12th Annual

Strategic Multilayer Assessment (SMA) Conference

Jointly with DHS

"The Evolving Anatomy of Conflict in a Dynamically Changing World"

Joint Base Andrews
21-22 May 2019

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

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

This report does not represent official USG policies or positions.

Table of Contents

Executive Summary

The 12th Annual SMA Conference, entitled "The Evolving Anatomy of Conflict in a Dynamically Changing World," was held 21-22 May 2019 at the General Jacob E. Smart Conference Center at Joint Base Andrews in Maryland. The conference theme was defined as:

> The actors, actions, and arenas of the emerging global security environment are changing. To navigate these murky waters, the United States requires effective statecraft that relies in equal measure on: (1) resurgent diplomatic application of national will, (2) information and technological overmatch including through artificial intelligence, (3) multi-use conventional and irregular warfighting capabilities, and (4) economic growth fostering national interests across domestic and international private-public partnerships. Such a comprehensive and nuanced approach is needed to achieve strategic success in diverse contested spaces, and address the complex political, economic, social, and ecological challenges that will face the nation.

Jointly with the Department of Homeland Security (DHS), SMA welcomed panelists and speakers from across the United States Government (USG), academia, foreign partner nations, and industry to explore this theme. This year, the Conference welcomed keynote speakers General Paul J. Selva, Vice Chairman of the Joint Chiefs of Staff (VCJCS), and Lieutenant General John N. T. Shanahan, Director of the Joint Artificial Intelligence Center (JAIC), and invited speaker Mr. Brian Murphy, Principal Deputy Under Secretary for the Office of Intelligence and Analysis in DHS.

General Paul J. Selva discussed historical cases of the US strategic calculus and how the previous lessons learned are shaping the current mindset of the DOD. He also stressed the importance of AI and machine learning to the current dilemmas arising from great power competition with Russia and China, stressing that the continuous integration of data information into the US military structure, doctrine, and decision making is vital to adversarial competition.

Lieutenant General John N. T. Shanahan detailed the importance of technological advantage in prior US conflicts and emphasized that the world is on the cusp of a military information and intelligent technological revolution. He went on to highlight the growing threat of China and Russia's respective artificial intelligence (AI) capability and how these adversaries and the US have moved beyond competition, into conflict in space, cyberspace, and the information environment.

Mr. Brian Murphy related the themes of the conference to the problem set that the Department of Homeland Security faces, stressing that a whole-of-government approach is necessary to tackling such issues. Mr. Murphy noted the unique challenges that Russia and China pose on US national security in a rapidly changing environment, noting that the premier challenge of integrating all levels and elements of government is vital to navigating foreign threats.

On DAY 1, the conference panels included:

> The **Conference** I**ntroduction Roundtable: State of the World—Opportunities and Threats on the Horizon**, framed the theme of the conference with a discussion of competing trends that contextualize great power competition. The evolving nature of state power, competition, and the persistent threat of direct conflict were discussed by panelists in the framework of rapidly advancing technology that are fundamentally altering the strategic landscape.

Panel 1: Opportunities and Risks of Stabilization focused on socio-cultural dynamics that often shape the nature and reality of stabilization and reconciliation efforts. Panelists considered issues that surround the complexity of culture and behavior and how they challenge national defense and national military strategies.

Panel 2: The Near Fight – USCENTCOM, USAFRICOM explored in-depth ongoing conflicts and crises in the Middle East and Africa, and how state and sub-state actors are influencing battlefields across these regions. Panelists discussed these issues in specific contexts, highlighting the commonalities and differences between them, and discussed how adversaries exploit US involvement in these regional conflicts.

Panel 3: The Nearing Fight – USEUCOM, USINDOPACOM, USSOUTHCOM investigated China and Russia's ambitions in these AORs, specifically in Columbia and Venezuela. Panelists also explored the political warfare Russia is engaging in the USEUCOM area of responsibility (AOR) and the "strategic hedging" USINDOPACOM nations are utilizing in the advent of great power competition.

Panel 4: Cooperation, Competition, and Armed Conflict: Globally-Integrated Campaigning for Today and Tomorrow discussed the changes and dilemmas that surround the military doctrine of competition. Panelists detailed how historical case studies, an empathetic perspective of the adversary, and technology can impact the US competition strategy as well as how to appreciate the role of the US military, and imagine effective uses of force below the threshold of armed conflict.

Panel 5: Pushing Boundaries of the Domain Concept: the Criticality of the Non- Kinetic Toolkit grappled with the impact and challenges of artificial intelligence/machine learning (AI/ML) on global competition and domestic populations. Panelists also stressed the importance of integrating such technological advancements into modern society and defense strategies, where Panelists detailed the progress and impediments to such integration.

On DAY 2, the conference panels included:

Panel 1: Integrated Operations in a Dynamic Environment delineated unique challenges across the Joint Force's AORs and how the respective Combatant Commands are consolidating responsibility and planning to tackle global concerns and adversaries. In particular, panelists focused on contemporary and pressing issues and suggested tools, technologies and organizational techniques to successfully integrate the Joint Force.

Panel 2: The UK Assessment of Future Competition laid out the UK perspective on how allies can fully utilize their respective defense bandwidths collectively across alliance partners. Panelists then noted a wide array of challenges and solutions to maximize the "alliance complementarity" between the UK, US, and other allies.

Panel 3: Future Global Competition between AI-Shaped Political Systems analyzed the emergence of AI technologies into the competition environment between the great powers. Panelists also reviewed how such technology is also engaging the progress of the societies of political regimes and the resulting implications for the US.

Panel 4: Strategic AI: Predictive Analytics, I&W, Counter AI/ML Alternatives examined the limitations of AI and the application of data science in terms of feasibility and efficiency. Panelists described explicit disconnects of the current capability and limitations of AI, incorporating AI into the systems, and structures of the DOD, and sheer complexity of modern operating/strategic environment.

Panel 5: Human Threats versus Machine Threats in Cyber Security considered how the cyber domain is "amplifying" global competition for influence. Panelists stressed the differences between human and machines and how emphasized that better understanding the confluence of both is critical to succeeding in the digital age.

Panel 6: Dealing with Surprise in Complex Systems reviewed medium and high-consequence "events" and how they affect high-level decision-making in the US. Describing specific and potential events, panelists explored how the US can defend against blind spots pre-emptively and bolster systems of response to prepare such surprise.

Panel 7: Risks and Opportunities associated with Human Biotech Engagement addressed the development of human biotechnology and related it to national security opportunities, risks, and threats. Panelists discussed specific examples and how current and future biotechnology can be engaged by strategic competitors, affect US and global stability and security, and how US national defense can mobilize to meet these threats.

Panel 8: Human/Machine Partnership for Decision Support in the Cognitive Space explored how AI/ML and the successful integration with human capability can augment US strategic understanding of competition and conflict. Panelists discussed how AI/ML can assist in integrated influence operations, human-machine decision collaboration, influence capabilities in the grey zone, and on human cognition and decision making.

Conference Intro Roundtable: State of the World – Opportunities and Threats on the Horizon

- Dr. Allison Astorino-Courtois (NSI)
- Dr. Spencer Meredith III (National Defense University)
- Dr. Barnett Koven (University of Maryland/START)

In this introductory roundtable, the panelists highlighted different perspectives on some of the concepts and issues that underlie our understanding of the current operating environment and the reemergence of great power competition.

Dr. Meredith began by discussing how we think about power, the capabilities that confer power on an actor, and how we measure relative power. He contended that, although our understanding of the nature of power is expanding, traditional measures of power, in particular military expenditure and capability, remain highly relevant; not only to the US, but to Russia and China as well. Dr. Meredith noted that while US military capabilities still outpace those of Russia and China, China is increasing its military spending, and while Russian spending is nowhere near US or Chinese levels, Russia's messaging, endurance, and resilience against sanctions suggests that military capability is still a relevant concept. He concluded by referencing how China's broader activities, in particular their space program and transportation infrastructure, support their narrative of expanding power (space) and control (infrastructure).

In contrast, Dr. Astorino-Courtois argued that the currency of power has changed and we need to adapt. She stated that the job of a military remains to defend their nation's territory and people, but to do this requires adaptation to new forms of power. In the current international environment, Dr. Astorino-Courtois contends that information and data are the currency of power that allows us to maintain and protect what we hold dear. It provides military targeting precision and allows us to communicate, conduct business, control our environment, and circulate our narratives (i.e., shaping the environment). The changing currency of power has different implications for different actors and Dr. Astorino-Courtois finished her discussion of power by posing the question of whether we have considered these changes, or whether we are still training/equipping to fight traditional conflicts.

Dr. Meredith held that conventional capabilities will remain essential for hybrid warfare, agreeing that influence matters, especially in democracies, referencing the role of Special Operations and irregular warfare capabilities in supporting resilience and resistance. However, Russian and Chinese behavior indicates that they care more about control as hard power than influence as soft, using the latter to reinforce the former. Finding a midpoint between these the positions of Dr. Meredith and Dr. Astorino-Courtois, Dr. Koven proposed that both conventional and informational warfare matter. To support this position, he noted that during the Ukraine conflict informational capabilities were (and still are) critical to Russian actions, but only because they were timed with kinetic actions.

Dr. Meredith then moved the discussion to the locus of power within the international system and noted that the resurgence of the state is driving this discussion. For the past 20 years, we have been dealing with low capacity (weak) states, but by returning to questions of great power conflict, we are dealing with the opposite—strong or hyper states, such as China. Strong states, he suggested, create different challenges to those that arise from weak states. He posed the question of how outcomes may have differed in Syria, Libya, and Egypt if their respective regimes had the surveillance capabilities of the Chinese regime. Supporting this position, Dr. Koven added that democracies are at a structural disadvantage when it comes to the types of competitions we are likely to have with strong states.

Dr. Astorino-Courtois agreed with the observation that democracies face a difficult road right now. However, she suggested that the types of control and surveillance discussed were also difficult for authoritarian states to exercise. She contended that no state—democratic or autocratic—can work too far in front of what its population is willing to tolerate. This implies that there is a cultural element to digital control; it is not going to look the same in every place. Even if, for example, China exports its surveillance systems to other countries, they will look and function differently outside China. Dr. Astorino-Courtois used the example of high levels surveillance in Western cities (London and New York) as a signal that this type of control is already coming into place within democracies.

The roundtable then segued into a discussion of Artificial Intelligence (AI), with Dr. Astorino-Courtois warning that, when combined with surveillance capabilities, AI is one of the most important, yet feared, types of control. She noted that AI can help us address complex problems (climate patterns, population resettlements) and provide unbiased diagnosis and analysis by cutting through noise of bias, and the cognitive limitations of humans. Dr. Koven offered a more skeptical view of the potentials of AI, and pointed out that our AI is still very limited in the types of questions it can handle. As an example of this he pointed to Amazon: it has more and cleaner data than anyone else; has the money to get the algorithms right; and yet given a fairly simple question (e.g., predicting what an individual might buy next, given what that individual just bought and other basic information), they are far from perfect. Dr. Meredith closed the session by commenting that there was a little artificiality in the disagreement between participants, which was designed to highlight the fact that these topics are not black and white.

Keynote Speaker

General Paul J. Selva (Vice Chairman of the Joint Chiefs of Staff)

Thank you for the opportunity to speak with you today, and let me note that I am really happy to be here. Let me start by rewinding the clock to provide a historical context. This week, 76 years ago, President Roosevelt and President Churchill met in Washington DC with all of the assembled military leaders from the European and Pacific theaters. With this meeting, Roosevelt and Churchill were formulating a grand strategy for the conduct of World War II. They were making choices about how to deploy forces across the European and Pacific areas of interest to attempt to win simultaneous fights in both regions. What those leaders were doing 76 years ago while meeting in Washington DC was debating the timing of the amphibious invasion of Sicily. They were also debating the timing, pace, and tempo of the invasion of France. They also had fairly significant debates about the value of strategically bombing German facilities that were supporting war efforts. World War II was a global conflagration, with 3% of the global population perishing during the conflict. The war so affected its leaders that they believed that they needed to be in control of the planet. Ultimately, Churchill was so affected by the carnage of World War II that, after the war, he said that "our supreme task and duty is to guard the homes of the common people from the horrors and miseries of another war."

World War II was caused, in part, by grave miscalculation between governments that at the time were significant global competitors. Japan was the industrial powerhouse of the Pacific, and in the lead up to the war, we had a spat with Japan that led to us imposing sanctions limiting iron and fuel from the country. In Europe, we miscalculated Hitler's ambitions, and as a consequence of that miscalculation Germany began to invade its neighbors, which lit the fuse for the explosion that turned out to be the war in Europe.

Let's look at today, but in doing so let's start by spinning the clock back 25-30 years. In the 1990s, the world changed, and when it did so we did not take appropriate notice. Our strategies at the time were filled with hubris. We were the world power. The Soviet Union had collapsed, and China was far behind and simply aspired to grow its economy. What did we do across that span of time? We sat on our laurels. We thought that we were number one and that we would always be number one. We even posited that if we could make friends with the leaders of Russia and China, we could help them emerge into the global community and emerging globalized economy.

It was a year later that Saddam Hussein invaded Kuwait in a dispute over oil fields. We, of course, marched with the coalition, taking six months to build up our power and then off we went to the Middle East. It took no time at all to completely decimate the Iraqi Army, which was built on Soviet technologies, tactics, techniques, and procedures. We used the processes and strategies that we had built for a war in Europe. Once we decimated the Iraqi Army, we quietly walked away, facilitating the partitioning of Iraq. I get in a lot of trouble when I make that statement, but what exactly could we do? We defended the Sunni minority in the south by creating a southern no fly zone that limited maneuvers in the south, and at the same time, we created a northern no fly zone in the north that we defended from bases in southern Turkey. In essence, the practical outcome was that we facilitated the ethnic partition of what had previously been a wholly sovereign country. There were some reasons for why we did what we did. In the south, we were protecting the Sunni minority who helped us defeat Saddam Hussein. In the north, we were protecting the Kurds who had been partners and helped us defeat Saddam Hussein in the north. We also probably prevented Saddam Hussein from committing unspeakable humanitarian crimes against those populations. But again, the end state of our actions was the partition of a nation.

While we were dealing with Saddam Hussein, we were still laboring under the misperception that if we were friendly to the Chinese and Russians then they would emerge as normal players on the global stage. With respect to China, by the way, that way of thinking is ahistorical. Any place that calls itself the Middle Kingdom is not likely to play by anyone else’s rules. If you look at what China is doing today, much of its activities are based on its careful academic study of the war I just described and the aftermath that followed. The Chinese refer to it as “informatized warfare.” We had the information advantage over Saddam Hussein’s forces, we knew what his forces were up to and, as a consequence of that, were able to execute our wartime strategy to defeat that army. In 1995, the Chinese said in the first text they produced on that war that they would not let what happened to Saddam Hussein happen to China. They said that they would hold in their hand an assassin’s mace—they would be nice to us, but they would find asymmetric ways to keep us from threatening their shores. China has been reasonably successful at deploying tools of asymmetric warfare to prevent us from threatening its interests. China is deploying AI at scale. China is using AI to create social compliance scores for its citizens. China deploys facial recognition and surveillance systems in most of its major cities. China monitors human behavior to determine loyalty to the Chinese Communist Party. China is investing more scientists and technologists in AI than any other country in the world. Ultimately, my prediction is that China’s early entry into AI and machine learning will be a little bit clumsy, but its progression will move relatively fast. For an analog to this, we can look to China’s ballistic missile and cruise missile programs from the 1990s to early 2000s. China is very good at prototyping and experimentation because they have nothing to lose—China has no reputational risk from failure. China will move with a great deal of alacrity to make sure that they do not fall any further behind.

Russia is an exceedingly clumsy example of the deployment of technology, particularly AI, machine learning, and computer technology. Most of the things Russia describes as AI-driven, autonomous machines, are actually just automated; they are not very smart in this regard and they do not adapt well. But, like China, Russia has no reputational risk from prototype failure. Russia is also willing to explore edges of this science that we choose not to, and my prediction is that Russia will be the first country to produce an autonomous killing machine. I do not think we will ever cross that line—not only do we have reputational risk, but we have an ethos across all of the Western world that says we will not cross that line. That is the singular nexus of conversations about military use of AI. I coined the phrase “the terminator conundrum” a few years ago to think about what happens when you put AI into military use. I think that where we draw the line is creating technology that will autonomously take human life.

The common myth today is that China is ahead of us. China may be ahead of us in a few unique corners of the technology sector, but as a general rule, China is not ahead of the Western world. The Chinese are fast followers and great copiers. They will attempt to buy what we will not teach them in our universities and high-tech industries. If we figure out a way of blocking them from buying what they are looking for, they have absolutely no problem with stealing it. These are all extremely effective ways to close a technology gap.

AI and machine learning will and must become a part of how we do what we do. The military’s mission boils down to killing people and breaking things. The military tool of national power is not about diplomacy, although the military can act in a diplomatic way. Rather, our job is to back up our national interests with the deliberate infliction of violence on our enemies. If we have the capacity and capabilities to do that, what the last 70 years of history tells us is that this may prevent miscalculation and war, and has a deterrent value. As a practitioner of the infliction of violence on enemies, it is actually the last thing that I want to do, but if violence is the last resort, we have to make sure we are good at it.

We have to bring modern information systems and processes into the way we operate across the board. If we are on the verge of having nearly ubiquitous sensing across the entire span of the globe, then in theory almost everything that happens on the surface of the Earth is knowable. If you can know things about your enemies, adversaries, and competitors, then you have to make sense of them. I am essentially talking about taking a synoptic view of the entire world. We are on the verge of that amount of information being readily available.

In 1996, I had the opportunity to brief the then director of what would become NGA, which at the time was a custodian of all of the imagery and maps that we had of the world. That year we were going to launch a space shuttle with a high-tech radar on it and we had to make a decision about the scale to which we would map the word with the space shuttle (i.e., at the 1m, 10m, or 100m scale). I argued at the time that we should map to the 1m scale because that density of information would be useful to everyone who needed maps—if you could define the world at a 1m scale, you would know where every obstacle and piece of geography is. The problem at the time, however, was where we would put the amount of data that would result from measuring at that scale. That amount of data that would have resulted would be miniscule in today’s standards, but it was overwhelming back in 1996. As a result, the decision was made to use the space shuttle to map at the 100m level. That level of measurement was completely and utterly un-useful. We could have advanced the science and the art of navigation simply by doing different math. We chose not to do it. This is where we are today with AI and machine learning.

What does AI mean to us? If you accept my notion of a synoptic view of the globe, it means that we have to understand all of that information, then we have to be able to focus based on the part of the information that is most valuable to us, and then we have to be able to act on that information. We have to be able to act decisively and precisely against objectives that matter. We have to take all of that data and make sense of it, make decisions based on what we know, and act quickly. We must have options and outcomes, we must be able to present them convincingly, and when we are given the authority to act, we must act in a timely way. If you think about cyber warfare, that means machine-machine interfaces that act independent of human interaction to protect our networks. If we are talking about a kinetic fight, that means everything from things that operate at speeds we are familiar with today to things that operate at hypersonic speeds, including weapons that operate at these speeds. If we cannot do all of this and integrate it, then we are at risk of the Chinese catching up.

I would propose, however, that doing this requires an understanding of how forces fight together that today the Chinese do not possess. We went through a process called Goldwater-Nichols in 1987 that forced us to act in a joint manner and forced us to acknowledge that our Army, Air Force, Navy, and Marine Corps are actually more effective operating together than they are operating independently. It took a while for us to learn this, but we eventually did. Today, it is very difficult to find anybody in the US who talks about strategy that is based on an individual service operating independent from any or all of the other services. The Chinese have not yet gone through this. They have artificially imposed it, but their services do not actually work together. Ultimately, that is a disadvantage that we should be able to exploit. We should think carefully about exploiting this. We should also think carefully about not teaching the Chinese how to jointly integrate their services. We will not sell or teach them this information, so at best they will have to steal it. They are fast followers, however, and will try to copy anything they can observe.

I mentioned earlier that the ability to inflict violence on an enemy can prevent wars and I would like to affirm my belief in that. Both the Russians and the Chinese are very dogmatic. They will engage in trying to understand the correlation of force, and if they do not have the upper hand in a given day, they will not engage in the fight. That is built in doctrine in both of their systems. We need to understand how they think. We need to understand how we would apply our levers of military power in the unlikely event that we ever have to go to war with them, and then make sure that we are able to make them understand that they are unable to win. That will change their calculus. Every text I have ever read about Chinese or Russia doctrine centers in on that similar concept of strategic thinking: if the correlation of forces does not appear to your benefit, it is not in your advantage to start the fight and you would be better off avoiding the fight. This puts a huge responsibility on the entire breadth and depth of our government. If we can prevent the fight, then what is the outcome that we want? Simply preventing the fight is not good enough because it does not actually advance the game—all it does is forestall the inevitable.

My view is that our government is incredibly myopic. Our processes are set up to worry about the next 1, 3, or 5 years. I would defy you to find a department in our government that has a planning process that looks out more than 5 years. We have to think much further out than this.

When the Chairman and I took our jobs, we posited that great power competition was going to be the controlling focus of our strategic planning. We both testified, about two weeks apart, and were both asked to detail the greatest threats to the US. I listed Russia, China, Iran, North Korea, and violent extremists. A Senator pushed back wondering how I could list Russia and China together with the likes of violent extremism, North Korea, and Iran, which he viewed as more serious threats as we have troops fighting violent extremism, an opaque and unpredictable leader in North Korea who is on the path of producing nuclear weapons, and the threat of Iran. My response was that Russia has enough nuclear weapons to make the US as we know it cease to exist, and as such it is an unpredictable and existential threat to the existence of our nation. China has the second largest economy on the planet and has aspirations to be the largest, President Xi has put himself in a position to be president for his entire life, the country is becoming increasingly authoritarian, and the Chinese military is quite large. Iran is opaque and unpredictable and has regional aspirations. North Korea is the Hermit Kingdom, and we know how to deal with that. Violent extremism is likely to be with us for the balance of my lifetime, so it is something that we will have to learn to deal with, but it does not threaten the existence of our way of life.

We have embarked on the process of changing the focus of the Joint Staff. We looked at Russia and China as global problem sets. We looked at Iran and North Korea as regional problem sets with global implications. We looked at violent extremism as a threat that we have to deal with. When you think of a potential adversary as a global problem set, you have to consider it in in its totality. How do you design a joint force that has all the tools to do that? How do you design a command and control enterprise that can take advantage of all of the available tools to do that? By not thinking this way, we may design a force that will be successful today, but we will not design a force that will be successful in a decade or two—it becomes an incremental approach to a long-term problem that is fraught with potential for miscalculation. We chose the long-term path. The Joint Staff authored a National Military Strategy, which became the foundation for a National Defense Strategy, and we are executing against that strategy. This does not mean that we will not be diverted, but if we maintain a long-term view, we will maintain most of the force back to the original trajectory we were on.

Question & Answer Session

(*Italics indicates questions from the audience.*)

Looking out to 2035, what do you envision the services looking like? Do you envision one joint service?

I do not think a single service is the answer. In fact, those that have tried a single service have found that it actually waters down the fervor of services arguing over how to best do things. However, having said that, our approach has to be joint. It also has to be multi-domain.

How do our long-term plans differ from the short- and long-term plans of our near-peer competitors?

Our Russian and Chinese counterparts are famous for saying that they are going to do something astonishing in 5 years and then failing to get there. The difference is that our plans will be less about material goals, which is what many Russian and Chinese plans tend to focus on, and more about creating a vector that will move us in a direction. We may deviate a bit from our planned direction, so we have to build in room for appropriating new processes, technologies, capacities, and capabilities.

How do you envision the strategic nature of the future non-kinetic battle space?

I worry a lot about genomes. In the science of medicine, there is unspeakable value in examining how to manipulate the human body. The more we learn about how the human body works, the more medicine becomes science. The reason I am concerned about this is because if you want to use that for ill effect, you can do some astronomically horrible things. This is a space in which we as a species need to get together on. If there were to be a movement for a convention on international behaviors and norms, this is a space where we would need to dedicate a lot of focus. We are incredibly vulnerable to this type of threat. We need to address that vulnerability as a nation. This not a DOD problem—this is an America problem.

How can we increase our competitive advantage with things like AI and machine learning?

We have to experiment with AI and understand it. We use technology every day that we do not understand. So, when we have conversations about AI and machine learning, we actually have to understand what it is and how it works.

What are our plans to train our military on AI and how it really works?

Part of that involves learning new tools. We have to pull in partners who understand how these things work. There are also some things that are dangerous with AI that we need to be aware of. One is that it becomes habitual. We also have to ensure that we have mechanisms for validating what AI tells us.

Joint Staff Remarks

Rear Admiral Jeffrey Czerewko, Deputy Director of Global Operations

RDML Jeffrey Czerewko connected the conference panels' themes to the current focus of the J39, and highlighted the role that the SMA community could play in assisting the J39's mission. He stressed that SMA's main advantage was its ability to tap multiple perspectives and methodologies to prevent insular thinking in three core issue areas: (a) understanding how different American competitors, such as China and Russia, understand global influence and resource competition below the level of armed conflict; (b) grappling with human and machine inputs in decision process to reduce misperception; and (c) assist in understanding when changes in technologies (e.g. AI) and international politics create new potentials for cooperation, deterrence of competition short of armed conflict, and leveraging whole-of-nation responses across multiple sources of national power.

Day 1, Panel 1: Opportunities and Risks of Stabilization

Moderator: Dr. Gwyneth Sutherlin (National Defense University)

- Dr. Spencer Meredith III (National Defense University)
- Dr. Laura Steckman (MITRE)
- Dr. Moritz Schuberth (Mercy Corps)
- Dr. Griffin Thompson (US State Department/Georgetown University)

Dr. Sutherlin opened discussion by noting a SMA White Paper on stabilization that was the inspiration for this panel. Like the White Paper, this panel had three audiences: “true academics” of cognitive cultural understandings, academic practitioners in the field, and operators. The discussion, which focused on how planning approaches were often forced to adapt to cultural issues, revealed two common threads united these various perspectives on stabilization: the importance of observation and the importance of (active) listening of local elements.

Dr. Meredith identified the criticality of culture in understanding and working through the challenges of post-conflict stabilization, noting the importance of setting the goal of “moving forward” earlier than the termination of conflict itself. The example of Ukraine and considerations of the country without Crimea and Donbas revealed the complexities of interests and identities, as much as wounds suffered in the ongoing violence by Russia. He proposed that attempts fall too far to one side; US policy, principally driven by partner perspectives or without their consideration all together, has been and will continue to fail. Some combination of core US interests and partner goals can expand the conceivable win-set, thereby advancing partner needs while also gaining strategic advantage for the US against great power rivals.

Dr. Steckman began by discussing her fieldwork in East Timor (also known as Timor-Leste) in which UN peacekeepers policed and enforced quality of life ordinances that were not a part of the local cultural understandings of law and compliance. This differing approach to enforcement compounded the coordination issues UN peacekeepers were already having with local police departments.

Dr. Schuberth continued by leveraging the example of gangs in Haiti interacting with peacekeepers. In Haiti, the sheer number and scope of foreign actors ostensibly there to provide social services came across to the local population as quite incoherent. Local Haitian gangs were better at observing and listening to local needs, and able to outwit foreign actors by portraying themselves as defenders of the neighborhood. Dr. Schuberth then pointed out that in 2008 Georgia, the models of addressing grievances didn't take into account the collective sense of victimization, and in not listening, pushed for *unilateral forgiveness* to overcome grievances, which was not effective.

Dr. Thompson argued that the otherwise nebulous idea of "culture" that is integral to stabilization, might simply mean less formal systems of social organization found inside civic organizations. Dr. Thompson illuminated this point with an example of the diversity of motivations and influences on consumer behavior, and noted that even such mundane things as energy infrastructure planning, would need to take consumer behavior cultures into account. The chief problems of stabilization are distributional problem and civic engagement. Dr. Thompson noted that foreign powers, trying to leverage economics of scale in their interventions, viewed all problems as solvable through either automation or machines; these approaches arise out of a larger political culture within the most powerful countries of seeing political questions as technological questions. Instead, stabilization planners should think of the strategic environment as being characterized by under-utilized civic cultures (plural) that can be mobilized to solve distributional problems.

Day 1, Panel 2: The Near Fight – USCENTCOM, USAFRICOM

Moderator: Ms. Sarah Canna (NSI)

- Dr. Sabrina Pagano (NSI)
- Mr. Vern Liebl, (USMC CAOCL)
- Ambassador Erica Barks-Ruggles (National Defense University)
- LTC Mike Maloney (USASOC G3)

Ms. Canna introduced the panel, which took a deep look into the ongoing conflicts in the Middle East and Africa. Focusing on non-state actors and partner nations, while drawing attention to emerging regional and global competition spaces in the region, panelists examined enduring challenges in these regions. The panel started with a look at internal stability dynamics within Afghanistan, and then looked at regional dynamics that may hinder a political settlement there, before turning the audience's attention to the ongoing conflict in Syria and—finally--irregular warfare challenges in Africa.

Dr. Pagano began by presenting a 2019 update to NSI's initial 2018 Pathways Model™ assessment for Afghanistan. She indicated that Afghanistan has remained since 2018 on a muddling along (status quo) pathway, but has moved closer to muddling down (a slow decrease in stability), largely due to social decline (e.g., in physical safety, social mobility). Dr. Pagano then illustrated that a failed Afghanistan would not be in the interest of the US, China, or Russia. Next, she characterized the interaction between the states' interests—from identical to zero-sum—in the global setting. She demonstrated that—while China and Russia's (short-term) interests are largely complementary or even identical to one another—US interests often range from competitive to zero-sum with China and Russia, making coordination unlikely. Dr. Pagano concluded by emphasizing the importance of examining these different levels of analysis—both the country-specific and the global—in the context of global competition and conflict.

Mr. Liebl took a more granular look at the Taliban in Afghanistan that is comprised of many different factions that are multidimensional and more complex than many believe. The complex structure of the Taliban and the many different governments that have previously risen and fallen, support an ongoing narrative of a country that relies on tribal structures and refuses to be governed from the center by a national government. Mr. Liebl also highlighted that the Taliban's version of successful negotiations results in the US leaving the region is also something that Pakistan also wants. The US wants to cut ties and leave; thereby cutting economic losses, but is cautious due to the high degree of uncertainty that would result from the departure of US presence from the region.

LTC Maloney began his presentation with a shift from Afghanistan to Syria, which has emerged an epicenter of great power competition in the Middle East as conflicting actors see the opportunity for both cooperation and conflict through combatting the Islamic State. The various actors involved approach the competition within Syria differently as the US, China, and Russia all see differing opportunities to expand their interests. The US, Iran, and China—who would rather not be involved—see a need for stability in order for their economic and energy initiatives while Russia sees the opportunity to launch experimental military operations against ISIS and even the US, in order to gauge what the US's response is to military aggression.

AMB Barks-Ruggles spoke on Africa's large youth bulge and how a lack of supporting economic infrastructure to ensure jobs has led to mass human migration to Europe through ports in Northern Africa and led to unemployed youth being attracted to militant activity in Boko Haram, AQIM, Al-Shabaab and numerous other VEOs. AMB Barks-Ruggles also stated that China has significantly expanded infrastructure investment into Africa, overtaking the US in investments in 2008 with a 4000% increase since then. The increased investment into African entities has also been exploited by China to foster debt traps that increase Beijing's control of critical infrastructure such as ports, roads and airports in several African countries.

Question & Answer Session

(*Italics indicates questions from the audience.*)

Would we be better disposed to create instability in Africa and potentially other regions where China is funneling money? (A change in strategy from escalating investing)

AMB Barks-Ruggles responded by stating that China has not previously engaged in addressing instability in the same way as the United States and other European countries. Therefore, it does not have as much concerned about instability in Africa. She pointed out that the United States works best in law-based societies with predictable political and economic environments whereas China operates very well in less stable environments, and does not ascribe to the same anti-corruption codes as the West, which give it an advantage in winning contracts, but also has led a number of African states into debt traps.

Ms. Canna asserted that if the United States is to become involved deep enough in a region or state that the effect on the great powers competition needs to be identified clearly beforehand.

What are the migration patterns out of Africa into Europe?

AMB Barks-Ruggles said many of the people migrating from Africa are not able to come through the Middle East due to geographical constraints and conflicts affecting the potential routes through that region. Instead, the majority of African migrants enter Europe through ports via boats from Libya, Morocco, and Algeria. This trend will likely continue if Africa's economies do not grow sufficiently to provide employment for its growing youth bulge.

If the United States was to find a partner for humanitarian situations to take some of the burden and pressure from the US and transfer some to its partner, would this allow the US to gain more influence over the situation?

LTC Maloney pointed out that partnering with other institutions would not only aid the US toward reaching its goals but also will keep them from becoming partners with our potential adversaries.

AMB Barks-Ruggles said that while partnering with other countries is beneficial, the United States should not slow down its own engagement or involvement with countries in sub-Saharan Africa. Through our active engagement since the mid-1990s, the United States has built credibility, grown indigenous capacity and skills to improve partnership with African nations, and has generated influence throughout the continent that has benefitted both the US and our African partners. This should be viewed as a long-term investment in relations, not as a quid pro quo or mercantile relationship.

Department of Defense Remarks

Dr. Charles Perkins (Principal Deputy for Emerging Capability & Prototyping)

In his role overseeing prototyping and experimentation for the Department of Defense (R&E), Dr. Perkins often starts by evaluating what could possibly go wrong. The DOD spends a lot of time thinking about material solutions to warfare, but we do not spend enough time thinking about cognitive warfare, something that is changing rapidly as can be seen by the themes driving this conference. Cognitive warfare tools include artificial intelligence, machine learning, and other cyber tools. In the spiral to warfare, how do we use these cognitive tools to slow down escalation so that we do not spiral out of control. These same tools and techniques also provide indicators and warning of when conflict might exceed the competition space. These are the tools we will rely on to stay in phases one and zero. The real challenge before us however, is in implementing new technological developments in this sphere so that we can stay in phase zero.

Keynote Speaker

Lieutenant General John N. T. Shanahan (Director, Joint Artificial Intelligence Center)

Emerging Technologies and Peer Competition: The Vanishing Luxury of Time

For those who don't already know me, I served previously in the Under Secretary of Defense for Intelligence as the first Director of the Algorithmic Warfare Cross-Functional Team, also known as Project Maven, which was the Department's pathfinder project to integrate AI capabilities to augment, accelerate, and automate collection from a variety of manned and unmanned ISR platforms and sensors. I've now been in the seat as the Director of the Joint AI Center, or JAIC, for almost five months. With the mission to accelerate DoD's adoption and integration of AI to achieve mission impact at scale.

Most of what I am going to speak about today concerns the future; an emerging revolution in technology that will play a central role in the future of military power and the future of global strategic competition, in particular with China and Russia. Before I do that, however, I must revert to the past.

My entire 35-year career has been in an Air Force uniform, with extensive joint experience. A great deal has changed since I entered my service in 1984. When I began my journey, what is now known as the military information technology revolution—what former Deputy Secretary Bob Work would describe as a major component of the Second Offset—was reaching its early crescendo. Technologies such as precision-guided munitions, stealth aircraft, and digital command, control, communications, and intelligence networks carried American military power to unprecedented heights. As a young officer, I could see the outlines of these major changes. But the rest of the world would not appreciate the full extent of America's military information technology revolution until the 1991 Gulf War. Many have forgotten this, but in the run-up to Desert Storm independent military experts testified before Congress that they anticipated 100,000 or more U.S. casualties. This did not seem nearly as ludicrous then as it does today. In 1990, Saddam Hussein's Iraq possessed the world's 6th-largest military, equipped with some of the best weapons technology ever exported by the Soviet Union. In actuality, of course, Iraq was no match for the United States and our allies and partners. The 700,000 American men and women serving in Desert Shield and Desert Storm suffered *fewer than 200 combat deaths*. Iraq's military capitulated astonishingly fast.

Desert Storm showed the world in unmistakable terms what it meant to be on the right—or the wrong—side of a military information technology revolution. Well-trained and well-led American and allied warfighters—equipped with a revolutionary technological edge—inflicted a stunning defeat upon Iraq. We were the first military in the world to capitalize on the information technology revolution.

When Desert Shield kicked off, I was in the last of the three F-4E squadrons at Seymour Johnson AFB in North Carolina to convert to the F-15E Strike Eagle. We knew the other two recently converted squadrons were heading to the fight. Our timing was bad, to say the least, as we would not convert until Desert Storm was already over. Yet we were itching to deploy with our F-4 Phantoms. We were at the top of our game. Our TTPs[1] were finely honed. We were a tight-knit team, with the most experienced aircrews ever assembled. We could read each other's minds when flying. We had new technology: I had recently successfully guided the first Infrared GBU-15 from an operational F-4E, at night; we were even projected to replace our ancient AIM-9Ps with mighty AIM-9Ls. Alas, politics are timeless, and the decision was to send the shiny new Strike Eagles and keep our dirty, ugly, yet high-performing Phantoms at home.

I mention this not so I can get all misty-eyed with fond remembrances of almost three decades past, but because of what I gleaned while watching my two sister squadrons learn how to fly and fight with their new airplanes as they prepared for war. While the airplanes themselves were an incredible improvement over the F-4, they were far from technologically mature. Some airplanes deployed initially without the LANTIRN navigation pods, while during the war only half of the jets carried a targeting pod. There were a lot of bugs in the new software—not a problem we experienced in our steam-driven F-4s. At the same time, a mix of former F-4, F-111, and A-10 aircrews had to figure out how to employ the new airplanes. They had the luxury of time during Desert Shield to figure out how to integrate new technology such as LANTIRN, precision-guided weapons, and terrain following radar along with new operational concepts such as buddy lasing. Supported by an amazing enterprise comprising unprecedented amounts and types of ISR, SIGINT, and C2[2]. Even with this luxury of time, however, the crews learned that they had to invent or reinvent ways of employing the new airplane. They also learned the hard way that the tactics we had all been training for – low altitude ingress at night against Iraq's formidable integrated air defense system – were absolutely the wrong approach. Leading to the tragic loss of an airplane and aircrew on night one of the war. And it turned out that maximizing the Strike Eagle's strengths meant flying it a lot more like

[1] Tactics, techniques, and procedures

[2] Intelligence, surveillance, and reconnaissance; Signals intelligence; and Command and control

an F-15C than an F-4 or F-111. When it was all said and done, however, when multiplied across every unit in every Service, the luxury of preparation time proved instrumental to our lopsided coalition success in Desert Storm.

Nearly thirty years later, we are on the cusp of another military revolution, one that builds upon the military information technology revolution and augments it with an intelligent technology revolution.

I've had the opportunity to witness first-hand the early stages of this military intelligent technology revolution. Everything I've observed over the past few years has convinced me that the implications of this new revolution will be every bit as profound and significant as the last one. *Fortunately*, there are others in the Department of Defense who also recognize this. *Unfortunately*, this is also exactly how Chinese military leaders describe the current moment—an *intelligent technology* revolution that will be more impactful than the prior information technology revolution. I will address China's AI strategy more shortly.

In 2017, the Department of Defense stood up the Algorithmic Warfare Cross Functional Team, aka Project Maven. (Pause for a moment to think about the name—just the title algorithmic warfare suggested a very different kind of future than almost anybody was anticipating merely two years ago.) Maven was the pathfinder project to operationally deploy capabilities at scale to make effective use of modern deep learning AI. We chose computer vision as our initial AI application, analyzing full motion video from tactical and medium-altitude remotely piloted aircraft.

In my previous assignment, I commanded 25th Air Force. Every minute of every hour of every day across the global ISR enterprise we experienced "success catastrophes" of the military information revolution. We continuously collected an astounding amount of information in the form of digital sensor data. We had oceans of data, but our only fishing nets—human eyes—were miniscule. The collection we managed from manned and unmanned aerial platforms were equipped with extraordinary sensors that generate massive amounts of data, and we could never keep up. Initial victory in the information revolution had spawned defeat from a data deluge, one in which the principal problem was not that we collected too little data, but that we collected so much that it was nearly impossible to analyze at the speed of operational relevance. We were hardly unique; it's been the same story across the entire National Intelligence Community and Defense Intelligence Enterprise. For every platform and every sensor in every domain.

Rather than try to tackle all of those data domain problems at once, Maven started with a single computer vision project because we sought a manageable, meaningful, tangible problem for which there were already existing commercial AI solutions. What started as a single line of effort two years ago has since expanded rapidly into a dozen different LOEs[3] today. With a true agile Sprint fielding approach, modeled after commercial best practices. Now moving to enterprise scale with cloud-based solutions.

While the Maven team is still a long way from declaring success and proving full return on investment, we have seen enough of the future to be truly energized about the potential for Smart Systems, ops-intel

[3] Lines of effort

fusion, and AI-enabled mission command to fundamentally change the future analytic and operations workforce.

I am tremendously proud of what we achieved with Maven, but it remains one project for one part of DoD. If we stop here, we will fail to come to terms with the full implications of the military AI revolution. Which will impact every corner of the Department, from the back office to the tactical edge. Shifting every part of DoD into a data-centric architecture and data-driven battle rhythm is a critical prerequisite toward seizing the potential of the AI revolution. We still have a long way to go.

Maven will continue to scale and accomplish extraordinary things. Yet, even in success, Maven demonstrated just how many obstacles—some of which can seem insurmountable at times—stand in the way of our military seizing upon AI's full potential. Thanks to the personal involvement of the Deputy Secretary of Defense, in 2017 we were able to go from receipt of funding to an operationally-fielded prototype algorithm in the hands of warfighters in six months. With a dozen updated versions of that initial algorithm deployed within eight months. That's lightning speed for DoD, but still a snail's pace as compared to commercial industry. We're trying to figure out how to bolt the newest technology on to legacy systems. That approach just doesn't work. It is also entirely unsustainable. The combination of legacy systems, legacy workflows, lack of a data-centric culture, and failure to appreciate the monumental retooling required across the Department is a recipe for calamity.

Maven underscores just how deep the chasm is between the commercial tech community and the AI capabilities of DoD and our traditional defense industrial base. This is nearly a complete reversal from how we operated over the previous 50 years; commercial tech is far outpacing DoD's ability to keep up. AI-centered vendors treat digital data as a core part of every aspect of their business and operational DNA. Collecting, storing, refining, and making decisions with terabytes of data is not only business as usual, it has been business as usual for more than a decade. By contrast, too many parts of the DoD are either collecting data using pen-and-paper methods, or, worse, they are treating data like engine exhaust: a useless byproduct. This is a catastrophic mistake, and one that our strategic competitors are avoiding. As Chris Brose of the Carnegie Endowment pointed out, China's military "is moving with authoritarian zeal to stockpile its data like oil, so that it can power the autonomous and intelligent military systems it sees as critical to dominance in future warfare."

DoD can never realize the full potential of the military AI revolution unless it addresses the long-lead items of AI transformation and digital modernization. Incidentally, digital modernization and warfighting modernization are synonymous. There are many communities within DoD that are not awash in data but *should* be and *would* be if they truly embraced the digital transformation that has become routine in American commercial industry. We must urgently begin collecting, digitizing, and curating data across the full spectrum of our operations—including business processes, logistics, training, intelligence, and combat. Commercial tech companies have focused on these AI long lead tasks for more nearly two decades, and they have reaped astonishing benefits. The top five largest companies in the S&P 500 stock market index are all technology companies that put AI at the core of their business. These companies are each worth nearly 1 trillion dollars in market valuation. Their combined market valuation is greater than the bottom 200 companies of the S&P 500 combined. That success is testimony to the power of a data-driven business strategy that recognizes the true potential of AI. We must take the same approach. We need to spend as much time working with the National Security Innovation Base as we do with the Defense Industrial Base. It's not one or the other. It must be both. Or we will fail.

Unfortunately, the United States is not the only country to have learned these lessons. China, in particular, is betting heavily on artificial intelligence as the future basis of conventional military superiority. And so now I would like to address head on the issue of AI strategic competition with China.

To begin, I go back to 1953, when the Soviet Union launched its Sputnik satellite into space. Sputnik's launch simultaneously revealed to the United States that we were behind in space and rocketry technology and that these technologies were going to be a critical aspect of Cold War strategic competition. In response to the Sputnik crisis, the United States took radical action, including creating two legendary organizations—DARPA and NASA—and even passing the National Defense Education Act, which increased federal spending on science and mathematics education by billions in today's dollars. We were on the moon within a decade.

In 2016, China had its Sputnik moment for AI. That was the year that Google DeepMind's AlphaGo AI system defeated the world champion in the traditional Chinese board game of Go. As everyone understands by now, the game of Go is many orders of magnitude more mathematically complex than chess and is deeply woven into Chinese culture. Having an AI system defeat a human grandmaster had been a stated moonshot goal in AI research for decades. In the United States only 100,000 people watched the AlphaGo match live. In China, more than *sixty million people* watched the match live. Like Sputnik, AlphaGo's defeat of Lee Sedol and Ke Jie convinced China's leaders in both business and the military that AI technology would be as critical to the future of global power competition as rocketry was in the 1950s and 1960s. Like America during the Sputnik crisis, China quickly responded to AlphaGo with a whole-of-nation leap-ahead effort, spending tens of billions of dollars to accelerate AI initiatives across government, the military, and the private sector. China even passed major reforms to its education system to incorporate new AI-focused curricula and massively expand its annual number of computer science graduates.

China's leadership, from the provincial level all the way to Communist Party General Secretary Xi Jinping, believe that leadership in AI is critical to the future of global power competition. China's government and Chinese companies are investing tens of billions to ensure they come out on top.

What does China have to show for their efforts? Quite a lot, actually. Chinese programmers—including teams from the Chinese People's Liberation Army—now routinely win international machine learning programming competitions. At top international AI conferences, Chinese researchers often present the greatest number of papers, and Chinese papers are becoming among the most highly regarded by other researchers around the world.

I suspect there are many in this audience who believe, as I once did, that China's authoritarian system and rote memorization education model mean that Chinese companies and labs cannot innovate, but merely copy. Perhaps this was true a decade or two ago, but times have changed. Irrevocably. I have personally spoken with many of the leading American AI researchers and CEOs of America's top AI companies. They tell me that the current quality of Chinese AI research and commercial AI product development is state-of-the-art. Chinese AI companies are generating billions of dollars annually in revenue and profit, producing software and hardware AI products that are increasingly competitive with what comes out of Silicon Valley. Chinese peer competitiveness with the United States in AI technology is not some worrisome potential future scenario. It is the reality that American companies face when competing in global markets today.

China is now working to translate this commercial market and academic research AI success into military power. Chinese military leaders and China's 2017 AI strategy state unequivocally and publicly that AI offers an opportunity to leapfrog American military superiority. China believes that their relative competitive disadvantages in—for example—aircraft carriers will actually be offset by the advantages accrued through rapid military adoption of AI at scale. China is betting that our military-industrial-political complex will make the fatal mistake of only using AI to upgrade our legacy systems while we try to arrange forced marriages between legacy doctrine and operating concepts, and leading-edge AI technology. China, on the other hand, wants to completely rethink military doctrine and operating concepts for an AI-enabled era. In China's leapfrogging mindset, the dominant military technologies of the future will in many ways more closely resemble today's commercial AI technologies than they do extant military ones. Our near-term military edge is likely to become a major long-term disadvantage in strategic technology competition. Put another way, China intends to offset our offset.

China's theory of victory in AI competition also assumes that the People's Liberation Army will be in a better position than DoD will to exploit commercial AI technology for military purposes. China's government has more tools to incentivize or even coerce the best of their country's commercial and academic AI talent to assist in military projects. Through the Chinese government's explicitly-stated policy of civil-military fusion and through China's National Intelligence Law, Chinese commercial companies and universities can be compelled to work on military and espionage technology projects. China's best and brightest can essentially be drafted at any time to assist in developing military AI technology.

Such coercion often isn't even necessary. The Chinese government is already the largest and most profitable customer for many Chinese AI companies involved in domestic surveillance and security. The current Chinese regime views America's cultural influence and promotion of democratic values as a threat to state stability and the regime's control over the Chinese population. This fear of its own population has pushed the government to be an early adopter of AI for surveillance, censorship, and public opinion manipulation. AI-enabled video, audio, and internet surveillance is a multi-billion dollar market in China, with government customers as the largest spenders dominating the market.

The Chinese domestic security apparatus is an AI early adopter, with the Chinese military close behind. The People's Liberation Army (PLA) is developing a diverse set of offensive and defensive AI capabilities across military robotics, autonomous systems, strategic planning, ISR, cyber, and more.

I don't mean to suggest that the Chinese military is an unstoppable technological juggernaut and that all of these projects will succeed. AI is not easy, and there aren't any AI silver bullets. The PLA will experience the same challenges and learn the same lessons we did with Maven. Moreover, many of China's AI projects are ill-conceived and will likely fail. But their willingness to take technological risk, learn from setbacks, and move forward relentlessly is something we cannot ignore. China has made significant progress on each of the elements of its AI strategy in recent years. When you put enough people and apply enough resources against any problem, eventually you will get where you're trying to go. It would be naïve—disastrous even—to assume that business as usual in the DoD will be effective at countering this strategy. The table stakes are clear: our military superiority, and our ability to credibly deter Chinese aggression against the U.S. and our allies and partners.

China is not the only strategic competitor aggressively pursuing military AI. I'm sure all of you are familiar with Putin's 2017 quote about the nation who leads in AI will rule the world. Unlike China, Russia does not currently have a credible path to being a leader in academic AI research or commercial AI product development. However, Russia was not a leader in either of those areas for internet technology.

Nevertheless, they developed formidable military cyber capabilities and internet disinformation operations that we've seen used against us with major impacts. As with the internet, Russia is not likely to be a leader in commercial AI, but there's little question they will seek to be a leader in weaponizing AI against the United States and our allies. We underestimate Russia at our peril.

We can rise to this challenge. Just as we have risen to many others like it in the past. Success will require that we speak candidly about the risks we face and appreciate the magnitude of the response and change required. The luxury of time is dwindling fast, if it hasn't already vanished.

So what can be done? To respond to this challenge we must make three core commitments. I will address each in turn.

First, we must commit to the reforms necessary for superior AI technology adoption capacity. China's strategy is premised on the hypothesis that they will be better at military adoption of AI than the United States will—both by superior commercial-military technology relationships and by a greater flexibility in reorganizing their military around AI technology, especially commercial AI tech. We cannot live down to Chinese expectations. We must improve our ability to access, adopt, and sustain commercial technology from the United States and partner nations. This will require major reforms to our culture of technology development, acquisition, fielding, sustainment, and program management approaches – issues long bandied about but never adequately addressed. It requires improving career prospects for those with the requisite technical skills, in both military and civilian ranks. It means ensuring that senior leaders responsible for major resource decisions in the Services, Agencies, and Components have the necessary depth and breadth of technical understanding. More akin, perhaps, to the training and promotion track of the nuclear Navy than the traditional promotion policies that have favored management breadth over technical depth.

Next, we must commit to fostering new concepts of operations and new organizations that recognize the potential of digital transformation and AI technology. I agree with those who suggest we are in a period equivalent to the interwar period of the 1930s. We must blend new technologies with new operating concepts, relying extensively on experimentation, wargames, and modeling and simulation to grasp the AI art of the possible while we still have a sliver of the luxury of time.

Above all, embracing the future will require a willingness not only to invest in the new, but also to make room by divesting the old. Where the Department observes technology trends that are unfavorable and yet inevitable, we should not waste time and resources doubling down. Instead, we should demonstrate a willingness to invest in technologies and operating approaches that might challenge our existing platforms and sources of advantage. Equally if not even more important, we must find and protect the AI mavericks, disruptors, and innovators. Those who refuse to accept the status quo. Who might be perceived as cranky and obstinate glass-breakers today, yet who through the lens of history will be viewed as true visionaries.

Given our strategic competition goals, we should think about what an ideal military would look like were we to start from a clean sheet, then let those insights inform our priorities and chosen path. Many if not most legacy systems will need to be abandoned or at a minimum gradually phased out over the next decade. Our objective should be to link those legacy systems with enduring utility to the new world of AI while avoiding the historical mistake of allowing legacy systems to consume so many resources that they leave DoD AI stunted from malnourishment.

Third, we must update our commitment to our system of alliances to account for technological change. Gauged against the United States and its allies globally, China is still by far the weaker competitor and is likely remain so. Thus, our success will depend in part upon the level of cohesion, firmness, and vigor that the U.S. system of alliances can demonstrate. AI can feed alliance cohesion. It can also feed alliance fragmentation. This is not a unilateral world. It still takes two or more to tango. Accordingly, we need thoughtful strategies about how and how much to share with allies, and how to ensure equal voices in the conversation from the beginning, not a decade from now.

These steps cannot succeed if they are perceived as illegitimate or even questionable in the eyes of the American public and America's allies. The DoD and other federal agencies must therefore do more to educate the United States public about China's strategy and the threat it poses to America's safety and vital national interests. It is a shocking public communications failure that some American and international groups protest American technology companies working with the military but are largely silent when American universities and companies announce large technology partnerships with Chinese universities and companies that have deep ties to China's military and/or government human rights abuses.

We must shine a spotlight on Chinese military's AI modernization and the international help they are receiving. China's technological gains have been enabled by its largely unrestricted access to global technology networks and markets. We also need to understand how we can make military AI capabilities less susceptible to theft, replication, denial, deception, or defeat. CFIUS reform, export controls, and sanctions are welcome steps in this strategy, but we can do more.

On the more optimistic side of the ledger, leaders in the White House, Congress, and the national security community recognize the challenge China's rise in AI poses to our collective security and are taking significant steps in the right directions. Beginning with the 2018 National Defense Strategy, which appropriately named AI and advanced autonomous systems as priority areas of investment for sustained competitive advantage. Followed this year by the White House Executive Order on AI, and the release of DoD's unclassified summary of its AI strategy, which directs the DoD to "accelerate the adoption of AI and the creation of a force fit for our time." Moreover, within the past week the administration has placed further restrictions on exports of our critical technologies, and I've seen new draft congressional legislative proposals that will constrain China's ability to act with impunity in our academic institutions and research labs.

Under the mandate of the DoD AI Strategy and Congressional legislation, we stood up the Joint Artificial Intelligence Center under the DoD CIO. The JAIC is a nascent but rapidly-growing organization. I only assumed my current position in January, and we received the bulk of our FY19 funds just three months ago. Still, we are moving out with alacrity to address each of the pillars of the DoD AI strategy, first and foremost of which is delivering AI-enabled capabilities in operationally-relevant timelines. In everything we do, we are motivated by a singular focus, passion, and dedication to improving support for the warfighter.

We benefit greatly from our collaboration with the intel community and with USD(R&E) to include DIU, DARPA, and the Strategic Capabilities Office, to improve integration and enhance unity of effort on current and future AI projects. We need to continue strengthening our partnerships across the Services, Agencies, and OSD Components. We need more allies across the DoD who understand the importance of the military human-centered AI revolution and are willing to do what it takes to rise to the challenge.

In closing, Desert Storm was a lifetime ago. We no longer have the luxury of time to prepare for the next fight. We've already moved beyond competition into conflict. We are in a fight today – in space, cyberspace, and the information environment. We've gone from owning the temporal advantage, to being at serious risk of ceding it completely. We understand the imperative: how to blend new operating concepts with new technologies. Now we have to do it. Whoever designs a data-centric warfighting operating concept that adopts and integrates AI, cloud, 5G, and quantum will gain a decisive upper hand. This AI-enabled transformation will unfold across the next decade. The critical question will be how thoroughly we embrace change. In AlphaGo, China already faced their AI "Sputnik moment." If we wait any longer for one of our own, we'll be too far behind. We're not in an AI arms race—a term I studiously avoid—yet there's no doubt we are in a major strategic competition. And we cannot afford any more delays. If anyone can help us figure this out, it's the collective grey matter represented in this audience. I implore all of you to help us chart the path for that inevitable AI-enabled future.

Day 1, Panel 3: The Nearing Fight – USEUCOM, USINDOPACOM, USSOUTHCOM

Moderator: Dr. Barnett Koven, University of Maryland/START)

- Mr. Adam Fields (Bureau of Conflict and Stabilization Operations/EAP-SCA)
- Dr. David Dorondo (Western Carolina University)
- Dr. Fabiana Perera (William J. Perry Center for Hemispheric Defense Studies)

Dr. Koven introduced this panel as a discussion of Chinese and Russian ambitions in within the USEUCOM, USINDOPCOM, and USSOUTHCOM AORs. He added that the precise way near-peer competitors and nations compete varies across nations, but the end goal is the same. Mr. Fields opened the floor by discussing partner nation strategy concerning Southeast Asia and the need for the United States to empathize with its partner nations. With respect to Southeast Asia, strategic hedging (e.g., pursuing mutually counteracting policies in order to maintain a semblance of neutrality while at the same time maintaining multiple fallback positions at a time when the future power structure is unclear clear) is a common strategy small countries adopt in the face of great power competition. In understanding this strategy, Mr. Fields suggested the United States should envision Southeast Asia as a "pivotal" region (i.e. a region that wants to pivot between the great powers) and pursue policies that help Southeast Asian countries protect their identity, sovereignty, and autonomy. This allows these nations to remain independent (i.e., pivotal), rather than becoming locked into a Chinese-led neo-tributary system. A "pivotal" Southeast Asia would ensure US values remain competitive and something countries in the region are free to choose, reject, localize, or aspire to.

Dr. Dorondo began his panel portion by denoting that the "nearing fight" isn't actually nearing, but rather is occurring in the present. Shifting his focus to Europe, he remarked that the region is embroiled in political warfare that is primarily non-kinetic, and Russian military ventures exist in cyberspace and ongoing disinformation campaigns. Several upcoming regional and national elections in the fall of 2019 are battlegrounds for influence, and certain actors in countries such as Austria are political Trojan Horses in the Russian-NATO conflict that will disrupt and fracture NATO-EU security. This is further complicated by the uncertainty of a post-Putin Russia in 2024 and that country' s stagnant economy that must face an increasing Chinese presence across Europe.

Dr. Perera shifted the focus to the Western Hemisphere and highlighted the diminishing US influence in the region. She underscored Venezuela as a key example of this development and discussed the evolution of Caracas from a key US partner that underwent a period of inaction and natural crises, and saw Chavez pursue new relationships with anti-Western nations (Iran, Syria etc.). The contemporary state of Venezuela is dominated by Chinese economically incentivized investment, and strategically incentivized Russian investment. Dr. Perera concluded that the current situation in Venezuela is a good opportunity for the US to support (economically and strategically) the rise of a democratic government.

Dr. Koven continued the focus on the USSOUTHCOM AOR by discussing Colombia, and began by emphasizing that Bogota is a key security partner for the US, and therefore of interest to China and Russia. He stated that Russia's involvement in Latin America, as a whole, is a direct response to US engagement in areas that Russia views as part of its traditional sphere of influence, like Ukraine. With respect to Colombia, Russia has been engaging in influence operations in Colombian media, specifically to cultivate skepticism over the Revolutionary Armed Forces of Colombia (FARC) peace process. Although Russia is relatively more active in Colombia, China does have limited economic involvement. They are especially interested in resource extraction. Dr. Koven concluded by suggesting a whole of government approach that can leverage regional partnerships and counter disinformation campaigns.

Day 1, Panel 4: Cooperation, Competition, and Armed Conflict: Globally-Integrated Campaigning for Today and Tomorrow

Moderator: Mr. Scott Kendrick (JS J3)

- Mr. Collin Agee, (Army GEOINT Office)
- Mr. Michael Ceroli (USASOC)
- Dr. Melanie Sisson (Stimson Center)
- LTC(P) JP Clark (Army War College)
- Mr. John Wallace (JS J3)

Mr. Kendrick framed the panel as a discussion of the realities of international relations that can influence the doctrine and practice of campaigning in competition, short of armed conflict. He explained that competition is not a new interpretation of deterrence, nor is it necessarily a prelude to armed conflict. Competition is its own unique, demanding, and indefinite contest where many aspects of malign influence and antagonistic behaviors are undeterrable. As such, we can either ignore these harmful activities at our own peril or seek to contest, counter, or even de-construct these adversarial approaches.

Mr. Agee presented the TRADOC depiction of the Operational Environment to 2035, highlighting the areas of potential competition and conflict. He noted that, after nearly two decades focused on counterinsurgency, the Army's pacing threats are shifting to peer and near-peer competitors, specifically Russia and China. He noted that our potential adversaries have closely watched US operations in the Middle East and are making great strides in areas such as counter-space, cyber, social media, and unmanned aerial vehicles (UAVs). Aware that they are overmatched conventionally, they will challenge us asymmetrically, and some areas in which we have long enjoyed overmatch, are increasingly at risk. He also noted the challenges posed by non-state actors, and the consistent challenges that present themselves during competition—that is, "peacetime"—short of a state of war.

Mr. Ceroli offered several thoughts. First, technological advancements provide DoD a high-speed avenue of approach to people and populations in previously denied territory. This is generating a renewed interest in using information to achieve US objectives. The Marines have established a 3-star Deputy Commandant for Information. The Air Force is recapitalizing their Information Warfare Flights. The Army has renamed ARCYBER as the Information Warfare Command. As you will hear later in this panel, the Army is also experimenting and developing the concept of Multi-Domain Operations (MDO) where peer competitors contest all domains, the electro magnetic spectrum (EMS), and the information environment. One of the tenets of MDO is convergence. The Army is currently experimenting to rapidly and continuously integrate the capabilities in all domains, the EMS and information environment to achieve a position of advantage. This renewed interest in the information environment requires new processes and structures to coordinate and synchronize physical and informational objectives for maximum effect. Mr. Ceroli's second point was that as DOD and the Services experiment with the use of information to achieve military objectives and support US National objectives, he has noticed two schools of thought: One school plans and executes information as a fire supporting maneuver. The other school of thought uses information as a form of maneuver. Both approaches have pros and cons. A common aspect the two schools share is establishing cognitive objectives at the campaign level supports centralized planning and de-centralized execution. These cognitive objectives also promote initiative and embody the philosophy of mission command. The third point is one of caution. Given this new access to people and the global information environment, when we say we are conducting strategic information operations, communication, or psychological operations, our civilian leaders take notice. The historic result has been policy restrictions or cuts in funding that negatively impact our ability to use information in support of military objectives. A thought is to state in our documents that DOD uses information in the operational to tactical levels of warfare to achieve military objectives and in support of US National Objectives.

Dr. Sisson's comments focused on understanding the role of the US military in competition. She offered a definition of competition as the ongoing pursuit of advantage, in which states vie to have their interests privileged in international rules, norms, and institutions, and work to minimize the frequency with which those interests are challenged. When challenges do arise, however, the military is a powerful asset available for use in pursuing US foreign policy goals not through war, but through coercion. Effective military coercion requires accounting for the international political and economic context; understanding the target state's incentive structure; communicating demands and the consequences of non-compliance clearly; and using the armed forces in combinations and in ways that make success more rather than less likely. Effective coercive strategy therefore requires the integration of military operations with the full complement of diplomatic, economic, and cultural levers of foreign policy.

LTC(P) Clark agreed with fellow panelists that the United States must change its way of thinking. LTC(P) Clark noted that the soon-to-be-published Joint Doctrine Note on the competition continuum would offer a different perspective in doctrine to reflect the dynamic environment. The competition continuum is a departure from the old peace/war binary that still underpins many defense processes. The new approach will better align DoD with interagency partners and is being picked up by allies, as well.

Mr. Wallace again emphasized that the big ideas of global integration translates to increased military competency and ability. He then stressed that the integration of new technology is vital to the US in the age of great power competition. This integration globally and across operational domains is a challenge and the difficulty is most apparent in competitions short of armed conflict.

Question & Answer Session

(*Italics indicates questions from the audience.*)

Using the concept of nested understanding, does the process include cognitive objectives and how can you justify these objectives without hard data?

LTC(P) Clark answered by noting that it is crucial that joint doctrine needs to be able to describe objectives well and clearly. Not being married to the data allows for nuance in how resources are allocated so that the issue can be addressed according to the environment as it changes. He said this was an example of centralized planning in a decentralized way.

Should the long-term plan be more than five years?

The panelists acknowledged that the decision makers are held hostage to institutional timelines. However, they did bring up the concern that the Joint Chiefs and the military is looking for short-term plans for a much longer war.

Who is constructing the strategy for future warfare beyond the five-year plan?

LTC(P) Clark said that nobody is doing an extremely long-term analysis. He said the closest thing is the J-5, which reevaluates organizational processes for 2028. He also pointed out that part of the issue is changing civil policy and that the military does not belong in policy-making scenarios.

How does the military ensure its allies when the DFE takes soldiers and reallocates them to another place that it is in the best interest for all?

The panelists agreed that the reallocation of forces is a function of a reprioritization of an on-going global campaigning effort. They stated it is a constant educational process both for the United States and its allies on how and why this is important. This relationship is due to the decision being placed on a cost-benefit scale on whether or not an action or exercise is taken.

Day 1, Panel: 5 Pushing Boundaries of the Domain Concept: the Criticality of the Non- Kinetic Toolkit

Moderator: Lt Gen (Ret.) Dr. Bob Elder (George Mason University)

- Mr. Mark Hoffman (Lockheed Martin Advanced Technology Laboratory)
- Dr. James Giordano (Georgetown University Med Ctr.)
- Ms. Regina Joseph (Pytho)
- Dr. Ian McCulloh (Accenture Federal Services)

Lt Gen (Ret.) Dr. Elder introduced the discussion by noting the rising activity in non-kinetic means of warfare, such as influence and coercion, and what this means for the DOD.

Mr. Hoffman began the panel by remarking that AI and machine learning are NOT a silver bullet, and they are not necessarily new or novel. He noted a recent DARPA paper that described AI's evolution as coming in waves, where there have been winters and springs during three successive revolutions dating back decades. The current third wave of AI research is now dedicated to the contextual adaptation of AI that seeks to make it less brittle and more relevant/useful to grey zone competition. Transferring human beliefs and understanding, while simultaneously increasing the transparency and contextual awareness of AI is the current frontier of innovation. Considering this, it is useful to conceive of AI as a journey, rather than a destination, as it is not static. Mr. Hoffman concluded by encouraging a whole of government approach to "distributed and collective AI" but warned that there will likely be continued future springs and winters of AI development in this ongoing journey

Dr. Giordano discussed the importance of understanding the human element in non-kinetic conflict and influence, with a focus on Chinese capabilities. He remarked that US competitors have been leveraging their own scientific, philosophical, cultural, and ethical capability to engage in types of research that

Western norms and ethics may not permit. Given this, the questions then become not what can be done, but what is currently being performed in emergent domains of competition and how will this affect US and global stability and security. China is moving expediently in this regard on three fronts: The first being the knowledge of the needs and values of Beijing's competitors (i.e., the West and specifically the US). The second being the ability to assess and penetrate those needs and values through information (e.g., AI, media, public opinion etc.). Third, understanding the biological basis of the way we interact in the psychological and social realms, to be able to influence our cognition and behavior. With all this in mind, competition is no longer as simple as hearts and minds, but is increasingly becoming a question of "affecting minds to then influence and shape the hearts of adversaries" at will. Dr. Giordano concluded by noting examples of how China is excelling in these areas of competition and are taking advantage of an increasing imbalances in and across numerous domains (e.g., biotechnology & bioscience, intellectual property, global investments) that China's integrated "triple-helix" of governmental-academic-commercial sectors empowers them to pursue through a whole-of-nation approach.

Ms. Joseph discussed the need to develop and evolve the defense community into a more technologically capable workforce, and noted that the shortfall of experts and skilled labor in AI and machine learning are affecting DOD readiness. She also remarked that utilizing the advancement of understanding of human intelligence can further assist the defense community in numerous areas (e.g., critical metacognitive & reasoning skills, digital information awareness, empathic intelligence etc.), and that micro-learning processes have shown promising results in mitigating these areas. There are also cultural and structural barriers to overcoming these shortfalls that are uniquely difficult, but not impossible to overcome. These barriers are especially relevant to the collective intelligence of the defense community that is operating in the non-kinetic environment. Despite an increasingly AI shaped world, human teams may be more competent than machines in certain areas in the non-kinetic space, further underscoring the need to resolve the aforementioned issues. Ms. Joseph concluded by noting that the true offset the US possesses is the freedom of information that citizens enjoy (which is something US adversaries lack), and the need to maintain the safe conduct and viability of this offset is imperative to the success of the US in the age of great power competition.

Dr. McCulloh expressed optimism on the adoption and adaptation of AI, the integration of AI into multi-domain battles, and the training of senior leaders to better utilize AI. He then described the genesis of deep learning from a nascent example of AI that could defeat a human at the game of checkers, and then related this to the development of his own work in AI. The problem set of the modern geo-political environment is far more complex than a game of checkers; however, simple iterations in the developmental processes of AI through human input and guidance can significantly manage and improve the implementation of an AI system. Specifically understanding the metrics (through subject matter experts) that are applied in the data labeling and data annotation phase can produce much better results. Dr. McCulloh concluded by arguing that the integration of the expertise that exists in DoD senior ranks is invaluable to improving AI systems from unacceptable error rates, to rates that are much superior to human only systems.

Day 2: Panel 1 Integrated Operations in a Dynamic Environment

Moderator: COL Paul T. Brooks (Joint Staff/J39)

- Mr. Bob Jones (USSOCOM)
- COL Gregory Beaudoin (USINDOPACOM)
- Mr. Tim Curry (USAFRICOM)
- CAPT Dan Stone (USNORTHCOM)
- CAPT Geoffrey Gage (OPNAV N3N5 Strategy Branch)
- Lt Col "Sloppy' Forrest (CHECKMATE)
- COL Jeffrey Brewster (USCENTCOM)
- LTC(P) George Corbari (USCYBERCOM)
- Mr. James Krakar (USEUCOM)

This panel—which included input from the global Combatant Commands, functional Combatant Commands, and the services—explored the challenges of conducting integrated operations in a globally connected and dynamic environment. In the current operational environment, it is no longer enough to orient on a geographic area of operations; adversaries are globally connected and conducting operations to compete with the US across multiple Combatant Commanders' geographic areas of responsibility. To effectively meet this challenge, the Joint Force must think, organize, and operate in an integrated and reinforcing manner that makes use of all the tools available to the DOD.

Colonel Brooks opened the panel by providing an overview of the panel topic, noting that there has been a significant evolution in how the US conducts global operations. He followed panelists' initial comments by asking them to discuss how focusing on great power competition while simultaneously conducting combat operations in some AORs has changed the way that Combatant Commands plan and execute operations. COL Brooks also queried the panel about dynamic force employment and how the joint force is evolving integrated operations planning.

Mr. Jones began by discussing how, in this era of unprecedented shifting power (between parties, between states, and from governments to populations), the United States, as the preeminent status quo power, views revisionists as threats. Moreover, these threats are viewed in the context of war and war plans, and as such, peace has come to be viewed as a prelude to war. Taking this view affects, and even corrupts, our thinking. He also argued that the US is still thinking about great power in terms of control and assumes that its adversaries are as well; making the transition to instead conceptualize in terms of influence will be important to ensure continued success. Mr. Jones also recommended that war should be defined as narrowly as possible and peace should be defined as broadly as possible—and that both ideally should be defined by civilian authorities. He further argued that it is important to recognize that competition is peace. However, unwanted or problematic competition below the threshold of traditional deterrence may prompt us to consider what type of traditional deterrence does not actually deter, and how the US might compensate for that gap. In competition, things like cyberspace or Special Operation Forces (SOF) may be the tools required to put pressure on state actors in ways that necessitate a geographic Combatant Commander to escalate to Phase 3 against a Phase 0 activity. Mr. Jones went on to emphasize that actors who can best influence populations by leveraging or mitigating existing grievances (versus suppressing or defeating such grievances) will have the advantage moving forward. He noted that the US competes not only with known nation-state and violent extremist organization (VEO) adversaries, but also with friendly actors or entities such as Canada, the EU, or India. In his response to the moderator’s query about dynamic force employment, Mr. Jones indicated that the US historically has issued forces by region, but may be more effective if forces instead are allocated by problem set.

Colonel Beaudoin continued the discussion by noting first that the US consider the risk to a given strategy in competition below the threshold of conflict; a decision to employ forces at a given location affects the level of risk the US is accepting, not only to the mission but also to its force globally. Further, COL Beaudoin discussed how the campaign plans that are the basis for executing US intermediate military objectives should be supported by some US (or with allies and partners) operation, investment, or activity globally. The ability to execute requires resources that, once moved, increase risk elsewhere. He argued that the US needs to be proactive in shaping its environment in order to reduce that risk. He also emphasized the need to consider the strategic gain from employing forces or moving forces from one area of the globe to another. Finally, COL Beaudoin noted the significant challenge to the Joint Staff posed by determining how the US can assess its decisions and especially their impact to the adversary decision calculus.

Mr. Curry from USAFRICOM highlighted the challenges of translating strategy as it is represented in documents, into operations, activities, and investments (i.e., “stuff to do” or execution). The US has an opportunity in this AOR where US competitors are increasing their influence as part of a deliberate long-term strategy. However, the US must decide how much influence it wants to have there, along with which effects and objectives it wants to achieve, and which operations and activities will enable their achievement. Building partnerships is USAFRICOM’s priority line of effort and Mr. Curry discussed the importance of the US being the partner of choice. This involves transparency, providing secure information, and the ability to be a reliable partner in order to overcome skepticism. There are also opportunities to compete effectively in the USAFRICOM AOR through the provision of technology.

Captain Stone of NORAD and USNORTHCOM discussed how, as nation state threats have reached across AOR boundaries, homeland defense has become a global problem. Circa 2010, planning across the joint force was regionally focused, never looking outside the AOR boundary on a map. In the 2016 timeframe and beyond, NORAD/NORTHCOM began looking at developing operation plans and the conventional map evolved into a globe. This has been an important development as, over the years, nation state actors have studied US ways of war, observed US capabilities, and developed their own capabilities that enable them to reach the homeland and prevent, delay, and degrade power projection to a forward fight. As such, the US requires the ability to detect attacks before they reach the homeland and preserve the decision-making space both for senior leaders within the DOD, as well as at the POTUS and tier zero level.

Captain Gage noted that great power competition is something that the Navy has embraced and is well positioned to do so, further emphasizing the urgency of accelerating learning to better understand the problem. The Navy is aligned with the National Defense Strategy and the National Security Strategy, and has followed these with its own classified strategy. He went on to note that, while the Navy can derive lessons from its successes during the Cold War, this 21st century era of great power competition is not the Cold War—the nature of the competition has changed and become multipolar.

Lieutenant Colonel Forrest from Air Force CHECKMATE indicated that the need for global integration is entirely clear from a service perspective, as opponents are global actors. However, while the need is clear, how this will be effectively achieved is still being formulated and established. There remain varying perspectives on priorities, requirements, and how to manage or balance the force. The services’ role as a force provider is still in a closed system in which risk can only be transferred. Similar to COL Beaudoin, Lt Col Forrest noted that moving forces from one AOR to another creates risk, and management of that risk must be considered in the global context as well as in the context of US strategy.

Colonel Brewster noted that Americans associate the USCENTCOM AOR with war, unrest, and totalitarian regimes; there is also increasing trouble along the seams. However, the DOD has been clear in its National Defense Strategy that USCENTCOM can no longer be the main effort, and USCENTCOM is subsequently working to reduce its footprint despite the challenges it faces. As such, USCENTCOM has significantly shifted its thinking over the last 18 months or so, as part of the discussion of great power competition. He went on to note that competition with China and Russia is predominantly for influence in the regions across diplomatic, economic, and military domains. Finally, he observed that US partners are maintaining their relations with the US while hedging their bets and pursuing stronger relations with Russia and China—a development that has become an area of concern and emphasis for the US.

Lieutenant Colonel (Promotable) Corbari from USCYBERCOM noted how the US has observed over the past ten years a significant increase in the frequency and intensity of malign behaviors in cyberspace, including the theft of personally identifiable information, exfiltration of trillions of dollars-worth of intellectual property, destruction of physical infrastructure. Moreover, there is the use of disinformation, mal-information, and hyper-information in deliberate maligning influence campaigns, designed to interfere with the democratic process and sow discord across the US population. As such, we are observing a change in the strategic environment, with the balance of power shifting from traditional patterns of international antagonism (i.e., armed conflict) to a more dynamic and potentially dangerous paradigm of great power competition. LTC(P) Corbari further noted that the emergence of powerful technologies distinguishes the era of great power competition from what was observed decades ago, with US adversaries now seeking to gain strategic advantage across every instrument of national power through the use of cyberspace. As emerging technologies permit malign actors to expand leverage over states economically, politically, militarily, and culturally, it is imperative that the US fully understands the risks and potential consequences, while still remaining mindful of the potential opportunities. LTC(P) Corbari noted that cyberspace has its greatest value and capability in influence, which should be emphasized to enable the avoidance of conflict. Further, he emphasized that our standard approach to deterrence does not fit in this space, and as such, the US needs to fundamentally rethink the role of the DOD amid great power competition. Finally, he highlighted that integration can be difficult to work out at the staff level, particularly with USCYBERCOM's battlespace being global and interconnected across domains.

Mr. Krakar emphasized that countering and deterring US adversaries should begin in Phase 0—shape. Should countering and deterrence fail, USEUCOM is prepared to execute the fight and win as necessary. He further noted that integration should be with the entire US government and intergovernmental alliances, such as NATO. Mr. Krakar went on to indicate that USEUCOM also deals with the Joint Staff, with which USEUCOM should work in Phase 0, thereby shaping operations in terms of dynamic force employment. Mr. Krakar finally remarked that USEUCOM has seen a tremendous change overall as a result of great power competition over the past five years, and a flexible nature is necessary in the conflicts to come.

Day 2, Panel 2: The UK Assessment of Future Competition

Moderator: Mr. Fergus Anderson (DSTL)

- Mr. James Maltby (DSTL)
- Ms. Malin Severin (DCDC)
- Dr. Nick Wright (Intelligent Biology)
- Mr. Richard Leigh (DSTL)

This panel offered UK perspectives on the overlap and divergence between the UK and the US concerning global competition environment and force levels. The discussion centered specifically on alliance complementarity—i.e., the defense bandwidth generated across alliance partners that is greater than any one nation could generate on its own.

Mr. James Maltby argued that the UK possessed limited forecasting bandwidth. Forecasting in the UK, he argued, was too deterministic and linear, based on mastering methods of assessment, rather than focused on improving efficacy of assessment. Mr. Maltby indicated that gathering feedback about forecasts was an excellent place for the UK to begin adding to alliance complementarity. Lastly, Mr. Maltby argued that forecasting could be improved with soliciting a wider array of inputs; too much emphasis on kinetic solutions from a transatlantic defense establishment that is too white and too male has created groupthink.

Ms. Malin Severin offered insights into the updated foresight philosophy of the UK's publication, Global Strategic Trends, emphasizing that good strategic foresight is about 'disturbing the present,' not about coming up with the most accurate description of what the world might look like in 30 years' time. Ms. Severin argued that the increasingly ambiguous operating environment has highlighted the need for the UK to reassess its approach to long-term strategic planning, noting that the core challenge in strategic planning is uncertainty management.

Dr. Nick Wright posed that whilst the UK has considerable strength in AI that bring benefits to the UK-US alliance, it is smaller than the US and so must carefully also maintain its own independent capabilities. Cutting edge AI research (much of it being pioneered in the UK) reveals that AI is really good at pattern recognition in images and speech, and choosing actions in tasks that are unconstrained enough to have vast amounts of data. Unfortunately, the current limitations of AI also limit its efficacy: not only does AI need huge amounts of data (often labelled), it exhibits extreme difficult in understanding context. Further AI developments, Dr. Wright maintained, will increase the UK's alliance complementarity by maintaining independent capabilities and increasing tech investments in perception, constrained choices, datasets, and human-machine interactions.

Mr. Richard Leigh discussed the implications of the panel for defense doctrine. Mr. Leigh observed that UK doctrine emphasizes the centrality of influence. Traditionally, most of the military training has been focused on war-fighting and maneuvers, but now the UK has introduced a new concept note called "Information Advantage," which is focused on information denial and information effectors. This concept note tries to combine intelligence/information activities to deliver a unity of purpose to create behavioral outcomes.

Day 2, Panel 3: Future Global Competition between AI-Shaped Political Systems

Moderator: Dr. Nick Wright (Intelligent Biology)

- Ms. Elsa Kania (CNAS)
- Dr. James Lewis (CSIS)
- Dr. Tom Wright (Brookings)

Dr. Nick Wright contextualized the panel discussion by questioning how the AI constellation of technologies affect Russia, China, and the global order. Emphasizing the impacts AI has on global order, he listed commonly discussed topics such as the 4th Industrial Revolution, but clarified that the focus of the panel is what AI means for the various types of political regimes, how they compete for global influence, and how it applies the societies that they govern.

Ms. Kania focused her portion of the panel on China and started with the notion that in many ways, the ground zero for the effects of AI on governance is in China. Under Xi Jingping, innovation, theory, and practice have been important in revealing Chinese ideology, particularly that of national rejuvenation. Pursuing technological advancement is critical to China's worldview and more importantly, for regime security. China's political campaigns to mobilize the public have historically been centered around technology and are central to the regime's influence; correspondingly, the Chinese Communist Party's (CPP) ability to control the population is technologically driven as well. AI is an ideal social instrument for social management in China; however, it is also a vital component to increasing China's global influence, and Chinese internet infrastructure can threaten US internet security. Ms. Kania concluded by remarking that Beijing desires to shape the future development, norms, and laws that will govern the implementation of AI globally.

Dr. Lewis began by noting that better technology doesn't necessarily bring victory—strategy, leadership and doctrine does—and the current global order, where the US was the dominant power, can entail significant disadvantages in multi-domain competition. He went on to posit that opponent governments are increasingly competitive where the US is not. Furthermore, the myth that US private sector is the saving grace is simply an excuse for not adequately funding necessary research programs. With respect to China, Dr. Lewis stated that China is likely on the path to becoming a true peer competitor to the US, but also emphasized that China, Russia, Iran, and the DPRK are brittle states that fear their own populations more than they do the US. The US is not ready and able to exploit this weakness, and is instead waiting for a "Sputnik" moment to mobilize the US into action with respect to the AI race. In the meantime, the US should be focusing perfecting doctrine, practice, and tactics to apply new technology. Dr. Lewis finally cautioned that AI is just another tool in statecraft, and great power competition is not centered around which nation has more AI technology, but which nation is better at utilizing this tech.

Dr. Lewis began by noting that better technology doesn't necessarily bring victory—strategy, leadership and doctrine does—and the current global order where the US is a hegemonic power entails significant disadvantages in multi-domain competition. He went on to posit that other governments are competitive where the US is not, and only by their inefficiency and corruption does the US remain on top; furthermore, the myth that US private sector is the saving grace is simply an excuse for not better funding necessary programs. With respect to China, Dr. Lewis stated that China is likely on the path to becoming a true peer competitor to the US, but also emphasized that China, Russia, Iran, and the DPRK are brittle states that fear their own populations more than they do the US. The US is not ready and able to exploit this weakness, and is instead waiting for a "Sputnik" moment to mobilize the US into action with respect to the AI race. In the meantime, the US should be focusing on innovation and perfecting doctrine and tactics to apply new technology. Dr. Lewis finally cautioned that AI is just another tool in statecraft, and great power competition is not centered around which nation has more AI technology, but which nation is better at utilizing this tech.

Dr. Wright directed the focus of his panel contribution to China as well, first by positing that the US is in competition with China because of a clash of systems and worldview. The success of the US modeled-liberal international order is an existential threat to the Chinese regime and conversely, the spread of authoritarianism threatens the US system. The points of conflict between both sides are numerous, dense, and complex, and both sides can pull levers to aggravate the other. With respect to AI, the Chinese believe that they can forge their own path to modernity by embarking on the AI journey that seeks to consolidate

Chinese Communist Party control over their society. Historically, nascent periods of competition are the least stable, and Dr. Wright argued that the current era is full of uncertainty that lack redlines and rules that can only manifest through complex interaction. He concluded with the notion that technology will be the defining force of this period of history, and that competition in peacetime is the environment where this technology will operate.

Day 2, Panel 4: Strategic AI: Predictive Analytics, I&W, Counter AI/ML Alternatives

Moderator: Dr. Kathleen M. Carley (Carnegie Mellon University)

- LTC David M. Beskow (West Point)
- Dr. Rebecca Goolsby (Office of Naval Research)

Dr. Carley introduced the panel by explaining that it was inspired by discussions on the limitations of AI. LTC Beskow then opened the floor by discussing some of the "lessons learned" regarding the application of data science more broadly. In particular, he emphasized the need to get the initial question right before moving to any data analysis. He noted that this problem was exacerbated by the current lack of understanding between operational personnel and data scientists. "Operational guys" need better training on what data and AI can and can't do, while "Trumans" need a better understanding of the needs of operators so they aren't just designing algorithms to answer the questions they can with the data they have. He pointed out that this disconnect led to inefficient and ineffective use of data science, and providing an example the time and resource intensive work of creating a stability model. The example being that while the model was able to accurately predict the Democratic Republic of Congo as unstable, it was ultimately telling you the same thing as a junior State Department official could do immediately and for much less money.

LTC Beskow considers the solution to this current disconnect to be more data-driven decision making, rather than less. He observed that currently, data-driven decision-making is happening only at the 3-star level, because there are not enough lower-ranked analysts. He identified two barriers to expansion: lack of human capital (too few cadets coming in with an AI background), and accessible data (i.e., data in digital format, such as tools that allow data collection by operators themselves and not vendors) that is properly managed.

LTC Beskow then focused more specifically on the issue of what we can currently do with AI. He noted that AI cannot currently provide answers to the questions we want to ask (e.g., "predict the next Russian disinformation narrative and target culture or sub-culture, and then automatically deploy culturally aware counter-narrative"), but machine learning (ML) does allow us to conduct pattern recognition to help people understand what is going on (e.g., can we characterize past disinformation campaigns and rapidly identify key factors such as, "bots and memes"). In other words, "there's not an easy button that will solve the world's problems," and we are not even close to full autonomy. He discussed several programs that have been used to identify and analyze disinformation campaigns: the use of advanced ML algorithms to detect bots in curated streams; the used of state-of-the-art, multi-model, deep learning to extract memes from curated event streams; and Sketch IO, which begins to sketch out major components of disinformation campaigns. All of these, he notes, are focused at the campaign level, and are still descriptive, i.e., not autonomous. Using the analogy of a bomb dog, he explained that all ML algorithms are the same; what you train them on matters, and they can only detect what they were trained to detect.

Dr. Goolsby, like LTC Beskow, focused her discussion on perception; however, her focus was strategic and not operational, arguing that perception is "the heart of warfare," and in the last five years, misperception elevated to an art form for shaping population perceptions on social media. Dr. Goolsby views actors that purview illegitimate information on social media as a constant and pervasive threat to the credibility and authority of military and government spokespersons. One that affects our ability to promote our own narratives about who we are, what we are doing, and what we intend to do.

Understanding how illegitimate information actors may influence audience perceptions is a very different application of AI than what is needed for autonomy and robotic applications. Although early work in the field (such as that done by Dr. Claudio Cioffi-Revilla) aimed at prediction, has demonstrated that human behavior is very difficult to predict, as adversaries are constantly changing in response to what we do. More recent work, therefore, looks to do more general forecasting—similar to weather reports—although this is still challenging.

In the context of disinformation and population perceptions on social media, Dr. Goolsby proposed that the question we really want to be able to answer is: "Am I losing the social trust of my target audience?" She sees this as a complex problem and one that cannot be answered by typical social media metrics (e.g., how big is my audience? How many people liked by tweet or story?). Rather, it requires relative metrics of competition (Is my audience larger than my competitor's? Is my audience share growing relative to my competitor's?) and conflict (Are my adversaries successful in destroying my authority? Is this disinformation about me, are my activities and intentions outpacing my ability to counter it?). It is to answer these types of questions, and to help IOs understand the information environment better, that ONR researchers developed BEND. BEND provides strategic guidance for how to operate effectively and insights into adversaries' information operations, and helps people understand how influence happens in social media.

Dr. Goolsby explained that social media stories are told in pieces that circulate through many different communities online. People consume these stories and use them to construct a narrative that, once established, can be difficult to change. Furthermore, because individuals put pieces together in different ways, even when they accept the same pieces, they can end up with different stories, or perspectives. It is this ambiguity that adversaries rely upon to confuse and manipulate populations using three "levers": community, content, and the underlying platform algorithms. Information maneuvers involve manipulation of community and content levers to compete for audiences on a social media platform. Algorithmic maneuvers are designed to "game" the social media platform's algorithms for distribution and recommendation to achieve a competitive advantage on that platform. Dr. Goolsby noted that while some algorithmic maneuvers are simply competitive (e.g., liking tweets of an embassy to improve the distribution of those tweets), others, (e.g., adding large numbers of fake followers), are deceptive, fraudulent or malign; designed to fool the algorithm into distributing more of an individual's tweets.

To spread a story on social media you need other storytellers to pick up your story and spread it. Within any cyber-social community (people who communicate regularly about a topic on an online social media platform), there are some members—Super-Spreaders—who have an exceptional ability to spread information (they communicate frequently, are frequently followed and mentioned, often across platforms), and others—Super Friends—who create a dialogue that makes them arbiters of opinion and gatekeepers in conversations, generating loyalty and social trust that enables them to shape the conversation, and alter perspectives and beliefs. Bad actors, understanding the way these communities work, aim to cheat the system by placing bots and cyborgs in these roles (super spreader and super friend) so they can then use the community, content, and algorithmic levers to shape the information environment. Positioning bots within a community can determine how these communities link or do not link. They can also inflame communities with targeted disinformation with emotional content; leaving them much more susceptible to disinformation and propaganda.

Dr. Goolsby went on to emphasize that it is on the community side (i.e., the social rather than knowledge network) where we need help. She noted that there are no obstacles to public affairs, strategic communications, and IOs operating when using positive community building information maneuvers (build, back, boost, bridge). She highlighted how states and civil society organizations have built communities such as Kremlin Watch, EUVsDis and YATAINT to support NATO's narrative of peace and security, and fight against disinformation and propaganda.

Dr. Goolsby, like LTC Beskow, concluded with a reminder of the limitations of AI to identify and counter disinformation influence campaigns. While AI can be used in positive ways, she argued that human behavior is constantly changing and is deceptive, and bots are not good at identifying networks. However, we need more tools to help human operators visualize and understand what is going.

Question & Answer Session

(*Italics indicates questions from the audience.*)

How universally applicable is the BEND system across social networks?

Dr. Carley answered that BEND is agnostic to platform, but added that she didn't know how it would be affected by censorship. Dr. Goolsby stated that it is a combination of social cognition and psychology and thus observable and inescapable. She noted that you don't need to be able to reach everyone on a community, just enough to plant a seed. Dr. Goolsby concluded by noting that different social media platforms allow for different capabilities (e.g., WhatsApp just limited the number forwards you can do) that change all the time, which may have some implications for how BEND is applied.

Regarding Chinese social media usage. Given that the Chinese population are "short on emails," they had considerable presence on dating platforms; is this a possible avenue for deploying BEND?

Dr. Goolsby replied that that is such a sensitive area and one which would involve collecting personal information, would need further guidance from the intelligence community.

How do we make our own citizens competitive in these [AI-relevant] fields?

LTC Beskow replied that STEM is starting to do this, but reiterated that AI "is not a magic button for" disinformation and influence operations. He questioned why there is no ROTC programs for data science and stated that we need to make sure that money is not an issue for cadets seeking AI education. He pointed out that big data and tech companies are buying startups just for their human capital, and that we need to become more competitive in attracting people. Dr. Goolsby suggested that we need to start funding strategic people in graduate schools to go into the defense industry.

How do we help senior leaders understand data science and AI?

LTC Beskow indicated that using online courses to learn is better in many cases than official training.

A lot of questions the defense community has don't need AI, and lots of new data scientists have tools, but can't tell you what the data mean, or don't know how to answer questions—how do you overcome this?

LTC Beskow reiterated the need for domain expertise, and stated that creating teams helps. Dr. Goolsby also stated that we need to have teams (like Google), and that cross training is also important.

Day 2, Panel 5: Human Threats versus Machine Threats in Cyber Security

Moderator: Dr. Gina Ligon (University of Nebraska Omaha)

- Dr. Kathleen M. Carley (Carnegie Mellon University)
- Dr. Douglas C. Derrick (University of Nebraska Omaha, The Center for Collaboration Science)

Dr. Ligon provided the context of this panel as answering the question of how the cyber domain amplifies global competition for influence.

Dr. Carley began by distinguishing that machines and humans separately are not the preeminent threat, nor are they the most vulnerable, but rather that the nexus of both human and machines together and their capacity for influence are the subject of concern. These human/machine teams are able to exert influence through a variety of ways via the internet, and dense communities (echo chambers) have been constructed and manipulated through various methods by these teams. Humans are very adaptive and thus susceptible to influence operations; consequentially, human/machine teams are more effective. Features on social media platforms can also be taken advantage of by malign actors. Dr. Carley also highlighted the different characteristics of humans and machines, noting that humans have social cognition (the immutable perception of the world through groups), whereas machines are very adept at scaling, but lack simple intelligence.

Dr. Derrick discussed the threat of machines and AI that can perceive and impact individuals, rather than group influence mechanisms such as trolls or bots. He then explained the importance of communication theory where encoding, interpretation, and response are the mechanisms of influence and how machines can automate this process. He then explained several experiments that tested the feasibility of influence mechanisms and leadership that can be executed by machines and AI. These experiments revealed that machines and artificial "leaders" could accomplish simple acts of influence in statistically significant ways. The major finding of these experiments being that study subjects readily accepted the role and influence of artificial agents, and that technology, when individualized, maximizes its ability to influence human behavior. Dr. Derrick concluded that by understanding the personality of the subject that you are trying to influence, along with the premise that leadership or influence is a set of strategically applied set of messages and skills; tailored, adaptable and persistent influence automation is possible and is occurring right now.

Invited Speaker

Mr. Brian Murphy (Department of Homeland Security)

Thank you for having me and I appreciate the opportunity to be here. I am the Principal Deputy and Deputy Chief Intelligence Officer for the Department of Homeland Security (DHS). The core of DHS is the 240,000-plus people that work within the Department. DHS is the second largest federal agency in terms of people, behind only the Veterans Affairs Administration. The core elements of DHS consist of US Customs, Border Patrol, ICE, FEMA, the Coast Guard, CISA, TSA, and the Secret Service. DHS also has numerous supporting efforts at its Headquarters Agency, including the Intelligence Analysis and Science and Technology initiatives.

One of the things that surprised me when I joined the Department a year and a half ago is that DHS is responsible for 16 of the United States' 18 critical infrastructure elements. DHS is in charge of protecting numerous critical dependencies. For example, DHS both manages Continuity of Operations (COOP) and Continuity of Government (COG) sites on behalf of the federal government and protects key officials within the federal government. DHS also has the ability to surge people back and forth pretty easily to meet mission requirements in ways that many other organizations are simply unable to match. FEMA, for example, is the mission manager for both natural and manmade disasters in the US.

DHS strives to provide information back to both its workforce and leadership. My office within DHS is the only element of DHS that is a member of the intelligence community. My office translates information between the intelligence community and DHS. To help this translation process, we have recently divided into several mission centers: counterterrorism, transnational organized crime, economic, cyber, exploitation, and counterintelligence. We have reorganized this in an effort to evolve from the way in which the intelligence community typically operates, which is within a Cold War paradigm. This Cold War paradigm can be seen very clearly at our overseas embassies, where there are three basic players—the CIA, State Department, and Department of Defense—and everyone else plays a much smaller role. This Cold War paradigm still exists, though it is changing slowly. A lot of the methodology that our government has incorporated comes from that history that was endured. But, today, we are in the middle of a major turning point, and we do not always recognize it.

We are in the middle of a very rapidly changing environment and more importantly, the adversary is in our backyard. They are in the seams between our agencies that are allowed to operate freely in domestic spaces and those that operate freely in spaces outside of the continental US. They live and enjoy that seam and are doing a great job of exploiting it. One element of this is non-traditional collectors, where there are large numbers of foreign students coming to the US and stealing information to bring back to their home countries. We in the US look at the free flow of ideas as a good thing but our adversaries, particularly China, do not. Another element of this paradigm is our adversaries' abilities to be involved in our political system. This is happening today in ways that we have never seen before, and there is also the cyber component to consider. The way our adversaries have internalized themselves in our critical infrastructures is something that we have never seen before. Quantum computing is another piece of this. Our adversaries' ability to gather data is close to or even exceeds our ability in some areas. Our adversaries understand the way that we are structured through our state and local governments and are outpacing us in the ability to influence both.

Our recent elections present a clear example of this rapidly changing environment. We are all aware of what happened in 2016, but many people are probably not aware of what happened in 2018 and where we are going for 2020. In 2018, DHS worked aggressively with all of the interagency partners, as well as with state and local colleagues where such collaboration is new. Most of the intelligence community is not interested in doing anything involving local, domestic US elements. But DHS introduced this new element of collaboration because state and local leaders are the ones that have bearing on how the electorate responds to things. From a basic civics lesson, state and local leaders are the ones talking to the American public on a day-to-day basis. These state and local leaders include chiefs of police, mayors, city managers, etc. We as a federal government communicate information and work to defend networks, but we will never be able to know everything that the adversary is doing. Therefore, it is important to inoculate the American public about these things in two areas: the critical infrastructure and the countering of foreign influence.

DHS had around 5,000 engagements with its state and local officials during the elections. DHS wrote more intelligence products for these state and local officials than any other organization within the government. DHS shared and continues to share unclassified products showing, for example, how Russia today is influencing the American public. DHS is often asked why it is taking the chance of risking sources and methods to explain these things to state and local officials. It is because the intelligence exists to do something with. We have to accept some level of risk and find a proper balance. As we look at the adversary and how they are able to be inside of our defenses in ways that we have never seen before. We have to know how they are penetrating those seams and they take advantage of our well-founded civil liberties and privacy rules, knowing that all our actions are bound to the respect of the laws of our land.

What is our biggest challenge? It is understanding how we can navigate the very complicated system that we have, from people at the state and local levels (i.e., our electorate and lawmakers) on one end to people at the federal and interagency level at the other end. If we do not get buy-in from both ends today, then the adversary will continue to cut across the way that we are organized and continue to make inroads into our systems and infrastructures (e.g., worming their way into our infrastructure through cyber means, stealing our advancements through non-traditional collectors, and influencing our leaders and public with disinformation). We cannot afford not to take some risks to explain things and move our information to the lowest common denominator as quickly as we can. In this shifting landscape from a Cold War paradigm to an enemy is within our gates paradigm, we need our key leaders to be a fourth element in this battlespace—they need to be at the table. And that is a hard thing to do because there are a lot of people involved when you get down into the state and local levels. For example, there are around 15,000 police departments and around 850,000 police officers in the US; there is about an equal number of elected politicians. There are a lot of voices at the state and local levels, but we have to navigate this issue, and our state and local collogues are more important than ever for such navigation. Ultimately, we must find a way to share with the American public, through our key leaders, as much as we can to inform them about what China, Russia, and other adversaries are doing.

Finally, in terms of solutions, one thing I would offer is that we have to move away from collaboration and toward the joint operational environment. We largely do not see this between civilian and military agencies. There is some overlap, but we have to get a whole lot more collaborative. Part of this is data; we need to share and manage data appropriately so that those working and operating across all levels can absorb and utilize it. We have to move from collaboration to joint operations in a mutually supportive environment. And at my office in DHS, we are working towards doing so.

Question & Answer Session

(*Italics indicates questions from the audience.*)

What do you see as a roadmap to creating an effective and enduring process for developing a joint model?

The more we educate our state and local authorities about the merits of the threat and the more we are willing to take some risks with the information needed to do so, the better off we will be with respect to inoculating and informing the American public about the details of the threat.

It is very hard to build a culture of trust at the state and local levels, but it is imperative now more than ever that we build that trust. Is DHS putting in place a sustained protocol for building this trust at the state and local levels?

DHS is investing in and continues to increase its investment in touchpoints at the state and local levels, including state and local government-owned fusion centers, to help build this trust.

Given that we have reliance on foreign imports, is there discussion about having strategic reserves for things that we are importing in order to reduce our reliance on foreign imports?

From a strategic level, there is an increasing awareness that we cannot continue to do business as we have done in the past.

Day 2, Panel 6: Dealing with Surprise in Complex Systems

Moderator: Ms. Gia Harrigan (Department of Homeland Security)

- Dr. Laura Steckman (MITRE)
- Dr. Molly Jahn (University of Wisconsin)
- Dr. Kay Mereish (DHS Office of Intelligence and Analysis)
- Dr. Robert McCreight (George Mason University)

Ms. Harrigan opened the panel by posing several questions. First, how can the US maintain global awareness and understanding of events in dealing with surprise in complex systems? The goal being to understand the impact on senior decision-making. Second, how are good decision define? Is it accomplishing the mission quickly? Minimizing collateral damage? Ms. Harrigan then clarified that this panel will consider high impact/medium-high consequence events

Dr. Steckman suggested that a good area to consider for emerging threats that carry the risk of surprise is in the new space race. With Russia and China already heavily invested in the space domain, a minor actor like the UAE is also pursuing efforts to colonize Mars. While there is no immediate threat, Dr. Steckman encouraged to have keen eyes potential elements of surprise that can cause "nth order" effects that may emerge from such innovations in technology. Many African countries (e.g., Nigeria, South Africa, and Kenya) also have AI strategies that are looking to integrate new technologies such as crypto currency into their statecraft. The era of great power competition entails an interconnected system where lesser actors can impact larger dynamics and relationships; surprise and complex systems further complicate this. It is the job of the analyst to forge a strategic plan to navigate these muddled waters; however, combining physical data with social data is very challenging.

Dr. Jahn started her contribution by noting that there is nothing inherently "surprising" about surprises, but rather that there is a tremendous amount of variation in existence, and the classification of that variation determines the nature and degree of that surprise. She then described several pitfalls in searching for surprises, such as "classic blind spots." There are several simple, powerful techniques to improve analysis drawn from the practice of "systems thinking" based on the precept that any issue of concern to the DOD can be understood as highly complex and complicated, non-linear dynamical systems. In this frame, plausibility space is charted and then explored by systematic queries. Systems thinking focuses on articulating the full spectrum of salient questions related to major threats or concerns, "seeing" what is there very carefully *and* seeing what isn't there; noting what is changing, and what isn't, asking what holds the present in place and what are large scale, imminent threats or opportunities that may be "emergent." She also noted the potential hazards of secret, expert culture in a century where major attack vectors both abroad and in the homeland are emergent and potentially wildly unconventional. This view requires fundamentally different ways of perceiving and interpreting concerns as dynamic systems properties. Well-intentioned efforts to harden defenses against emergent threats, as we did in the 20th century, may have aspects that are more detrimental to national security than doing nothing at all. Dr. Jahn noted that she is frequently called to evaluate or develop stress test scenarios used by governments and financial institutions and finds that they are often very narrow and falsely constrained by disciplinary expert culture. This is a general observation that the DOD should take seriously. There are networks of seniors, analysts, strategists, planners, experts, and operators across the DOD who recognize and work to implement these insights in their day to day decision-making.

Dr. Mereish noted the dichotomy of two main issues, "surprise" and the 'the complex system," both of which are an increasingly important issue in all aspects for politicians, economists, and even in healthcare systems. Surprise is undesirable because it is "a condition in which perceived reality departs qualitatively from expectations[4]." Many surprises the DOD faces are a consequence of living in an increasingly complex and connected world. However, some surprises are due to lack of sufficient data an analyst can use to predict what is next. Dr. Mereish continued by stating that within a receiver operating characteristic curve (ROC), the more available data points, the better curve is (i.e., sensitivity vs specificity), which leads to higher sensitivity that results in lower specificity as it is applied in many medical diagnostics tests. Intelligence analysts faces much more complexity than healthcare professional or economists, as they try to combined physical data (information about sites, material, equipment etc.) with social data (leadership characteristics, intentions, motives etc.). This complexity must be resolved in order to predict an outcome in specific region or topic where unpredictability and surprise are fundamental aspects of the world around us. Dr. Mereish concluded with several examples of how big data can help these analysts: the partial prediction of analysts of H1N1 pandemic, seismic detectors to predict tsunamis and earthquakes, and hurricane relief efforts.

Dr. McCreight began by suggesting that strategic surprise needs to be viewed along a threat spectrum: i.e., unexpected, unplanned, and unanticipated. Unexpected events involve new foes, alliances and technologies. Unplanned for scenarios include future battlefields, future conflict scenarios and covert attack situations. The unanticipated includes specific avenues of attack, mixed threats involving conventional and unconventional weapons, and dimensions of combat involving future convergent weaponry. He also noted that we lack sufficient levels of detection, deterrence, and defense against emerging and novel future weapons technologies because we risk strategic surprise which confronts US interests in unplanned, unexpected, and unanticipated ways. He also asserted that future strategic warning must be modified to account for DUST (Dual Use Science and Technology) and widened to contemplate the true breadth of tomorrow's threat spectrum. We must consider the next war will not resemble the last war and will likely feature a mix of traditional and novel future weapons. The nature of future conflicts after 2020 must be grasped, dissected and rigorously examined.

Further, adjustments to strategic warning must account for determining if the US is under attack especially by covert and non-kinetic means. If the US risks strategic surprise from failing to appreciate future convergent DUST threat, where cyber, nano, neuro, hyper, genomic, and outer space arenas can be blended, a dismal result is possible. Overlooking these issues represents and avoidable fatal mistake. Threats from emergent future battlefields (both kinetic and non-kinetic) need to be a part of evolving doctrine and strategic warning systems where multiple spaces and domains will redefine the battlefield. Accordingly, strategic simulations and wargames are the appropriate space to accommodate these concerns, and they must evolve with as new threats and surprises emerge. It may also be helpful to conceive of adding an extra "D" to our description of WMD where the notion of disruption, [meaning technological disruption to our systems, infrastructure and neural domains involving cognition,

[4] Per the "Holling" definition

perception and thought processes] are truly at risk. Dr. McCreight concluded by stating that the current mindset of viewing these threats as “20 years away,” is mistaken and dangerously detrimental to US safety and security. As the nature of warfare and the battlefield changes after 2020 we must be vigilant about the authentic spectrum of threats and challenges we will face.

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

We tend to be reactive. How do you move to be more proactive to predispose and outcome and objective you want?

Panelists responded that Counter measures and counter offenses are key, as well as defining objectives and coordinating with other interested parties/COCOMS/etc. The US can’t accomplish this until it has definitive goal and strategy.

What about team performance?

In team performance, there is need to set example skill sets, look at people outside an organization, and cultivate positive characteristics of a team within.

Day 2, Panel 7: Risks and Opportunities associated with Human Biotech Engagement

Moderator: Dr. James Giordano (Georgetown University Medical Center)

- Invited Speaker: Mr. Rick Bremseth, CAPT USN SEAL (Ret.): *Emerging Threats and Technologies as Non-Kinetic Hostile Engagements*
- Dr. Vincent Clark (Mind Research Network, University of New Mexico)
- Dr. Richard McKinley (United States Air Force)
- Dr. Rachel Wurzman (Johns Hopkins University Applied Physics Laboratory)

This panel examined developments in the field of human biotechnology, and specifically scientific advancements and their applicability to the national security problem set.

Captain (Ret.) Bremseth began the panel by speaking broadly on non-kinetic hostile engagements. He stressed the continued importance of Sun Tzu’s *The Art of War* on his intellectual development, and highlighted the applicability of some of those lessons to the current environment. These included maxims on the necessity and criticality of actions and decisions taken before the commencement of warfare, as well as the importance of deception in conflict. He continued, using those lessons as a framework for understanding the United States’ current threat environment. For example, the proliferation of large amounts of fentanyl originating from China into the United States represents one of several threat vectors that China has been executing in non-kinetic engagements. This flooding of the opioid market of Chinese-origin fentanyl represents an escalation of an already dire crisis that claims the lives of 50,000 Americans annually. In response, he indicated that the Department of Homeland Security has considered designating fentanyl as a weapon of mass destruction. He also suggested that policymakers update their threat perception to reflect a priority on disrupting opponents, and encouraged an adaptation of a C-WMD² (counter-weapons of mass destruction and disruption) policy. His comments also touched on psychological operations, media warfare, and legal warfare, all of which represent “war by other means.” The United States has not yet met these challenges because of a failure to recognize the threat environment; this lack of recognition is advantageous to its adversaries, because it allows for continued ambiguity in competition. He concluded his comments with an indictment of what he referred to as a lack of imagination in recognizing the changing character of warfare.

Dr. Giordano then outlined the rapidly changing environment within the field of science and technology, and highlighted advancements made by US strategic competitors in this field. Current estimates based on trend analyses project that China will be the world's leader in many subfields within science and technology by 2030. Part of that, Dr. Giordano suggested, is due to the deductive nature by which China (and other adversaries) prepare for challenges, where, they begin with a final objective in mind, and then plot a path towards achieving that goal. This represents a departure from the traditional method of identifying what is probable, to what might be possible, to imagining potentiality. In order to best assess emerging threats and technologies, Dr. Giordano suggested a four-thrust approach: stakeholders must (1) examine threats that are present, (2) evaluate those threats, (3) find solutions to eliminate them, and then (4) develop capabilities to exploit opportunities in the global arena. He also suggested two broad organizing principles to consider if the US is going to engage in kinetic and non-kinetic spaces, namely to fortify one's own forces, and understand how best to compete with hostile forces. Dr. Giordano closed with an emphasis on increasing the health of operators, improving operational protection, and enhancing their neuro-cognitive and neuro-behavioral capabilities.

Presenting his team's findings on neurostimulation, Dr. Clark first defined the goal of neurostimulation as the ability to modify human brain functions through the use of energy. Dr. Clark then detailed a study in which researchers identified the parts of the brain associated with learning to detect threats. The team then hypothesized that the stimulation of those parts of the brain would result in a greater ability to detect those identified threats, which ended up being borne out in the experiment, where a doubling of performance was found. A parallel team at another research institution was able to replicate the study with similar results, where a doubling of performance was again found. Relatedly, Dr. Clark and his team conducted a study wherein subjects were asked to identify in what countries, certain images were taken; using a similar pattern of stimuli yielded increased performance and increased recognition, and a quadrupling of performance was found. Additionally, Dr. Clark also outlined research on electrical brain stimulation during sleep, and explained the results of such trials. Interestingly, whereas brain stimulation during training helps subjects internalize that which they are taught, when stimuli are applied during sleep, the brain becomes better equipped to deal with novel situations in which the user has not necessarily received training. He continued, noting the significance of ultrasound technology as a key to better comprehension of the nervous system. Despite the positive results highlighted in his talk, Dr. Clark presented some situations in which these advanced tactics could be used for malign effects, and cautioned about the many lingering questions still extant in the field.

Following Dr. Clark was Dr. McKinley, who presented findings complementary to those discussed by Dr. Clark. Specifically, Dr. McKinley addressed the ability to enhance threat detection and its applicability for the intelligence, surveillance, and reconnaissance capabilities that are particularly relevant to the Air Force. Dr. McKinley then mentioned further attention on issues of attention and fatigue, which also are central to Air Force capabilities. Whereas normal analysts begin to "miss" targets starting after twenty minutes, Dr. McKinley found that stimulation of the brain's arousal systems can result in a degree of vigilance that is sustained over six to eight hours. These tactics have also been applied in sleep deprivation studies as well. Additionally, Dr. McKinley outlined other efforts to access arousal systems, and highlighted some projects aimed at accelerating learning. He also noted that a number of these subjects who received stimuli, have also experienced increased capabilities for up to 90 days. In concluding his remarks, he noted that the scientific community is just scratching the surface of advancements in neuro-technology, and anticipates contributions to the science from several sources, including consumers can buy some of the technology on commercial markets.

Finally, Dr. Wurzman provided important context to the information presented by the preceding speakers. She noted that such experiments are highly sensitive to environmental conditions. For example, the activity that a subject was engaging in prior to brain stimulation has an impact upon experimental outcomes and results. Thus, more attention must be paid to the emotional and cognitive states of subjects. Solutions to such issues could be as simple as having operators meditate before stimulation to achieve a more controlled brain state, but this is presently untested. Furthermore, increasing threat detection capabilities also increases a hostile attribution bias. This feature, despite operating cleanly in a laboratory, presents challenges in an informational, or kinetic environment. In conclusion, she noted that policymakers should consider the complex behavioral impacts of stimulation; indeed, this vulnerability can be exploited by adversaries who seek to further complicate an environment. Dr. Wurzman reinforced Dr. Giordano's perspective that US strategic competitors may be exploiting differing cultural values, economics, and ethics to advance R&D in key arenas of potentially dual- or direct use in non-kinetic as well as kinetic domains.

Day 2, Panel 8: Human/Machine Partnership for Decision Support in the Cognitive Space

Moderator: Mr. Steve Jameson (BAE)

- Dr. Brian Kettler (DARPA)
- Dr. Nathan Schurr (Aptima Corp.)
- LTC (Ret.) Dave Johnson (C4ADS)
- Dr. Fotis Barlos (DARPA)

This panel explored how artificial intelligence and machine learning can help US strategic decision makers visualize and understand the complexities of strategic competitions and conflicts facing the United States. Mr. Jameson framed the panel's discussion in terms of two problems: (1) how to apply the potential capability of AI/ML capability at the strategic level as we move from the kinetic to the cognitive space, and (2) how to build effective human-machine interactions.

Dr. Kettler looked at the problem set proposed by Mr. Jameson from a multidomain operation perspective—at the core of which is integrated influence operations. Every word and action of the United States is a form of influence operation. To be successful in this domain, the US must develop a common operating picture of the influence space. To this end, the US need more data—and must build in human interaction to help deal with uncertainty and determine how to respond. Aside from the technological challenges, the US also needs to develop a theory of influence to help guide human-machine interaction in multidomain operations.

Dr. Schurr stated that his interest is not just in using AI/ML to support decision-making but to design a system that supports human-machine decision collaboration. Finding the right data to make decisions is half the battle, but the harder part is to develop meaningful, important insights quickly enough to provide actionable information to enable real-time decision-making. The collaborative nature of the system is essential so that workflows, insights, and secondary effects can be calculated simultaneously to allow for proactive decision-making.

Dr. Barlos highlighted the work in the DARPA COMPASS program within the Strategic Technology Office (STO). STO focuses on developing a system of systems approach to disrupt and impose lethality against adversaries. An important part of this mission is to exert influence, particularly in the gray zone. Successful influence operations rely on understanding populations and actors in complex environments. COMPASS analyzes and fuses data to allow decision makers to test hypotheses in an environment without causing instability, ultimately revealing information about an adversary's intentions and likely responses. He also highlighted some advancements being achieved under the DARPA Hallmark program for human/machine interaction with automated decision aids for space situational awareness.

LTC Johnson made four key points: (1) Humans do art (conceptual modeling and causation) and machines do science (pattern recognition and correlation); (2) only applied science counts; (3) focus on the data management layer; and (4) develop in the agile private sector and adapt rapidly. The human brain is designed to take into account context and can make decisions based on small data sets. There is no silver bullet for AI/ML-supported decision-making, but AI can enhance the ability of human analysts to understand the environment and make sound decisions. AI/ML finds patterns and develops rules to apply patterns to problems. Computers cannot determine causation—so there is danger if a human does not understand its rules. He concluded that effective use of machine learning faces important challenges in culture and in process. We will have to rapidly change our institutions. We will have to incentivize, nurture and rely on the wild, powerful private sector innovation engine. Rapidly identifying and acquiring emerging technologies, agile public-private partnering, and adapting proven use in the exponentially larger and more dynamic private sector market, will be the most effective approach to development of AI for strategic decision-making support going forward.