is politics by other means, but the Chinese say that politics is war by other means.

For the People's Liberation Army (PLA), political warfare *is* a form of warfare. The main difference is the battlefield, which is human rather than physical terrain.

IT provides greater access to people more than any other form. In the PLA, political warfare is a form of combat that encompasses all nonkinetic strikes that emphasizes political, psychological, and moral operations. Political warfare is a tool of the armed forces. The military plays a central role here. Political warfare is conducted similarly to other military operations. You need to have planning, coordination, and synchronization with other operations.

Political warfare is the hardest form of soft power. The advent of the information age allowed for modernization of political warfare. Political warfare is conducted to secure the political initiative and create and advantage over the opponent. Central to this is the idea of three warfares identified by the Chinese in 2003 PLA regulations and updated in 2010. The operationalization of political warfare includes four kinds of operations.

The first kind of warfare is public opinion warfare. This is the struggle for the venue in which the other two forms of political warfare will be conducted. The audience is the domestic population as well as the adversarial, civilian decision makers. The goal is to preserve positive moral at home and abroad as well as to alter the enemy's situation assessment. It involves channels of mass information to reach foreign and domestic audiences conducted systemically according to a previously determined plan an objective. This is seen as so important; it is an independent form of warfare. It is a constant activity that shapes the long-term environment. We are in phase 0 with the Chinese in terms of the public opinion war. The goal is to get one's message across first. It is easier to create a first impression than to dislodge one. In the Chinese view, even before troops move or there are overt activities, political warfare is underway first.

The second kind of political warfare is psychological warfare. It seeks to cause the enemy to second guess themselves and erode confidence. It comprises five tasks:

1. presenting one's own side as just (and the adversary as unjust);
2. emphasizing one's advantages;
3. undermining the adversary's will to resist;
4. encouraging dissension in the enemy's camp; and
5. implementing psychological defenses.

Psychological warfare is also linked to information warfare, which involves electronic, network, and psychological warfare. This means going after hardware, software, and the mentality of the consumers of information.

The third form of political warfare is legal warfare—arguing one's own perspective is in compliance with the law and the other side's is illegal. Then, if that argument

does not work, the Chinese argue that they only broke the law because the adversary made them.

Political warfare is conducted in China through the General Political Department (GPD). The PLA is also run through the general departments, not the services. The GPD is responsible for all human aspects of the PLA, not only for political orthodoxy but running legal elements, officer promotion, troop morale, and political warfare. If they had a chaplain's corps, it would be in the GPD. This means that political warfare is not an afterthought. The second most important general department in the Chinese military is conducting it. The GPD is bureaucratically equal to the General Staff Department. When political warfare is conducted, it is done at the highest level. GPD has a direct link to the rest of the Communist party. They sit with the civilian component that facilitates access to civilian resources like media experts. They are bureaucratically and politically linked.

Mr. Cheng presented three takeaways. First, the PLA sees political warfare as a form of warfare. It requires planning and coordination of operations. Second, political warfare blurs the line between peace and warfare, requires peacetime operations and understanding in advance the psychological and decision-making process. Third, it is aimed at pre- and intra-war time periods as well as in the post-war context (this is phase 4). As the PLA doctrine states, political warfare seek to secure the political fruits of kinetic combat.

Discussion

Mr. Flynn stated that the information revolution is changing warfare; we need to understand how other countries are planning to conduct future wars.

Counterinsurgency deals with the population. Looking at Afghanistan, what are the lessons learned from our nascent population shaping efforts there?

Dr. Blank stated that Russia has been fighting counterinsurgency wars for 500 years. They have an enormous amount of experience. The Russians seems to have adopted 2 fundamental lessons from this experience: 1) they come in strong, devastate the enemy in a scorched earth fashion and the adversary usually fails, and 2) they try to find leverage positions in target societies and coopt the plot. Elites that are susceptible to working with the Russians is a much more successful pathway. The Russian empire has always been able to find "Moscow's men." But when they can't find them, they fail. The essential lesson is to define those elites who can govern the country with legitimacy and authority (not power) and bring about a situation acceptable to the US on their own. We have been quite inept in Iraq and Afghanistan in doing so. Karzai's relationship with the US was a disaster as was the relationship with Maliki. We always seem to find the wrong guy. We have to accept what we are dealing with: a SOB, but our SOB. The Russians are not afraid of that tactic. They will ride that horse. When they fail, it because they cannot find their "Moscow's man."

How do you assess China and Russia using political warfare to achieve strategic objectives? How should we compete in space?

Mr. Cheng replied that China is a status quo power. So are we. The problem is how we define things. We define our status quo based on history. In 200 years, we have had a pretty good run. We like the system and our status quo. But China has a longer history. The Chinese name for China (zhongguo) can be translated as "middle kingdom" or as "central kingdom." China has been at the center of Asia for centuries. Their perspective on the normal state of international relations in their region is very different from the European model. Asia was never a land of shifting alliances like Europe has been. In Asia, what you have is bandwagoning, tributary states. The neighbors offered tribute to the center—China. It was not a bad status quo for them. China wants to re-establish its pre-eminence in the region. This does not mean there will be Chinese troops in Manila, but it means they want a defacto seat in every presidential office so that leaders have to think about China's desires. The Chinese government wants to make sure its interests are not challenged. After that, the Chinese do not care whether these countries suppress ethnic or religious minorities. As long as China is buying products from a country and the country delivers, China does not care about that country's internal politics. That is a very different model than Europe or America. It establishes a sphere of influence. The three warfares create conditions whereby it will be hard for local leaders to invite Americans in on a regular basis rather than making nice with China.

Dr. Blank added that, first, Russia want a group of ruling elites from the old KGB. They see their power and wealth being challenged by the US and its allies inside of Russia. They want to maintain power and wealth by creating a foreign enemy and a great power restoration—something akin to the USSR minus the ideology and complete control of the caucuses. They want to establish a sphere of influence in the region. They want to revise the 1989-91 settlement in Europe. Moscow believes that not one state in Europe has true sovereignty that has to be respected. They want to have Moscow's men in every capital in Europe that exercises leverage. They also want the US to get off their backs. They do not want the US to lead a unipolar world. They want veto power on the US. The Russians say they get no respect. The problem is the Russians are trying to gain respect in the same way Tony Soprano would.

Mr. Scharre added that the USG could shore up its architecture space. We are doing that to the best of our abilities. His larger concern is the inherent vulnerability to cascading effects. For example, there have been two incidents to date regarding space debris. There will be escalating debris over time. The challenge is hard to quantify, but it could deny us a particular orbit. We are not going to access to communications and we are not resilient to a complete denial of an orbit in space. We need to invest in ICISR resiliency. If he was China and wanted to escalate a conflict, he would detonate a series of ASAT test satellites to create enough space debris to deny orbit.

Mr. Cheng replied that he is not sure that is a Chinese model of space behavior. He agreed that a more resilient C4ISR architecture is important. The degree to which we rely on space is affected by our reliance on other assets. If a high bandwidth territorial capacity is eliminated—like a submarine line—you put a lot of burden on space. This is a recognition that they know that if you hold a gun to your own head, it can be dangerous to everyone.

Mr. Flynn noted that other actors, such as ISIL and Iran, are also exploiting information technologies and social media. Iran refers to the concept of "soft war" to describe threats posed by informational and media operations. . If the Chinese think political warfare is the hard edge of "soft power", then the Iranians probably believe "soft war" is the soft edge of "hard power."

In China, there seems to be gigantic ream of pulp fictions being published that seems aimed at domestic Chinese audiences from the PLA press. Can anyone explain this?

Mr. Cheng stated that the PLA's publishing system serves multiple purposes. It serves to educate PLA personnel. It is the largest military in the world. Additionally, the PLA has to fight for resources, so it publishes part of ongoing debates. It also publishes internal propaganda. Finally, it is a moneymaking operation. Depending on the material, it may function for one or more of the above motives. The pulp fiction aspect is an easy sell. Being anti-Japanese in China is an easy way to make money. Is there a political warfare aspect? Yes in that they can dial it up or down. It is also a unity thing that is turned toward mainland China and Taiwan. Revisionist history is popular. The Chinese frame Chiang Kai-shek, now, as a nationalist—he believed in one China. There was this anti-Japanese iPhone app in China that got pulled. There was no evidence it was produced by the PLA, but it sold millions of copies in China.

Mr. Flynn, can you provide insights about what is going on within DNI and the intelligence community to conduct foreign influence analysis that incorporates human factors in an operational construct? How well poised are we to provide data to key audiences to fight adversaries in the information environment?

Mr. Flynn stated that the USG has to allocate more attention to this problem. If Russia and China are already executing "phase 0" operations against us, how do we attune our policy makers to that challenge?

Panel 4: Operational Perspectives: Opportunities and Challenges (Joint Staff and the Commands)

This panel asked representatives from the Joint Staff and Commanders to discuss how the information revolution is shaping their worlds. There is a correlation of information environment to the national security environment. The same freedoms we seek to protect are being used in an agile manner by adversaries and potential adversaries to our disadvantage. Information is a combat multiplier but we are moving into an age where user generated content allows adversaries the ability to employ the ever-growing list of social media that nation-states cannot match. How do we account for this trend?

Panel Members

- Brig. Gen. David Béen, Joint Staff/J-39 (moderator)
- Mr. Randy Cieslak (PACOM)
- LTC Lance Rasmussen (SOUTHCOM)
- Mr. Marty Drake (CENTCOM)
- Mr. Hap Harlow (AFRICOM)
- LTC Dave Creasman (I Corps)
- Mr. Ed Doray (NORTHCOM)
- LTC Brian Mellen (EUCOM)

Brig. Gen. David Béen, Joint Staff/J-39

Brig. Gen. Béen stated that we if we are in the information age, then the US military must be masters of information operations, right? Not necessarily. There are two reasons why. First, the military has a focus on kinetic and maneuver warfare as a primary way to fight. And when the military does try to incorporate information operations into its plans, it is sprinkled into the O-plan at the end instead of baked in. Some critics say the US military should not be trying to influence people's minds in the first place. So you can kill an adversary, but not mess with their minds? Some say the military should not be the face of the USG on the Internet. But as you saw with Putin in Crimea, he used all of his capabilities effectively. Last spring in Crimea, Putin was maneuvering forces, had political speakers carrying the party line, had academics blogging positively about it, and the news broadcast all supported the same line. Then, the Chinese are conducting unrestricted warfare.

In 2014, controlling information is vital to the nation's success if you want non-kinetic success. The COCOMs are facing these challenges daily. How do we counter an adversary that uses Twitter to target or Skype to do command and control—and what about actors who do not distinguish between state and private property online? Theft of private—and commercial—property online takes $300 billion out of our national economic power. And when do influence operations by nation states using cyber capabilities rise to a level of invoking NATO's article 5 actions? These

are the concerns that commanders are dealing with. He asked the Command representatives to talk specifically about the issues that keep them up at night.

Mr. Hap Harlow, AFRICOM

External actors, not Africans, largely shape the information revolution in Africa. Similarly, in many cases, the violent extremist organizations (VEOs) operating in the AOR are also shaped by external actor or borrow lessons learned from outside the continent. However, our understanding of the problems emerging from large data sets are skewed primarily for three reasons. First, because of the large African diaspora population outside Africa with more access and voice. Secondly, rich, urban young African Internet users skew the data as well. Finally, the vast majority of Africans do not have access to social media. Therefore, trends based on what we see in social media and large data sets are often not an accurate representation of how the information revolution has affected Africa.

When thinking about information operations, we have to ask ourselves whether we have the right tools for the mission. Regarding the correlation of information environment to security, we do not have a very good understanding of the environment in Africa and its underlying causes. The vast diversity, huge populations, and vast geography challenge our ability to identify fixable problems—particularly in the security sector. The gross lack of understanding results in oversimplification of complex problems that defy success with our current planning structure, authorities, and funding. Too often we find ourselves in a whack-a-mole problem.

External actors are seeking economic opportunities in Africa, which is approaching a billion people. These largely extractive investments are undermining activities, norms, and standards the USG is trying to reinforce.

The physical reality and material facts form the bulk of politics in the AOR and puts them into the "global others" category. Africa eludes stereotyping. We see contrasting scenarios from prosperity to conflict. Societal, economic, political, and security factors all influence the pace and form of the information revolution, but the velocity of change is slower in AFRICOM than in other AORs due to poverty, demographics, and weak institutions. These drivers of instability are well known and are not forecasted to change through 2025. Information technology, social media, and big data are not a large source of instability in Africa where the bulk of the population likes on less that $1.25 a day.

Demographics are very important in this AOR. There are nearly a billion people with many dialects. Our ability to understand data is related to context. Understanding the multitude of social and language dialects is a continuing challenge. There are three potentially destabilizing demographic trends of concern: rapidly growing populations, youth bulge, and rapid urbanization.

Our African partners are not asking for help with complex technologies. Only Morocco has asked for cyber security help. While we are trying to introduce command and control, we have not seen much success. Most countries want soldiers' gear, vehicles, etc.

Information operations in Africa rely mostly on shoe leather, not on the Internet. Our information operations campaigns are soccer balls and T-shirts. We rely on radio, which remains the #1 conveyor of information in Africa. It is a one-way system absent a good feedback loop.

Mr. Randy Cieslak, PACOM

One of the main challenges PACOM faces is the tyranny of distance, which covers half the world, mostly maritime. This AOR is hard to connect geographically as well as due to the diversity of cultures. Reaching people is very important in this domain even though information technology has not reached all corners of the AOR.

PACOM does not have a big alliance in this AOR. It has several significant allies. Japan is a hard ally to have because of its World War II history. We are making progress on a partnership between Korea and Japan though. The AOR also has despots like North Korea, China, and Russia (which is not technically part of the AOR but has influence there).

However, the information age has allowed PACOM to reach large populations over long distances. It allowed us to broadcast to populations that were unreachable decades ago.

Mr. Cieslak then discussed the challenges facing the information and acquisition efforts in the United States. He used four metaphors to describe the challenges:

1. "Not Invented Here" Each organization believes they have a special mission and requires a special information system. The result is many different systems that require extensive efforts to become interoperable. We would be better off if we had better integration resulting in fewer systems.
2. "I've Got a Secret" Information is power. Some organizations and personnel hoard information thereby depriving the enterprise of the ability to integrate information for greater knowledge. A related corollary is when we overclassifiy data that prevents us from sharing important information with our allies and partners. Most of the time this is because users do not know the sensitivity of the information that they hold, so they take the most conservative approach, which dilutes our collective situation awareness.
3. "Crabs in a Bucket" As soon as one program gets a break through, someone grabs the resources and pulls it down.
4. "It's Mine" or "This is my rice bowl." I am special, so I need my own resources. This is a different excuse to justify what I described in #1 above.

The USG acquisition system is not able to cope with the information age. This is our biggest impediment.

Mr. Edmund Doray, NORAD/NORTHCOM

Although the NORTHCOM AOR includes Canada, the US, Mexico, and portions of the Caribbean, we tend to say that we are the paranoid COCOM because we worry about everything: China, North Korea, Iran, cartels, trafficking, earthquakes in California, and homeland defense. The NORTHCOM team is as diverse as the challenges it faces.

NORTHCOM and NORAD face extremely challenging threats and also some opportunities. NORTHCOM has to rely on its mission partners. Its actions are also constrained by the US Constitution. The laws, policies, and authorities NORTHCOM must make sense of are immense. NORTHCOM also faces political and interagency challenges over resources and ownership of issues. There is great opportunity though to overcome rice bowl challenges to create an interagency campaign plan and share data, but this is currently hard to do on a regular basis.

For example, counterthreat finance is a great opportunity for information sharing not only within NORTHCOM's AOR, but across others. However, individual responsibilities, authorities, and information sharing challenges quickly bog it down. The biggest opportunity is to create an environment where we can share information in the open source and allow it to be leveraged and shared with a broad audience including individuals who want to conduct analysis in these areas.

Mr. Marty Drake, CENTCOM

Marty Drake is the Chief of Science and Technology Division and Command Science Advisor to U.S. Central Command located in Tampa, Florida. Directs a staff chartered to conduct discovery, research, analysis, and sponsor development of new and emerging technologies and techniques which have the potential to provide solutions to Headquarters and Component validated Joint needs. Additionally, pursues integrating and non-material solutions to satisfy current and future military operational capability gaps. Holds a Level III Systems Planning, Research, Development, and Engineering (SPRDE) qualification for Technology Management. Frequently lectures on technology impacts to the current and future military force.

Mr. Drake stated that as science advisor, he is a technologist that roams the globe looking for new approaches, techniques, and tools to make life easier and safer for those at CENTCOM. SMA is a gem in that regard. It represents the new way we all need to think about the challenges we face.

In Iraq and Afghanistan, we realized our adversaries were not playing by the rules of armed conflict. We could not describe it though. From a military standpoint, we are great at operationalizing something. But when you start talking about threat finance, proselytizing, infrastructure, lines of communication, etc., we suddenly realize that these issues are outside our comfort zone. We coined a phrase that it takes a network to defeat a network. That is what we are trying to do today.

What keeps the CENTCOM commander up a night are some pretty big problems. Somewhere in the data is the answer, yet we only seem to find it in hindsight. We need to move this discovery and analysis closer to the decision cycle. We can take huge data, extract information, create knowledge, and create understanding to yield wisdom.

Some in this room know where we need to go, but we need to step back to figure out how to work together to fix problems in a holistic manner. What frustrated CENTCOM is that we keep getting attacked from a swarm of ideas. We need to create proactive solutions that are extensible to other AOR partners. We all have the same issues. We have to take the decision cycle, analyze information in a cogent, knowing manner, and make better decisions. The problem we face today is how to use knowledge and how to use it to disadvantage our adversaries.

LTC David Creasman, I Corps

From an operational context, US Army I Corps is the only united assigned to PACOM but tied to FORSCOM. It must remain regionally aligned and globally responsive. I Corps has formed interagency partnerships to integrate assets to operationalize what PACOM wants us to do. We take strategic guidance from PACOM and tailor it into an operational requirement. We conduct phase 0 operations on a yearly basis.

While the diversity of the PACOM AOR is a challenge, we see a lot of potential for information sharing with joint partners in the AOR. We are working towards interoperability with our partners. Our main partners are South Korea, Japan, and Australia. We conduct exercises with them, but we operate on different systems and cannot share information. We need a common operating picture in the Pacific, which is a daunting task.

However, one way to share information is through persistent engagement. Country plans developed at PACOM go five years out. We operationalize the five-year plans and engage our partners on a regular basis.

One operation—Pacific Pathways—is work toward interoperability. It will take a brigade combat team and a mission command node and deploy it to 3 countries to conduct bilateral training and establish force presence across the International Date Line. We have to move at the speed of our partners. It is not just about building military-to-military relations. We have to consider what our partner countries want to achieve. And we have to acknowledge that military and national government desires may not align.

We also have to think about the way we do war. We used to say that we never go to war alone. Now we should take that further as say that we will never go to war alone as a military.

LTC Lance Rasmussen, SOUTHCOM

The information age provides opportunities and challenges. In DoD, policy is not keeping pace with the rapidly changing environment. SOUTHCOM wants to do a lot more to engage with foreign audiences at the strategic level. So we created a military-to-military website, Dialogue, that allows us to share information about engagement and regional exercises with our partners.

Every COCOM has a strength. SOUTHCOM's is engagement at the partner nation level as well as working in the unclassified domain. It takes a network to defeat a network and that is particularly true with regard to SOUTHCOMs countertrafficking mission. JIATF-S networks with US Government, Interagency and Partner Nations by sharing unclassified air and maritime tracking information.

Information sharing by itself is not a technology; it is a social and cultural behavior that has to be learned. How do we develop the right capabilities to share information? When we share information, we can weed out those maneuvering in an illicit manner. It is a challenge because in the DoD, we communication on NIPR, which is not truly unclassified. Having a collaboration site, like APAN, helps share unclassified information but it is not a command and control tool and provides no common operating picture.

SOUTHCOM needs to address the unstructured data mining challenge. For example, look at how we assess anti-American sentiment. Often, operations and exercises unintentionally create negative stories in the media. Social media picks up on these cues, which are of great interest to current SOUTHCOM operations.

LTC Brian Mellen, EUCOM

EUCOM's responsibility is the global nexus for culture, communication, and ideology. Europeans are increasingly using the Internet to influence one another. Europe is a close second for Internet penetration rate after the US. That makes it vulnerable to terrorist information operation campaigns.

Alternatively, the annexation of Crimea and the Ukrainian conflict represents the most amazing information warfare blitzkrieg we have ever seen. EUCOM wants to message at risk populations, disrupt information operation campaigns, etc. EUCOM is seeing three trends: increasing use of mobile devices, social network, and programmatic targeting.

EUCOM wants to leverage traditional military support and information operations to provide effective means to counter adversarial propaganda. Social media is a great tool for influence, but there are some issues in implementation—such as constrained resources. EUCOM's main operation, Assured Voice, is only allotted $3 million. Russia spends $15-20 billion per year. We are constrained by authorities.

There are several problem sets:

- increased budget constraints;

- who does EUCOM engage with for a whole of government response?
- how to work with NATO partners to counter terrorism; and
- how to optimize NATO command element to react to a new security environment.

Discussion

Many of you touched on idea that big data poses problems for the decision maker. There are many people ready help, civilians who can act like an army of microtasking volunteers. They can sort through imagery, translated, etc. People lack a challenge. This community could help with disaster response or any other mission. I know there are issues with this idea, but a crowd can be leveraged to do these things. They can help verify data. Are there any potential points of collaboration?

Mr. Cieslak responded that PACOM does a lot of disaster relief work and it does welcome community help. The challenge is that classification issues bind the DoD. That is the biggest challenge. The reaction to Snowden was to classify more, but to really take advantage of existing resources, we have to minimize classification.

I am a social scientist who works in the field to help commanders use complex information. Information operations were the biggest problem set. Half of the battle is in targeting the right solution and achieving positive effects. To do this, commanders have to conceptualize the information. What theory of information is the DoD using? Our enemies, particularly jihadists, understand information in a completely different way than we do and they dominate. We are hampered by our legacy of information science. However, insurgents understand that information is about community trust and collective will formation. We cannot understand or find value in big data unless we move away from the information paradigm.

Mr. Drake responded that the US does not have less of an understanding; the two sides are playing different games with two sets of rules. They have no rules; we do. They are not better; it is just that we are hampered by policy, authority, and other issues. For example, CENTCOM may have a capability, but if it does not have a mission and the authority, it cannot use its capabilities. The adversary does not have to play by those rules.

Does EUCOM have a Twitter feed or Facebook account? Are we enabling Ukrainians? We can put out messaging through public affairs.

LTC Mellon responded that Twitter users in the Baltics receive Russian satellite TV. They speak Russian. We want to use social media to send messages to particular population segments.

Brig. Gen. Béen said that ISIL tells fighters they will take good care of them. But when they arrive, they find they are treated horribly. There is not enough food or ammunition. Would it not be nice to get ahead of their messaging rather than reacting? Why cannot we go online and stop cyber activity?

Mr. Marty Drake responded that it is an away game but played with home rules. We have to get into their ballpark and play and we do not have permission to do that.

Brig. Gen. Béen concluded that it has been interesting that some AORs want soccer balls for influence/information operations, and others want Internet and mobile apps. Information operations encompass all of this. It is the smart way to fight when we do not want to get into a kinetic war. We are not going to win an asymmetric war with ISIL if we stick with kinetic effects alone.

Panel 5: The Intersections of Big Data, Neuroscience, and National Security: Technical Issues, Derivative Concerns

This panel's objective was to define how big data approaches are vital to the operationalization of neuroscience and neurotechnology (neuroS/T); describe exemplary scenarios that will require the harnessing of big data methods and tools to engage neuroS/T in operational settings; and address the technical, epistemic, and ethico-legal issues arising from convergent neuro-cyberS/T and big data methods, as relevant to optimizing effective and sound national security and defense operations.

Panel members:

- Dr. James Giordano (Georgetown University Medical Center)
- Dr. Diane DiEuliis (HHS)
- Dr. Jason Matheny (IARPA)
- Dr. William Casebeer (Lockheed Martin)

Dr. James Giordano, Georgetown University Medical Center

Dr. Giordano discussed the reliance of neuroscience upon large-scale data engagement and how big data could be of high value to both advancing the validity and applicability of current and near-future neuroscientific and neurotechnological approaches in national security, intelligence, and defense. There have been significant advances made in the field of neuroscience. Translationally viable tools and techniques including anatamo-physiological correlation, individual trajectories of expression, and population variation and pre-dispositional assessment have been developed. Assessment technologies (various forms of neuroimaging, neurophysiological recording, neurogenomics and genetics, neuroproteomics, and neuro-cyber informatics) and interventional technologies (cyber-linked neurocognitive manipulation, and brain-machine interfaces [BMIs], etc.) that are also reliant upon large-scale data and/or advanced computational capabilities have also continued to develop.

Integrative scientific convergence (ISC) in neuroscience conjoins natural and physical sciences, biotechnology, and the social sciences to focus upon assessment, access, and affecting neural structures and cognitive, emotional, and behavioral functions in both individuals and groups. ISC is highly reliant upon data integration, sharing, and use (see Giordano, 2012 for detailed description). In short, neuroscience may have "put the brain at our fingertips," but neuroscientific information and the insights—and capability—it yields will not be operational to the extent needed for national security, intelligence, and defense without the scope and depth of informational use that will be afforded by big data approaches.

Neuro-cognitive intelligence (NEURINT) is a new dimension of neuroscience that employs a range of approaches to gain descriptive and potentially predictive insights to possible neurobiological aspects of cognitive and behavioral processes underlying and explicit to human emotions, decisions, and behavior (for overview,

see Wurzman and Giordano, 2014). NEURINT provides insights across domains, levels, geographic locales, time, and groups. However, this new dimension is highly reliant upon multiply tiered data acquisition, integration, and availability for use and, thus, necessitates an ever-expanding set of data gathering, sharing, and assimilation tools and techniques. Big data approaches will be vital to both developing and expanding NEURINT on operationalizable scales. But the use of tiered, large/vast data arrays, as pursuant to and/or incorporated in a big data framework also has a number of important caveats. First, if data are assessable, they are accessible. Second, if it is tagged, it is targetable. Third, if it's stackable, it is hackable. Fourth, what is hackable is manipulable. Finally, what is controllable is corruptible.

However, these caveats should not retard research and development of NEURINT-type methods that could be of value to national security and defense initiatives. Rather, such caveats are precisely that—warnings that are of sentinel value to prompt devoting time and resources as necessary to establish systematized, secure, and sound approaches to neuro-cognitive data acquisition, integration, storage, analysis, and retrieval. Potential neuroscience and technology influence and deterrence scenarios include accessing neural systems/brains to mitigate/control social violence and "protect the polis." What we can do is provocative, but what we *should* do and how we should do so remains contentious, and at issue.

In the main, it is important to recognize that if/when attempting to operationalize neuroscientific and neurotechnological approaches within massed scale data architectures, a number of potentially ethical and legal issues can—and likely will—arise. These include a perceived inviolability of "mind" and "self;" need to balance protection vs. privacy; incentives for mitigating violence vs. perceptions of "mind manipulation;" the validity, reliability, and admissibility of NEURINT-type information; and if and how such data can and should be assessed and perhaps used (to affect influence over individuals' and groups' cognitive, emotional and behavioral states—for example: hostility, disgust, arousal, aggression, violence) in light of pluralist socio-cultural diversity in norms and mores. Addressing these tasks, issues, problems and solutions remains a focused priority of Dr. Giordano's working group.

References cited:

Giordano J. 2012. Integrative convergence in neuroscience: trajectories, problems and the need for a progressive neurobioethics. In: Vaseashta A, Braman E, Sussman, P. (eds.) *Technological Innovation in Sensing and Detecting Chemical, Biological, Radiological, Nuclear Threats and Ecological Terrorism.* (NATO Science for Peace and Security Series), NY: Springer.

Wurzman R, Giordano J. 2014. NEURINT and neuroweapons: Neurotechnologies in national intelligence and defense. In: Giordano J. (ed.) *Neurotechnology in National*

Security and Defense: Practical Considerations, Neuroethical Concerns. Boca Raton: CRC Press.

Dr. Diane DiEuliis, Department of Health & Human Services

Dr. DiEuliis discussed the intersections of big data, neuroscience, and national security and their technical issues and derivative concerns. Small neuroscience data can be made meaningful on the large scale. Studies from genomics, molecular/cellular, individual neurons, physiology, etc. show that at the individual level of the neuron there is very high complexity. Using big data computational methods, the goal is to summarize the activity of a large number of neurons (reducing the number of variables), so that more generalized behavior can be observed and predicted. For example, looking at healthy vs. diseased brains for large-scale observations of movement, behavior, etc. can be translated to generalized behavior in various scenarios. She referenced the idea of "dimensionality reduction" (Cunningham and Yu, *Nature Neuroscience* **17**, 1500–1509, 2014) where the goal is to go from neural similarly to semantic similarity. Dimensionality reduction is not a new idea, but is relatively recently applied to the neurosciences. The challenges in its application include not just reducing dimensionality, but to find the right dimension to reduce to, and further, understanding the comparative level of what is actually meaningful. In terms of neuroscience, the most meaningful yardstick of measurement in that regard is behavior, and having the ability to understand, and potentially predict population regularities in behavior.

In disaster preparedness and response, the human element is key in determining the outcome, or ability to recover. Prosocial behavior can be a useful yardstick to explain what underlies whether a person decides to help or withdraw from helping. This can then extend to what promotes successful recovery from disaster events Research into prosocial affectors has found that individuals who carry a genotype associated with higher anxiety (as dependent on serotonin levels) are less likely to engage in prosocial behavior; mitigating anxiety would then be a key factor to focus on in such a population. Additionally, media programming/narratives that contain acts of altruism leading to positive outcomes affect a viewer's likelihood of prosocial behavior and social media is frequently used as a catalyst for emotional and financial support in disaster scenarios. There is a belief that prosocial behavior is the behavioral "default," and that without other affectors, people behave in prosocial ways.

Dr. DiEuliis concluded by noting a point about the relationship between resilience and stability, which is something that was discussed earlier in the conference. Resilience is tied very closely to stability. Resilience was noted as the ability to absorb some kind of shock and is frequently measured by how quickly or easily a population or state can return to a level of "normal" after the shock. The inability to absorb a shock, whether naturally occurring or man-made, could have significant effects on overall stability. West Africa's inability to handle Ebola is a clear example. West Africa has very low level of resilience to the significant health threat that Ebola

has posed—the health systems within the countries affected are unable to manage the complex health needs of a tier one viral hemorrhagic fever. The sequelae from a lack of health system resilience to Ebola are now fundamentally threatening the stability of those countries, including food shortages, the creation of an at risk orphan population, travel and trade concerns, etc. These represent clear national security concerns that go beyond the primary "resilience to Ebola" capability or lack thereof. Thus, there is a strong relationship between stability and resilience that warrants consideration.

Dr. Jason Matheny, IARPA

Dr. Matheny discussed IARPA's Open Source Indicators (OSI) effort. The goal of OSI is to develop and test methods for continuous, automated analysis of publicly available data in order to anticipate and/or detect significant societal events including disease outbreaks, political instability, and political elections. OSI works to "beat the news" by fusing early indicators of events from diverse data. OSI's approach consists of a three year forecasting tournament where research teams train machine-learning models to detect patterns in publicly available data that have historically preceded societal events. Teams are evaluated on the accuracy and timeliness of forecasts they deliver about real-world events in Latin America, the Middle East, and North Africa. Examples of successful forecasts from the OSI effort include riots after impeachment of Paraguay president (2012), the "Brazilian Spring" (June 2013), Hantavirus outbreaks in Argentina and Chile (2013), Venezuelan student uprising (Feb 2014), and recent elections in Panama and Colombia (2014).

Dr. William Casebeer, Lockheed Martin

Dr. Casebeer discussed operational applications and issues in big data techniques for neuroscience and technology in national security, intelligence, and defense. With the right kind of science and technology, we might be able to operationalize neuroscience and technology in the context of big data.

What kind of data is available?

In the context of neuroscience and technology in national security, intelligence, and defense, there are three primary types of big data: behavioral data, psycho-physical data, and neuro data. With respect to behavioral data, the information revolution has revealed massive amounts of this type of information. Psycho-physical data can be used to help connect neurobiology mechanisms to behavior. Neuro data incorporates the use of the traditional tools of the field of neuroscience. Significant progress is being made on all three of these types of big data. More and more of this data is becoming publically available and research groups are leveraging the data to make interesting advances.

What can you do with this data?

Big data related to neuroscience can be utilized in shaping and deterrence type activities. Shaping involves thinking about how environments interact with brains. In deterrence it has been found that sacred values play an important role.

Neuroscience data can help understand both how environments effect the brain for shaping activities and what values are sacred to someone or a group to influence deterrence decision making.

Technical Gaps

Many technical gaps exist in the field of neuroscience and technology. Additionally, the field is one in which many claims are made that are not always scientifically supported. Three main things can be done to help close some of the gaps in the neuroscience and technology field. First, neuroscience and technology has a small end problem and to close this gap we need to build technologies for crowdsource cognitive neuroscience technologies and the right kinds of equipment. This will require low cost equipment that allows for control of the environment to eliminate traditional sources of error. A standardized test environment is needed and this is where industry could play a role. Second, we need to establish the correct kinds of test-beds. We need the right types of labs equipped to rapidly assemble test populations. Currently, some labs like this exist, but hopefully something will spur the development of more of these test-beds. Finally, we need the framework and equipment to make ourselves visual to our machine partners in this enterprise. Given big data, there is no way a human or team of humans will be able to sift through it all or make use of it in tactical situations without assistance of a computerized assistant.

Panel 6: Understanding Social Systems in Phase 0: Human Geography, Big data v. Micro information, and the RSI Paradigm

This panel discussed how Combatant Commanders (CCMDs) contextualize social, infrastructural, and environmental information for effective planning and decision making. It also addressed what impact the Reconnaissance, Surveillance, Intelligence (RSI) Paradigm has had on CCMDs.

Panel members:

- Dr. Charles Ehlschlaeger (ERDC)
- Dr. Jean Palmer-Moloney (USACE ERDC, NGA)
- Dr. Val Sitterle (GTRI)
- Mr. Kalev Leetaru (Georgetown University)
- Dr. Jen Ziemke (Co-Founder & Co-Director of the International Network of Crisis Mappers)

Dr. Jean Palmer Moloney, USACE ERDC, NGA

Dr. Palmer-Moloney discussed the context of data and the various perspectives data can provide. The context of data is what geographic combatant commanders focus on most frequently. Data can come in various different forms and provide important insights into factors like location, place, region, movement, and human-environment interaction. Location data can be absolute, which is found using grid coordinates, or relative, which is found with respect to other features (north, south, east, west, near, far, etc.) to orient position. Place data provides the physical and human characteristics that make a specific location unique. Region data provides information on physical and human regions to connect places with similar characteristics. Movement data provides insights into how people, ideas, and earth elements move. Human-environment interaction data provides insights into how people impact the environment and the environment impacts people.

Visualizing the themes of geography can be quite varied. There are many ways to model the information collected including using points (pairs of x, y coordinates), lines (sequences of coordinates), polygons (closed sets of coordinates), remotely sensed images (from space and air platforms) displayed as pixels, and other images (jpg, png, tiff, pdf). However, most frequently the two-dimensional map is the method used for modeling the world. Currently, NGA with help from other partners is working on the GEOnarrative Method to create interactive story creation/telling tools for analysts and decision makers. NGA has been working to apply the GEOnarrative Method to understand the current West Africa Ebola crisis and its human security implications.

Dr. Charles Ehlschlaeger, USACE ERDC

Dr. Ehlschlaeger discussed SMA's *Megacities – Reconnaissance, Surveillance, Intelligence* (M-RSI) effort in support of USPACOM. The M-RSI effort augmented USPACOM's two frameworks for organizing and understanding information and knowledge required for planning, assessing, and providing situational awareness to phase zero operations. The SMA team aligned social, infrastructural, environmental, and political needs to USPACOM theater campaign plan objectives. Ultimately, aligning the framework to USPACOM mission objectives allowed the SMA team to provide metrics for issues that are operationally important to USPACOM.

The M-RSI effort created and mapped original socio-cultural information by combining multiple open source inputs that traditionally are not used. Urban Security Maps aligned to the needs of USPACOM's Socio-Cultural Analysis Team. In addition to "place-based mapping", the effort mapped neighborhood and regional connectedness to understand population mobility and its communicative ecology. Urban Security Connectedness Analysis provided automatic measures of what regions and neighborhoods have regular travel between them. These techniques can be run with any geotagged social media information.

USACE ERDC is also working to connect meta-narratives to media events by mapping the ideas of social groups to geographic locations. For communicators, this will help identify important target audiences and understand how they are connected. For analysts, this will provide real time information on information flow and key organizations not only within each cultural group, but also for each relationship between cultural groups. These mapping techniques take Global Knowledge Graph (GKG) events into weighted directed graphs to derive social group influence. This last research topic is still in its preliminary phases.

Dr. Val Sitterle, Georgia Tech Research Institute

Dr. Sitterle discussed the importance of having the correct information in the correct places at the correct time across all agencies that are operating. When analyzing a problem, it is crucial to begin by defining the purpose, perspective, and process to make the best use of available information and have effective intelligence. The distinctions between what problem you are trying to solve and why it is important to you drives what kind of intelligence is needed, why it is needed, and who needs it. RSI models, analyses, and processes to support one COCOM need often do not readily translate to effectively addressing other needs.

Dr. Sitterle also highlighted the importance of understanding perspective and its impacts. We need to understand how information that is available and its context influences the actions of various actors in theater. For example, many information technologies exist that automatically limit what data given users can access based on clearance levels. Such processes exacerbate the challenge of having multiple perspectives across various groups driving their actions as they operate in parallel even if not collaboratively in the same theater environment. The potential impact of

disparate perspectives therefore requires re-envisioned concepts of interoperability and understanding how this may change our vulnerabilities and hence actions.

Systems are constantly changing. In models to support analyses, what constitutes an element will change; what constitutes a relationship will change; networks and the very nature of what is licit versus illicit will change; phenomena that drive or otherwise significantly impact the system will change. Traditionally, researchers produce frameworks and models that are matured into computationally supported analysis engines. Then, the focus shifts toward getting the new "tool" into hands of operational analysts while the researchers exit the process. The evolution of the systems we need to understand, however, renders this prior approach ineffective. The system will change too much in nuanced and connected ways that may be critical to operational understanding for these viewpoints to be sequentially delineated in the future. Collection, model development (modification), and analysis should work in parallel—each informing the other. The relationship between research and operational analysis communities needs to evolve new collaborative and supporting processes that translate effectively and efficiently into RSI needed by the COCOMS.

Dr. Sitterle concluded with three takeaway points. First, there is a distinction between frameworks to integrate analyses and supporting modeling and simulation (M&S) in order to confer understanding and inform analytical products and frameworks to organize and plan intelligence derivation and dissemination to support operational needs. Failing to devote equal effort to the latter will create RSI message dissonance. Second, self-context is just as critical as analytical context. Defining what problem a COCOM is trying to solve and why will drive the design of effective and efficient RSI information derivation and dissemination to support those needs. Finally, uncertainty, ambiguity, and surprise will persist. We should therefore expect surprises and failures in our predictions. Resilience, even in RSI, means rapid and flexible response and recovery.

Mr. Kalev Leetaru, Georgetown University

Mr. Leetaru discussed the GDELT project. GDELT is a global societal-scale real-time dashboard that consists of global event databases, global knowledge graphs, and global interactive maps. GDELT works by scooping up world media in real time. It combines Google translation with machine translation and scoops up a massive fraction of the world's media to 1) construct catalogues of everything important in the world media each day and 2) couple that material to help create global knowledge.

GDELT allows user to create live interactive maps. The powerful part of data likes this is that it shows micro-level material from every area of a given location. GDELT has created live interactive maps for the Ukraine and Boko Haram activities in Nigeria. GDELT can also go beyond physical activity to influencer maps. This can help identify influential people, media, political, elites, etc. within an area. These maps can be scaled globally to watch how global influence is changing throughout

the world. Furthermore, GDELT can identify global emotions and themes from media. For example, with respect to Ebola, we can track how global emotions evolved as the Ebola outbreak progressed. What we have seen is that the mainstream media has been very level headed but social media has had a much more extreme reaction. Ultimately, the goal of GDELT is to fuse together all information available in the open source.

Dr. Jen Ziemke, Crisis Mappers Net

Dr. Ziemke discussed using big data to actually generate insight and knowledge. There is a gap in a way between the micro-level volumes of data being collected and the deductive reasoning piece, which creates the grand theories. Something is missing. What is the connective piece between data collection and deductive reasoning? It seems like it would be a level of decision-making used to make sense of everything. We do not collect data on or understand that middle level as we should. We need to look more closely at how decisions are being made.

Many people can be considered experts, but often time we lose important insights because the right people, often people not labeled as an expert, are not being tapped. Twitter exists, but it does not ask what people are concerned about. If a portal existed where people could be asked about their experiences and concerns, it would enable us to collect a different kind of data. This would be somewhat like second order data. If there were a place where we could share our hypotheses, hunches, concerns, worries, etc. without having to set off alarm bells it would be very beneficial. If there were better places where people could provide this type of information it could provide us with great utility. People want to help. People want to provide their insights. If we started at the meso-level and worked up, this type of information could help inform us at the strategic level. It would also help provide further insight into potential patterns.

Discussion

With the technology containments that exist in terms of data display, what is the hardware solution to bring these types of tools into the hands of the users?

Mr. Leetaru noted that there is great interest in this area, however it is important to not go down a path of shiny new object syndrome. The GDELT project has been working with USIP to build a fusion center to combine multiple technologies. The USG needs to become more innovative. Some of the most innovative things happening in the United States are taking place in the corporate world. The USG could learn from how corporate companies fuse their data and tools together.

Dr. Palmer-Moloney noted that NGA is looking into ways to work with the J2 to have support teams share information. The GEOnarrative tool has been created in an unclassified environment so information derived is easily accessible. Getting these types of tools into the end users is also heavily tied to education because if you don't

know how to use or understand the tools then you will never even begin to start looking for them.

We have to find an onramp for information technologies to get into our educational military institutions. We need to educate military scholars to being talking about these technologies so they can then move those technologies into workflows and operational environments in ways that make sense. USSOCOM is currently developing a research test bed that will allow researchers and operators to play with tools to determine what is effective and operational.

Dr. Sitterle noted that training this type of community of scholars will help create a next generation that understands just because you can combine these types of simulations doesn't always mean that you should.

How are you able to evaluate, validate, and verify the quality of the data itself within the systems developed?

Dr. Ehlschlaeger noted that data will come in many different levels, but it is important that all information also comes with meta-information that specifically defines how trustworthy the data is and where it applies. As a geographer, it is often worrisome when data vaguely states where and when it is from because people may use the data in an inappropriate manner. The metadata is critical.

Dr. Ziemke added that the crowd can be leveraged to help verify its own content. In a crowd sourced environment, we can look at numbers of accounts talking about something. Additionally, the crowd also often has a self-correcting mechanism.

Dr. Palmer-Moloney noted that in addition to understanding confidence levels, it is important to understand that very good data can sometimes be at a scale that is inappropriate for a given analysis.

Panel 7: Implications of the Speed & Global Reach of Information on DoD Missions II: Effective Deterrence and Influence Strategies

This panel explored the implications of what we have learned about increasingly rapid availability of large and micro data for the ability of the US government to influence world affairs. Issues considered included: What will be the impact of instantaneous, global communications on the effectiveness of US deterrence messages? Is "universal messaging" inconsistent with the idea of "tailored deterrence"?

Panel Members

- Mr. Hunter Hustus, USAF/A-10, co-moderator
- Dr. Allison Astorino-Courtois. NSI, co-moderator
- Mr. John Rendon (The Rendon Group)
- Dr. Amy Zalman (World Future Society)
- Dr. Bill Casebeer (Lockheed Martin)

Dr. Allison Astorino-Courtois, NSI

In order start on the same page, Dr. Astorino-Courtois asked the panelists to focus brief opening comments on what their disciplines suggested about deterring people from acting in line with ISIL messaging campaigns. By way of background she cited a recent article in *Politico* that reminded us that ISIL was virtually unknown by the American and European publics before this summer when the news was dominated by the brutal beheadings. According to the article, public polls show that the beheadings are the best-known news event in the last five years, and that after the beheadings, public support for US action in Iraq and Syria increased from 36 to 60 percent. Arguably, the same violent message also helped it recruit up to 20,000 fighters. The SMA effort for SOCCENT is looking at the intangible sources of ISIL's appeal. One finding was that success in and of itself was a potent source of support and sympathy; success breeds success.

Mr. John Rendon, The Rendon Group

The pivotal question is what is the strategic imperative? When we look at ISIL, the strategic imperative is to make sure that our actions, whether operational or informational, do not enhance our potential adversaries. We need to particularly focus on deterring young people under the age of 25.

When thinking about who we message, we have to first ask: who is "we"? US partners overseas are the worst messengers in the space. The USG should not message unless it is the last resort. We need third party validators, especially those under the age of 20.

What was striking about the Foley beheading was that it presented a strategic vulnerability for ISIL and a huge opportunity for the West, given that the best messengers in this space are the brothers and sisters of victims of violence by these kinds of groups. The siblings that already have a talent at speaking out should be trained and sent out on the information front to target the terrorist that killed their loved one.

In thinking of ways to respond to ISIL, this might be one situation where you want to bring your kids to work. Describe the problem to a group of teenagers on the unclassified level. They know more about platforms than any contract you can hire. There is a generational fault line. If we do not get to the population under 20, the math works against us. It is important to understand the mediums they are using and what they get out of it.

Dr. Amy Zalman, World Future Society

Dr. Zalman said it distresses her that we are asking this question in the same syntax as we did 15 years ago: What should we be doing to group X with jihadist intentions? The USG has failed to institutionally integrate the answer to this question. First, do not make assumptions about the group's religion. Labeling something as religious that we do not understand in the first place does not help us answer the question about what the group's specific motivations are. People do things in the name of religion: good things and bad things. The point is that we know very little about ISIL and we have already labeled them without understanding.

Second, we talk about ISIL's messaging using marketing terms, which is not terrible. We are all objects of marketing all the time. We should assume that our adversaries are as complex and conflicted as we are. If we can get to them in small demographics, we will be more successful.

We should not be surprised that non-state actors acting on a multifocal information landscape. Bill Gates in a non-state actor and so are NGOs. Why do you think ISIL is going after state status? Why is Scotland? The nation state is still a good brand.

We do not understand the concept of narrative well at the institutional level.

Dr. Bill Casebeer, Lockheed Martin

Bill Casebeer is a Research Area Manager in human systems optimization for Lockheed Martin's Advanced Technology Laboratories, where he leads science and technology development programs to improve human performance in the intelligence world, cyberspace, and piloting. Bill served as a Program Manager at the Defense Advanced Research Projects Agency from 2010-14 in the Defense Sciences Office and in the Biological Technologies Office. He retired from active duty as a US Air Force Lieutenant Colonel and intelligence analyst in August 2011, where he earned multiple Distinguished Meritorious Service medals. He holds a Bachelor of Science in political science from the US Air Force Academy, a Master of Arts in national security studies

from the Naval Postgraduate School, a Master of Arts in philosophy from the University of Arizona and a joint PhD in cognitive science and philosophy from the University of California at San Diego.

We have to create a preliminary framework of analysis before we can start to answer the question of how to deter ISIL. Groups like ISIL are essentially violent social movement. The literature on violent social movements says that to be successful, a group has to 1) lack of perceived opportunity for political discontent, 2) have mobilizing resources (arms, money, etc.), and 3) have a resonant frame that is justice oriented.

If you look at the deterrence literature, we know there are several dimensions, general to specific, that set conditions for how to generally deter. Deterrence can be achieved through denial and punishment. For example, the USG could attack ISIL's ability to behead victims. When the attack is effective, it might deter ISIL from doing it again (denial). Punishment does not take away the ability to behead, but makes the price so steep that ISIL would choose not to do it.

We have to look at motivational factors from irrational to affective including classic cost/benefit analysis that large organizations like to make.

The information operations framework includes doing things like identifying target audiences all the way up to developing information series that could be assessed for affect. If you consider how groups form, deterrence theory, and how information operations are carried out, we can have a semi-comprehensive conversation.

We are in some respects not well poised to deliver messages in southwest Asia, and need to cultivate alternate, trusted voices that resonate strongly with recruits (as well as the justice one does which is being told by violent non-state actors in the region). We need to shake the environment so stories that exist motivate less—move them to an alternate social network and stop them from hanging out with vulnerable populations. We also need to shake the environment in such a way that causal factors that contribute to violent mobilization are less efficacious particularly to those related to justice.

Moderated Discussion

Mr. Hustus opened up the discussion session with one observation. Yesterday, several people indicated that we are all here because we are part of Dr. Cabayan's network. That is true, but we are also here because complex problems are a narcotic; we love them. Yesterday, panelists emphasized that we need to solve the right problem and we need to control the narrative. This panel discussion could help determine how to go about doing so.

Mr. Rendon noted that in too much of the world, we are a poisoned well when delivering messages. Dr. Astorino-Courtois then asked whether our actions and inactions were not also messages?

Dr. Casebeer responded that our actions and inactions are indeed messages. Influencing how a message is received is about much more than offering an alternate message. It is thinking about the world view the audience will filter our actions through independent of our message. Words and deeds are equally important. First, they must be synchronized. Tactical considerations may require us to do things that undermine our words, so we need to let other trusted voices spread the message for us.

Mr. Rendon stated that if you look back to research conducted in 2001-2003 in any country with a Muslim population, the youth felt that the USG looks at them but does not see them. It talks to them but does not listen. They admire US technology, but it does not share them. The USG believes in democracy in its own country, but not in theirs. The street was calling for recognition, respect, hope, and opportunity. That was Tahrir Square. Other countries and cultures need to be able to look at the same information we are because they will see things differently than we do, which will generate knowledge and insight.

Dr. Zalman added that the USG tends to think of actors, states, and groups as having one identity or role, but they have several. The US is not trusted on one level, but may be trusted on another. It is complex and multilayered. This is where network building offers opportunities: the ability to produce communities based on roles and identities. There are many opportunities to create networks and use what we know about what influences to create coalitions with divergent narratives in them. We can create group of people within a particular age group that shares common interests: hope, career, community building, even religion. There are messaging opportunities, but that has to be done outside official pathways.

Mr. Rendon stated that the operational art has shifted. In a framework, we would create dots, line them up, assemble them and then hit the intended target over the head and then wonder why the audience did not like it. We need to put the dots into play and allow the audience to connect the dots and they will do it on their own.

Dr. Casebeer stated that he was not comfortable with the objective of "controlling the narrative." We need to take biology seriously and the experiences of individuals seriously. Instead of controlling, we need to think about having analysis that allows us to reach an inflection point where we can cause a phase shift.

One participant challenged Dr. Casebeer's conclusion. He asked Dr. Casebeer to explain why Russia is so good at controlling social media.

Dr. Casebeer responded that what you see in Crimea today is the result of 500 years of Russia shaping the environment. Do not look at the IO campaign and think you have seen the whole forest.

Mr. Hustus added that some parties welcome even the shallowest excuse to buy into a story and it does affect our ability to get the public behind our narrative. We have lost some precision on the effects we want. We confuse persuasion and prevention. Ideally, what we want to do is create a narrative so that when something happens, the person or group feels the negative consequences from his own community. These effects need to occur without the USG ever putting its face on it.

We have lost some precision on the effects we want to occur. We confuse persuasion and prevention. Ideally, what we want to do is create a narrative so that when something happens, the person or group feels the negative consequences from his own community. These effects need to occur without the USG ever putting its face on it.

Dr. Zalman responded that context matters. Some of the areas where ISIL is most active are areas that have experienced extreme violence in the last decade. There is a culture of violence that has been present there for a long time. Whatever is being done to others in ISIL's name needs to be understood within this context. Non-government sponsored public diplomacy is a great model (e.g., J. Christopher Stevens Fund). The Fund fosters extended high school exchanges between schools in New York and Casablanca. The two schools will study major problems like river health for an extended time. The basic idea is that people with longer familiarity will come to understand one another. Guided virtual interaction is almost as good as real interaction.

Dr. Astorino-Courtois noted that it seemed that the group had convinced itself that it needs to think carefully, or better yet, cease and desist on the idea of discrediting or countering narratives and perhaps even messages.

Mr. Hustus responded that we need to conduct state-to-state strategic dialogue. We need to make general deterrence specific. That is the effect of modern communication. How do we think about long-term deterrence and assurance?

Mr. Rendon added that the USG has to make space on the team for everyone. If you have partners and give them a specific assignment, that covers assurance. Deterrence is fascinating because everyone agrees we have a credibility deficit. So if you know the audience does not believe what we say, that is really important. However, if the audience does not believe what we say and we use words wisely, we can take them to where they already want to go to create a set of behaviors that lead them to a place where they cannot win. The structural framework is creating political transaction costs for political behaviors that work against them. If we know where they are likely to go, it provides opportunity.

Dr. Casebeer asked how deterrence is different for the leadership versus the population? It might be that for a committed and resolute leadership that we are stuck thinking about specific deterrence by denial and punishment and that efforts at shaping the environment would not work well. Rational actor theory is good

intellectually, but rationality is an achievement, not a necessary characteristic of individuals going about daily life.

Dr. Zalman stated that this is the point in the narrative where the audience's expectations and leading people where they want to go intersect. The reason why certain people want to go to places is because they have preconceived expectations for how to read small triggers. Underneath these expectations are cultural narratives. That is why 16 year olds are an important place to start with new or revised expectations. Narratives are about understanding what the audience expects of you in a particularly moment. We can play in that. It would be interesting if the US could surprise audiences with regard to their expectations sometimes.

Dr. Astorino-Courtois summarized that what the panel is saying is that we should not try to control the narrative, but try to use it.

General Discussion

We do not have to counter narratives if there is a strong narrative out there.

Mr. Rendon responded that what is fascinating is that we often talk about our narrative, but this has to be about their narrative. This is not about counternarratives. The US message is our narrative. It is not a battle of narratives. We need to create a space where they battle their own narrative. We cannot engage in that debate or we establish a raison d'etre for the adversary.

The third rail here is domestic messaging. We spoke yesterday about US persons and controlling the domestic narrative. How do we message our own audience given decreasing education, narratives from gaming and Hollywood, and the 16 and under crowd? Should the DoD have a role in domestic messaging?

Mr. Hustus stated that yesterday someone acknowledged that we have restricted networks and organizations. This is not just a classification issue. We reinforce the microcosm.

Mr. Rendon said one alternative is to look at the audience in the target country through the eyes of a domestic diaspora community. You want to make a difference through indirect messaging. Let USAID and State take the lead, particularly for issues like Ebola. Encourage a member of Congress that represents a diaspora community to do briefings with that community in the US without media coverage. It will be tweeted and blogged about, but if you try to control the message, it will fail.

Dr. Casebeer stated that the comment about creating alternate social network that fills the vacuum of the government not stepping up to the plate is important. It is

connected to the rentier relationship; it is not a dignity relationship. Shifting that relationship involves setting up transactions that are dignity oriented.

Mr. Rendon stated that he was working with law enforcement in Boston. There were a ton of kids hanging out on street corners. One long night when he was out with a Sargent from Dorchester, he wondered why the cops did not do anything about it. He said that if they are on the street corner, at least he knows where they are. If we ran them off, we would be responding to calls all night long.

With regard to toxic branding and poisoned well, it might be instructive to look at brands that lost credibility and then gained it. Think of Jack 'n the Box restaurant and Pintos. Both were good brands until a disaster (poisoned food, exploding gas tanks) and then no one wanted to be in a Pinto or eat at Jack 'n the Box. But look at Coke, Tylenol, and Toyota. Each has had problems and survived.

Mr. Rendon stated that Coke succeeds because its message is happiness. Blockbuster is another interesting example of failure to adapt to change. When you are in the midst of good times, you do not see the change. Strategically, you have to steer towards change. Lead it instead of follow it.

Warfare in the Western world is an extension of politics. When politics fail, we impose our will on an adversary. So deterrence is the threat of bringing capability to impose will. Influence is much the same. We are not structured properly for this. The challenge the DoD has is in the area of hostility. How do you account for the fact that we do not have a way as a nation to deter or influence from a whole of government perspective?

Dr. Zalman said influence as an instrument of power relates to how we do statecraft in the digital age.

Mr. Hustus offered a concluding question. What can we take away from this panel discussion?

Mr. Rendon stated that direct action has a clear process that works well. There is no comparable indirect process. So how do we adjudicate among taskings? There is no peer-to-peer tasking. The system is stressed, but how do we take some issues off the table? One way is to nest them under NCTC because they have interagency authorities. DoD is an enabler and should not own this process.

Dr. Zalman added that the DoD needs more foresight tools.

What I have learned from this panel is that we are seeking to apply non-traditional focus and non-traditional science and we think we are going to be effective within the traditional structure and process. We will have to work on interoperability to work this problem set effectively.

Dr. Casebeer added that the best thing we can do today to help on this front is to give the military the ability to act more quickly. There were so many examples from Iraq and Afghanistan where quick respond could have made a difference, but they did not have the authority.

Panel 8: What's in Store for the Pacific Region: U.S./China Relations and the 'Information Revolution'

This panel explored the unprecedented ability to reach billions of people with various messages in an attempt to influence views and activities. It asked, how can we use this new info structure to share values? Change values? How can we protect the info structure to protect command and control? How can we use it to build trust? What is the Chinese view of Cyber? What does the rise of new media and social media mean for China/U.S. relations, in relation to Chinese Internet controls, government policy concerning new media technologies, and the global platform gap?

Panel members:

- Mr. Randy Cieslak (USPACOM/J6)
- Brig Gen Tim Fay (USAF AF-A3-5)
- Dr. Michael Swaine (Carnegie Endowment for International Peace)
- Dr. Cliff Whitcomb (NPS)
- Dr. Randy Kluver (TA&M)

Mr. Randy Cieslak, USPACOM, J6

Mr. Cieslak noted that over half of the world's population resides in USPACOM's area of responsibility (AOR), which consists of 36 nations. USPACOM's AOR offers a number of unique characteristics and challenges. The AOR covers roughly 3.42 billion people and more than 1,000 different languages across roughly 52 percent of Earth's surface across 36 countries and 16 time zones. Historic animosities and grievances including unresolved wars, separatists movements, territorial disputes, and religious conflict are common throughout the AOR. The military footprint is significant in USPACOM's AOR where the world's six largest armed forces reside, five of the seven U.S. Mutual Defense Treaties are in place, and countries with nuclear weapons and unbalanced military forces can be found.

In order to create trust and improve security using the ongoing information revolution, we must establish and build upon the following elements: (1) connectivity, (2) communication/language, (3) cultural understanding, (4) confidence and confidentiality, (5) collaboration, (6) coordination, and (7) cooperation.

Brig Gen Tim Fay, USAF AF-A3-5

Brig Gen Fay provided a strategic context to what is in store for the pacific region. When looking through a deterrence lenses, the typical strategic approaches for understanding the U.S.-China relationship commonly set conditions first and then hope for a positive outcome. However, effective deterrence is reliant upon communication. The information revolution has provided us with new methods of communication. We can now look at possible second and third order effects of communication activities. The information revolution is providing us with the opportunity to assess our effectiveness in our relationship with China. For the first time, we have the opportunity to fully understand communications with China. The

next step will be to use communication as a means to deter. How can communication be used to drive an outcome? How can communication help us achieve desired end states? There is great opportunity for assistance in communicating strategic messages in the strategic environment.

Dr. Cliff Whitcomb, NPS

Dr. Whitcomb began by noting that the term information revolution raises the question of *how long is the revolution going to last*? The information revolution has rapidly increased its speed and changed its direction. Penetration of the information revolution has been global and in an extremely short period of time. The level of technology evolution and innovation has been remarkable. The newest innovations, no matter where it comes from, can be pushed out immediately to almost anybody. There is very little learning curve for new technologies amidst the information revolution of today.

From a technology perspective, the amount of information and computing available is remarkable. These tools can be used by almost anyone to get their messages out. This type of access and information makes planning into the future extremely difficult. Using systems dynamics approaches can help provide insight into influencers and variables to better understand the dynamics possible futures of a situation over time. However, the populations, people, and technologies are going to continuously adapt over time so it is important that we continuously update the systems dynamics models to account for this evolving environment.

We need a change in how people approach the problems we are facing today. These problems are complex and will require new tools to help develop a full understanding. We must remember that outcomes are going to be dynamic and adaptable.

Dr. Randy Kluver, Texas A&M

Dr. Kluver discussed U.S.-China relations in the information revolution. It was believed that the Internet would democratize China because 1) the Internet is inherently democratizing and 2) because the Internet is inherently global, but this was not the case. We focused so strongly on whether or not China would democratize because of the Internet that we missed the way in which the Internet really did impact China.

Chinese Internet population is close to 700 million people. The mobile population is even larger. China's Internet population is larger than any other country in the world. Most of our attention has been focused on the control of political content, but what the Chinese government is most interested in controlling is the development of political or social organizations that might challenge the authority of the CCP. There is also an interesting transition from Weibo (similar to Twitter) to Wechat (which does not allow strangers to view your postings). This means that we have less opportunity to see the fascinating challenges to the state that are emerging.

In relation to how the rise of Cyber-China will affect its relations with other states, there is an emerging "app gap," or disconnect between the applications most popular around the world, and those that are popular in China. What has emerged in the social media world is a bi-polar environment, driven not by ideology, but by technological platforms. This illustrates that the technical platforms we use do matter. Different platforms can in some cases have significantly different usage levels depending on the country. The decisions that China has made to develop their technical platforms are interesting. The strategy of platform substitution is reminiscent of the economic strategy of import substitution and probably has both economic and political goals. However, the consequence is that we have developed global platforms that unfortunately exclude China.

Dr. Michael Swaine, Carnegie Endowment for International Peace

Dr. Swaine discussed Chinese national security related issues relating to the Internet, social media, and information technology. Social media has infused large sectors of the Chinese population. The Internet has connected large amounts of Chinese people and provided them with opportunities for significant discourse. The initial hope was that the Internet would be a democratizing force in China, but to some extent it has become an empowering force by providing many Chinese with the ability to communicate with each other in real time in ways that they have not been able to in the past. Recently, China has tried to eliminate anonymous message posting on the Internet as a means of somewhat controlling these new communication methods.

The active elements of Chinese Internet users are incredible active. This is particularly the case for issues of Chinese nationalism. The Internet has provided an information portal to inform the Chinese population of what is really going on internally and globally from a source outside of simply official media. This has altered the state-society relationship on some issues. Chinese civilians can now be rapidly motivated on a wide variety of issues because of the Internet, which can be good and bad for the Chinese government. The Chinese government has realized that it must be aware of what is going on within the Internet to motivate its citizens. The question then becomes, *to what extent does the Internet function in ways to which the Chinese government finds useful or threatening*? It is not clear whether the Chinese government has a clear answer to this question.

The fear of chaos within the country has a significant influence on Chinese perspectives. A force like the Internet can easily create instability through chaos and, as a result, regulation of the Internet is widely accepted throughout China. The Chinese government sees both danger and advantages from the Internet. All Chinese recognize the importance of the Internet, but at the same time there are some aspects of the Internet that are too democratic in the eyes of the Chinese government. The government does not want the Internet to undermine their authority. The Chinese government believes that governments must govern the Internet. They believe that there should be certain boundaries with respect to Internet freedoms that should be agreed upon by all countries and established by

the United Nations. This is a point of disagreement between the U.S. and China. The Internet is not often governed when it comes to content that is not criminal, but in the eyes of the Chinese it should be. Furthermore, the Chinese perspective on this issue is not unique among countries of the world.

Another notable issue between the U.S. and China in the realm of the Internet relates to national security and specifically the issue of hacking and Chinese efforts to attack U.S. commercial enterprises through the cyber realm. The Chinese engage in aggressive behavior to try and steal commercial information from the United States. However, the Chinese do not admit to any sort of engagement in these types of cyber activity. Instead, they say that they only respond to threats and do not engage. There is a significant clash between the United State and China when it comes to cyber warfare.

Discussion

Has the presence of social media in China increased protest levels? Is there a link between the openness of social media and protests over things like corruption?

Dr. Kluver responded that China has developed something like an in-between Internet where the government maintains some limited controls over Internet activity. Once something gets to the point of organizing a protest, you can be sure the Chinese government will shut it down. The government allows for criticism over the Internet but it does not accept any effort to organize a protest or something similar.

Dr. Swaine noted that as with so many of these issues, anti-corruption is a two-edged sword. Anti-corruption is a good thing, but it can also be used to attack the government and create unrest.

Do the Chinese have any influence on social media in Africa or South America?

Dr. Kluver noted that this is a fascinating question. The Chinese are currently building huge amounts of communication infrastructure throughout Africa, which will have huge geo-political implications in the future.

Panel 9: Bringing it all Together (JS, Command Reps, and Panel Leads)

This panel asked representative from the Commands to discuss what they have learned at the conference, what they will be bringing back from the conference, and where they anticipate needing further assistance.

Panel Members

- Dr. Tom Allen, JS/J-8, moderator
- Mr. Randy Cieslak (PACOM)
- LTC Lance Rasmussen (SOUTHCOM)
- Mr. Marty Drake (CENTCOM)
- Mr. Hap Harlow (AFRICOM)
- COL Lynda Granfield/LTC Dave Creasman (I Corps)
- Mr. Ed Doray (NORTHCOM)
- Dr. Regan Damron (Booz Allen Hamilton & EUCOM)
- Mr. Ric Schulz (JS/J-7)

Dr. Tom Allen is Deputy Director for Studies and Analysis, J8.

Dr. Allen stated that SMA cuts across a lot of areas where no one agency is expert. A key is determining how SMA can help ensure operational relevance. We need to know whether, at the end of studies, Commands adopt new tools, methods, or insights generated by SMA. Similarly, we need to identify what can we take away from this conference. The purpose of this panel was to help identify what new insights have we generated at the Conference that we can take back to our organizations.

Dr. Allen offered that one insight he gathered was that the USG is not clearly messaging its own narrative. We need to figure out how to strengthen the US narrative in the information age.

Mr. Randy Cieslak, PACOM

Mr. Cieslak stated that he was awestruck by the level of participation and insight during this conference. But he was concerned that we were just talking to ourselves. It seemed like the main targets of the insights were political officials. How do we convey the insights we've developed to the decision makers who can best make use of them?

The information revolution was spurred by information technology advancements, but it is different from previous revolutions that were based on breakthrough inventions. IT continues to advance and expand. The thing we must follow and manage is not the technology, but the evolution of technology. We do too much

management and control for what we think is our own good: to save money or protect ourselves. It is a big task to protect the nation, so why does the government not have modern technology? Why do we only have access to 1990s technology? The reason why is because we have to control information and secrets and we cannot trust the technology to protect information well enough. Once we crack that code, we can move on. We overclassify information, we do not take enough risk, and we do not have enough technical knowledge to take risks. There is a movement to do that, but it needs to move faster. PACOM is trying to adapt as fast as it can.

With regard to influence, Mr. Cieslak was struck by a comment from Dr. Casebeer about sacred values and level of trust. The root of differences is misunderstanding. We need to get to the common set of sacred values. We need to more efficiently take advantage of the information revolution.

LTC Lance Rasmussen, SOUTHCOM

LTC Rasmussen agreed that he should have brought his IO team to this conference. Their participation would have been value added.

LTC Rasmussen was very encouraged by the conversation during the conference. He hopes that whatever the output of this conference is, it would include an actionable document. It should go to people who make decisions, change policy, and create guidance.

He said his main takeaway was to look at problem sets today using a variety of perspectives in comparison to how we compartmentalized before. He was excited to see various disciplines come together to discuss these problems.

Mr. Marty Drake, CENTCOM

Mr. Drake stated that he should have sent CENTCOM's IO team to this conference. CENTCOM has not done a great job of articulating the challenges it faces with regard to information operations and, therefore, has generated misconceptions about its challenge space. Cyber is simply a medium in which information exists. For the purposes of our discussion, we agreed that we are going to have equal access to that space. We probably do not realize it, but, in this room, we are a microcosm of what we are trying to discuss. There are many disciplines here. But despite our differences, we are all playing by the same rules and were willing to cross boundaries to do so.

Mr. Drake stated that he believes we have the capabilities, mission, and resources to act. The problem we are trying to resolve does not exist in the real world. We divide information into operational and intelligence. Our adversary does not. We have rules; the adversary does not, and they use our rules against us. We have boundaries; our adversary does not. We have to be everywhere, ready to respond with verifiable truth. The adversary controls the pace, timing, and content of this information conflict. They are able to be instantaneous where we are ubiquitous.

We came here with rules. How would your participation differ, how would the outcome be altered, or how would the value change if there were no rules? Welcome to the CENTCOM IO team's world. That is what they deal with.

Panel 8 talked about the timing of a message. The way we approached the IED problem was to get between the device and the initiating device. Can we do that with other forms of messaging—intercept and act on the message before it has been received?

This has been an amazing group of people gathered together to solve a problem. The audience brought a multidimensional and widely varied background to bear. The audience members are talented and dedicated. This mirrors what we as a nation must bring to bear to tackle these tough problems.

Mr. Hap Harlow, AFRICOM

Mr. Harlow stated that conference attendees heard yesterday that there is no good, old-fashioned war left. However, there are still some in Africa. The continent continues to suffer under internal and border conflicts, and increasing numbers of coups. While we think we understand the causes of conflict in Africa, the roots actually go much further back that we are prepared to acknowledge—often back to colonialization.

Too frequently, USG Africa policy is driven by political whims or emerging crises. This adversely affects the long-term US military strategy degrading our ability to achieve measurable progress in Africa. ADM Rogers' comment was relevant; our ability to generate US political will and willingness to address hard problems in Africa is difficult. At the same time, the US population is becoming more polarized, frustrated, and angry—greatly detracting from a focused approach. We have to work on our messages within our own borders.

Mr. Harlow suggested that the next time a conference like this is convened, he would like to bring some African partners to participate. We could benefit from outside voices.

LTC David Creasman, I Corp

LTC Creasman agreed that he should have brought his IO team to this conference. Their participation would have been value added.

He suggested that it would have been useful to have a third day of the conference with an operational focus on how to do IO from the operational commands. It would be interesting to hear how the COCOMs each conduct information operations.

This conference is a starting point from which we need to synthesize the problem facing us. It is important that the various organizations struggling with big data and messaging come together to propose solutions, which need to be presented to senior officials so that policies can change.

Information management will remain key to all of us. How do we gain access to information when there are interagency firewalls? How does information help us understand the people we deal with? We need to use the new technology that is out there. How do we leverage that through data? How do we counter messaging against us?

Mr. Edmund Doray, NORTHCOM/NORAD

Mr. Doray stated that there is tremendous value to COCOMs from this conference. Although this is the 8th year of the conference, in reality, there has been a tremendous amount of work done to leverage this capability. NORAD's Santa Tracker is one way NORAD remains relevant to many people in the US and across the world.

To illustrate the difficulty of the problem facing the defense community, imagine that every three hours, thirty percent of conference attendees had to leave and were replaced by new attendees. This is the challenge COCOMs have.

NORTHCOM is monitoring social media to the extent it can to clarify messages and to put message out. We pushed out information during Sandy about utility trucks from California being shipped to New Jersey to help respond.

When we look OCONUS towards Mexico, we still have challenges with regard to resources, policy, and authorities. Some believe we can look at monitoring what is happening using an e-campaign. But then we would have to create a metric to evaluate its usefulness, which might have to rely on paper surveys.

One opportunity this conference presents is taking a step towards creating a roadmap from a capabilities standpoint. We need to put something together so the four stars can take an advocacy role to ensure the initiatives are funded and transitioned. We have a transition pipeline for operators so we can capitalize on capabilities as they come to bear. He believed that NGA is the only agency that has established a legal finding on the use of social media. He was encouraged to hear than EUCOM wants to go down that path. That will help other COCOMs as well.

With regard to interagency and sharing, we need to create a common environment so we can leverage data collection that will allow us to share and reintroduce findings back into the community that that we can be more effective in execution of missions. We are still leaving data on the floor for others to analyze.

Dr. Regan Damron, Booz Allen Hamilton & EUCOM

Dr. Damron stated that he is contract personnel and cannot speak directly for EUCOM. He emphasized that overclassification and compartmentalization erect artificial barriers between operations and intelligence. He structured his presentation by taking themes he gleaned from the conference, pairing each with a

"radical thought," and then briefly discussing some ideas about how to implement those thoughts.

Theme: The USG must be more introspective and self-questioning. *Radical thought:* Commission a U.S. "master narratives" study. *Implementation:* Use this to better understand how different population segments within the U.S. are portraying themselves (ourselves, collectively) to the world, how these messages may interact with (help or hinder) the messages we (the military) want to send, and how all of this impacts perceptions of us and our messaging abroad.

Theme: Unclassified information holds much value. *Radical thought:* Explicitly invert the traditional intelligence information flow (from classified to unclassified (top-down) to unclassified to classified (bottom-up). Traditional intelligence typically begins with classified information and fuses unclassified information with it in a complementary fashion; such "all-source analysis" is certainly a good start, but it leads to (1) labor-intensive review of products to redact for releasability and (2) releasable products that are often unnecessarily stripped of information that could have been available via open sources. Exhausting the potential of open-source info first would lead to efficiencies and make products more shareable more quickly. *Implementation:* Segregated open-source research cells with one-way flow of information into the IC could be set up. They would be aware of U.S. strategic goals and priorities, but not intelligence requirements.

Theme: Phase 0 is not everything, but it is not far from it. *Radical thought:* We must be more proactive, less reactive—but how? *Implementation:* Make the aforementioned "open source research cells" forward thinking as well as strategic and locate them at the COCOMs. Make them leverage the full power of unclassified information by working closely with their local partners and allies to understand emerging trends. Situate them as conduits between the partners and allies and a "mother ship" organization in the DC area, with information flowing both ways. This would be a true sensing organization.

Theme: We tend to focus on figuring out new ways to generate knowledge from new sources using new techniques. *Radical thought:* We also need to innovate in the realm of knowledge dissemination (this is not really that radical, but roll with me here…). *Implementation:* Position the aforementioned open source research cells above and across the J-codes at their respective COCOMs so they can better perform their role as information conduits and theater-strategic contextualizers.

Theme: Interagency coordination is imperative, but nobody seems to know how to do it well. Often, COCOMs have conferences around themes. These cultivate institutional knowledge and personal relationships, but because there is much turnover in personnel, most of this is lost. *Radical thought:* We need a way to know what every arm of the U.S. government (USG) is doing in order to facilitate synchronization that is less personality- or relationship-dependent, thus institutionalizing this knowledge. *Implementation:* Construct a central clearing

house on data at the subnational level showing what the USG is doing and where. We do not have this at an interagency level. It would aid us in identifying gaps and seams. It would enhance cooperation and synchronization. It would allow us to tie activities directly to national policy guidance and increase accountability.

Discussion

During the conference, we talked about big data and narratives. There is a connection there from data to actionable knowledge, and narrative captures that. One way to think about warfare is a conversation. It is our messaging versus their messaging.

Mr. Cieslak agreed that big data and cyber are trendy ways of talking about things. Big data is a resource. We have a ton of data, but what does it matter? He agreed that we collect big data, make sense of it, but what is our objective? How do we use this resource to get us to a useful end point? Influence, understanding, and effectiveness are all possible if we know how to render data into action. You can make a message with a little data, but big data can increase the accuracy across social, cultural, and other aspects.

Mr. Doray stated that following a tornado in the Midwest, NGA used open source big data to do a damage assessment within 12 hours, before we had overhead imagery available. This is a new capability. We need to figure out what we can do with it.

Regarding sensemaking at an organizational level, how do we get from big data to narrative? For example, say you have a big government initiative and are asked how effective it has been? How do you assess whether it has been an effective program when there is not a linear input-output relationship? This is analogous to communications. This is a problem where we can apply an analytic approach, but perhaps narrative came about as a topic because deriving narratives is one way to make sense of an effort or initiative. Maybe as a community, we should think about ways to operationalize that.

Dr. Allen responded that big data captures inputs and translates them to narratives as a simple output to make understanding easier.

Dr. Damron added that the USG needs to anticipate how to measure effectiveness when it is creating planning actions and programs (DoD does this better than most others, but even it still struggles). We need to think about efforts in a more deliberate, planned, and prescient way. Doing so would yield better evaluation results.

Mr. Schulz asked, how do we create operation advantage to a novice commander? What needs to be known, when? How does information need to be expressed so a commander can turn information in action? Nothing he has heard during the conference could shape that kind of thinking. This needs to be done as soon as a commander decides what action he has to take. His staff has to form these questions.

Mr. Drake stated that if you collect data without knowing what you want to do with it, you can collect the wrong data. You have to define the operational parameters and create a dendritic of questions you think you can answer. Use that to go and look for certain kinds of data.

This is a complex area. We need to look hard at various pieces of the information struggle. The point needs to be pursuit of competitive advantage. We have limitations, constraints, and restraints that in some aspects put us at a disadvantage to counter enemy propaganda and influence foreign segments. Anywhere we fight from continual and unchangeable disadvantage is a fool's game. We need to look for aspects of where we can get ahead and win and not continue behind the barriers of uncertainty and legal boundaries.

Second, as someone from the J2 and intelligence communities, it is not always clear how to tap into the SMA community more formally. The SMA community brings something to the table that the intelligence community desperately needs. What can SMA bring to bear on the information problem and what is SMA's willingness to participate in future efforts? The JIOWIC J9 has been tasked to provide a framework for the information operations community. We can share that.

Dr. Allen responded that Dr. Cabayan always makes sure there is representation from the J2 on all efforts; representatives need to get the word out to the wider community they represent.

Are there gaps in big data?

Mr. Cieslak stated that PACOM's number one priority is to create a multi-partner technology environment. We want to share information. The trouble is that we have to create separate networks with our partners to protect classified information. We do not have enough men to build the right network. It is ridiculous to create completely new networks with their own infrastructure for every different situation with its own combination of partners, such as for the Ebola and ISIL efforts. One network infrastructure should be responsive enough to handle any situation we are confronted with. The technology exists to solve the problem and we are working on it, but input from the broader community on how to resolve this is welcome.

Conclusion

COL Eassa stated that the participants in this room represent the cutting edge of knowledge and debate at the nexus of information technology and operations. He said the challenge remains, how can we help commanders, their staffs and in particular, those on the information operations staff, solve emerging challenges under pressure, in a crisis, and without the benefit of the experience and talent in this room? As they take action, how are other competing narratives changing? How does the information environment evolve over time as the adversary's tactics

change and we engage in information activities? How do we message to different demographics? How do we do it in near real time? Those are my takeaways.

Appendix A: Agenda

Day One Tuesday, 28 October 2014	
0730 - 0800	**Registration**
0800 - 0810	**Introduction:** CAPT Todd Veazie (NCTC)
0810 – 0840	**Opening Session:** Brig Gen David Béen (JS/J39), Mr. Ben Riley (PD DASD (EC&P))
0840 - 0925	**Key Note Speaker:** LTG Edward Cardon (U.S. Army Cyber Command)
0925 – 0945	**Break**
PANEL DISCUSSIONS	
0945 - 1045	**Panel One** **Complexity, Interdependence, & Emergence in an Interconnected Information Age** Moderator: CAPT Todd Veazie, (NCTC)
1045 - 1145	**Panel Two** **Setting the Stage: The Information Age, Networks, and National Security** Moderator: Dr. Dana Eyre (SoSA) Invited Panel Speaker: Mr. Josh Kerbel (DIA) "Information Age, Simulations, and forecasting"
1145 - 1245	**Lunch**
1245 - 1345	**Panel Three** **Geopolitics and National Security in the context of the Information Age** Moderator: Mr. Dan Flynn (DNI/NIC)
1345 - 1500	**Panel Four** **Operational Perspectives: Opportunities and Challenges (Joint Staff and the Commands)** Moderator: Brig Gen David Béen (JS/J39)
1500 - 1520	**Break**
1520 - 1640	**Panel Five** **The Intersections of Big Data, Neuroscience and National Security: Technical Issues, Derivative Concerns** Moderator: Dr. James Giordano (Georgetown University Medical Center)
1640 - 1650	**Day One Wrap Up**

1700	**Clear The Building**

Day Two Wednesday, 29 October 2014	
0730 - 0750	**Registration**
0750 - 0800	**Introduction:** COL Chuck Eassa (JS, J39)
0800 - 0830	**Key Note Speaker:** ADM Michael Rogers (Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service)
PANEL DISCUSSIONS	
0840 - 1000	**Panel Six** **Understanding Social Systems in Phase 0: Human Geography, Big Data v. Micro Information, and the RSI Paradigm** Moderator: Dr. Chuck Ehlschlaeger (USACE/ERDC)
1000 - 1120	**Panel Seven** **Implications of the Speed & Global Reach of Information on DoD Missions II: Effective Deterrence and Influence Strategies** Moderators: Mr. Hunter Hustus (Air Force) and Dr. Allison Astorino-Courtois (NSI)
1120 - 1300	**Lunch**
1300 - 1400	**Panel Eight** **What's in store for The Pacific Region: US/China relations and the 'Information Revolution'?** Moderator: Mr. Randy Cieslak (PACOM, J6) Invited Panel Speaker: Brig Gen Tim Fay (USAF AF-A3-5)
1400 - 1530	**Panel Nine** **Bringing it all Together** Moderator: Dr. Tom Allen (JS, J8)
1530 - 1550	**Day Two Wrap Up**
1550 - 1600	**Conference Summary & Closing Remarks, Dr. Hriar Cabayan (JS/J39)**
1700	**Clear The Building**

Appendix B: Biographies

Biographies of all the speakers are located in the Conference Booklet. Please contact Ms. Meg Egan for a copy at margaret.j.egan2.ctr@mail.mil.