CYBER BEACON III

Exploring Cyberspace Through Engaging Thought

Conference Proceedings

July 13 - 14, 2016, National Defense University, Washington D.C.

About National Defense University

NDU is a strategic national resource that prepares senior leaders to think and operate effectively at the highest levels in an increasingly dynamic, complex, and unpredictable international security environment. It does this by preparing them to understand, develop, and employ strategies that incorporate all elements of national power.

This senior leader development is made possible by NDU's holistic approach and unique combination of curriculum, location, and student/faculty diversity. NDU students develop an understanding of the canon of strategic theory, and are able to apply and creatively adapt this knowledge to current and future security challenges. This foundation of theory and application is informed by cutting-edge research. The educational experience is also enriched by the many distinguished speakers who engage the students in candid discussions. The university's ability to attract these top speakers and build relationships with federal agencies, academic institutions, and international partners is enhanced by its location in Washington, DC. Intentionally integrating students and faculty who come to NDU from all military services and a broad spectrum of interagency, industry, and international partners provides a diversity of thought in every seminar. This ensures that NDU students are exposed to an exceptionally wide range of perspectives, and fosters personal relationships and peer networks, which continue to serve NDU alumni throughout their careers.

About the Information Resources Management College

The NDU Information Resources Management College educates and prepares select military and civilian leaders and advisors to develop and implement cyberspace strategies, and to leverage information and technology to advance national and global security. Although most students are military or DoD civilians, the school also accepts federal agency, private sector, and international students into its graduate programs. The college offers a Master of Science Degree in Government Information Leadership, JPME II credit as a Senior Service College and graduate certificate programs (Chief Information Officer, Chief Financial Officer, IT Program Management, Cyber Security, Cyber Leadership). The National Defense Authorization Act for 2017 officially changes the name of the Information Resources Management College to the College of Information and Cyberspace. As soon as supporting administrative actions are completed, the new name will take effect. For more information about the college, visit our website at http://icollege.ndu.edu.

Table of Contents

This proceedings report was prepared under the direction of Major General F.M. Padilla, NDU President, and Chancellor Jan Hamby, Information Resources Management College, and was edited by Dr. Cassandra C. Lewis, Associate Dean of Academic Programs, Information Resources Management College. The interpretation of speaker remarks expressed in this report are those of the author, and do not represent the official position of the National Defense University, nor the Department of Defense.

This proceedings report was designed by Mr. Michael Jacobs, Instructional Designer, Information Resources Management College.


BEACON
h Engaging Thought

Executive Summary

On July 13-14, 2016, over 100 government leaders, academics, and private sector executives gathered at the National Defense University (NDU) campus at Fort Lesley J. McNair for Cyber Beacon III. Highlights of the event include keynote speeches by Admiral Michael S. Rogers, Commander U.S. Cyber Command, Director National Security Agency, and Chief Central Security Service; and by Letitia Long, Chairman of the Board, Intelligence and National Security Alliance, and Former Director, National Geospatial Intelligence Agency. Cyber Beacon III was coordinated by the Information Resources Management College (IRMC or iCollege) at the National Defense University (NDU).

The two-day conference met its goal of provoking the development of creative ideas on how we collectively deliver national security in cyberspace. Cyber domain thought leaders confronted existing approaches, and each other, using a cross-discipline lens examining critical issues in policy, operations, and technology.

Day One sessions focused on current and emerging challenges and opportunities in cyberspace, from what constitutes cyber war to the basic assumptions about defense in depth. Day Two discussions centered around innovation and technology, and the impact on how we develop our workforce. Four panels, over 20 expert panelists, and afternoon executive working sessions ensured that all participants had the opportunity to contribute and take home valuable action items.

Welcome Remarks

Jan Hamby

RADM (Ret), USN
Chancellor, NDU Information Resources Management College

The conference convened with welcome remarks from Jan Hamby, RADM (Ret), USN, Chancellor of the NDU Information Resources Management College (IRMC). Chancellor Hamby shared that Cyber Beacon III represented a bridge year for the conference. Previous Cyber Beacon gatherings focused on the development of cyberspace issues in DoD educational programs and institutions. Cyber Beacon III expands the aperture of past events to create a venue to explore how we collectively deliver national security in cyberspace, and provide guidance for our way ahead.

RADM (Ret) Jan Hamby

She noted that the intimate, by-invitation, conference was intentionally designed to foster debate and dialogue throughout the two days. Attendees were also encouraged to identify political issues and changes, and share their perspectives with the IRMC about what is needed in strategic leader cyberspace education.

Major General F. M. Padilla

USMC, NDU, 15th President

Major Gen. F.M. Padilla

General Padilla welcomed attendees to the National Defense University and Cyber Beacon III by sharing that Cyber Beacon will be "the place to be" to engage, connect and collaborate on pressing issues, now and for years to come. He congratulated the faculty and staff of the Information Resources Management College (IRMC) and other colleges and components of NDU for planning the event. General Padilla highlighted the inclusion of keynote speakers: Admiral Michael S. Rogers, United States Navy Commander, United States Cyber Command, Director, National Security Agency/Chief, Central Security

Service; and Ms. Letitia Long, Chairman of the Board, Intelligence and National Security Alliance, Former Director, National Geospatial-Intelligence Agency (NGA), and acknowledged the panel members, who represented the brightest minds tackling major issues related to national security in cyberspace.

General Padilla noted that the innovative ideas shared about cyberspace represented cross pollination among academia and the operational world. He stressed that this type of collaboration would result in identifying and putting actionable items forward to enhance cyberspace security. This approach, he remarked, was directly aligned with Secretary of Defense Ash Carter's initiatives to promote innovation, and increase collaboration with the private sector.

In closing, General Padilla, challenged participants who represented government, academia, and the private sector to actively engage in the discussion and executive sessions to produce actionable recommendations for government leaders, DoD cyberspace programs, and the entire cyberspace community of practice.

Mr. Ken Robinson

Director, National Defense University Foundation Board of Directors

In his opening address, Mr. Ken Robinson set the stage for the day by highlighting the importance of identifying indicators and warnings of a cyber attack and developing collaborative solutions. He posited that as a nation, we are more prepared but not safer, noting that attacks can occur at all levels since the perpetrators can be teenagers or nation states. He also pointed out that offensive cyber attacks are not the only cyber risk faced by the nation. An extraordinary natural disaster such as a super solar storm, which last occurred in 1859, or the disruption of the New Madrid fault line, could have devastating consequences for life and property.

Mr. Ken Robinson

Mr. Robinson connected the potential calamity caused by a natural disaster to cyberspace by asserting that it should force us to evaluate continuity of operations plans, and gives rise to critical questions. "How, and in what form, will we communicate? What would happen if large segments of the population are denied access to the internet for extended periods of time?" He urged participants to think as leaders—to operate beyond a particular issue and give attention to the whole problem set. Build action lists to identify and solve what we can;

and anticipate what we cannot. He noted that 50% of cyberspace problems are caused by largely self-inflicted, internal problems based on poor standards of practices and poorly improved capability maturity models. It's the other 50% that we need to identify and anticipate. "We have to solve a very important problem and we need to think about it over the next two days and its event recognition". We need to know who did it, and who paid for it. Answering these questions, he noted, called for different approaches such as: identifying standards and practices; exploring the dark net; harnessing artificial and general intelligence; and challenging the culture of DoD, The Services, and industry. In conclusion, he asked participants to innovate and develop relevant and timely thoughts and recommendations. He dared participants to be different by looking past long-held beliefs.

About the Panel Sessions

Cyber Beacon III convened thought leaders of the cyber domain from government, academia and the private sector to examine critical issues in policy, operations and technology. Panelists were challenged to confront existing approaches, and each other, using a cross-discipline lens.

Day One sessions focused on current and emerging challenges and opportunities in cyberspace, from what constitutes cyber war to the basic assumptions about defense in depth.

Day Two sessions examined innovation and technology, and the impact on how we develop our workforce.

Session I:
The New Face of Conflict

Dr. Alex Crowther
NDU Center for Technology and National Security Policy (CTNSP), Moderator

Dr. Julie Ryan; Mr. Joel Harding; Dr. Alex Crowther; Dr. Martin Libicki; Mr. Thomas Wingfield

Every day brings a new round of attempts to probe our networks and to influence our personnel to inadvertently open pathways for intrusions into our systems. Some say that this constant engagement by adversaries, both nation state and non-state actors, is tantamount to war. Others maintain that it is espionage. What constitutes actual cyber war? And given the implications and possible mutually assured impact, do we really think we will one day find ourselves in the midst of a full-blown war in cyberspace?

Mr. Thomas Wingfield
Professor, NDU Information Resources Management College

Mr. Wingfield began his remarks by asserting that "law applies in cyberspace and the law of armed conflict applies in cyberspace." He then offered three key points to frame discussion on the topic. First, he noted that cyberspace law is not a monolithic body of law that can be reduced to a simple test of whether or not an event or action is legal or not. Rather, cyber law can be categorized into three bodies of law, each providing three different perspectives, including: 1. Law Enforcement (criminal law), 2. Intelligence

Collection, and 3. Military Operations.

His second point examined the question of "how do we know when we are at war legally?" According to Mr. Wingfield, although there is no ambiguity at the occurrence of a 9/11-type event, as it pertains to law there is no such thing as an "act of war"; only a "use of force," which is to be measured along a continuum. Lower-level military actions, such as threats and demonstrations, may be unlawful but do not permit an armed response; Higher-end actions, such as raids or strikes, are categorized as "armed attacks" and may draw a lawful use of military force in response.

Leaders need to understand this range, and especially to know the tests we apply to distinguish a mere use of force from a true armed attack.

Mr. Wingfield's third point explored the application of a two-part special legal test to understand the nature of a cyber conflict. The first part of the assessment is called a Schmitt Analysis test. This test makes qualitative judgment of whether an action is criminal, political, diplomatic, or military. If it is judged to be military action, then a quantitative test is used to identify the scale and effect of the force and damage done in cyberspace.

Dr. Martin Libicki

RAND

Dr. Libicki noted that throughout his career, the question of whether or not a cyber event rises to the level of an "act of war" has been a constant. However, he posited that this is the wrong question to ask since it conflates a "conclusion" with a "decision." He explained that an act of war is a decision not a conclusion because of responsibility and consequences. Countries must be prepared to deal with the real consequences that will arise from their decision to regard a cyber event as an act of war. As such, questions of "what is an act of war?" can be more appropriately reduced to an assessment of whether or not it is in the best interest of a country or organization to decide a cyber action is an act of war.

Dr. Martin Libicki & Mr. Thomas Wingfield

Dr. Libicki offered the example of the 9/11 attacks to illustrate his point. He noted that several factors converged to prompt the United States government to decide 9/11 was an act of war namely: the heinous nature of the attack; what is the best interest of the country; and the political support of NATO allies. According to Dr. Libicki, politics and the ability to persuade others (e.g. other countries or internal stakeholders) of your

point of view of government must be part of the analysis. A cyber attack, of the magnitude of a 9/11 or Hurricane Katrina, would require similar analysis— is it in the country's interest to decide that the attack as act of war? How will the country respond to the act of war? Who (notably which countries) does government need to bring along to support this decision? And, will these entities agree that the magnitude of the chosen response is merited?

Dr. Libicki added to his analysis by noting that in addition to the law, other constraints that countries face in determining what is an act of war include: money, efficacy, manpower, and what precedent will be set by the decision. In conclusion, he contended that all of these constraints must be evaluated as part of a decision that ultimately leads to responsibility. Thus, an act of war is a question of volition and one of responsibility; it is not a conclusion.

Mr. Joel Harding

Cybersecurity Consultant

Mr. Joel Harding shared personal experiences working in the international cyber area to highlight critical differences in how Russia and China approach cyberspace, cyberwar, and military operations compared to the United States and other ally countries. Mr. Harding discussed how cultural norms may have shaped the Chinese response to the Mandiant report (which implicated People's Liberation Army Unit 61398 of espionage). In his discussion on Russia, Mr. Harding covered key differences in Russian conception of Information Warfare and Information Operations and traced the details of the Russian attack in Estonia and the Ukraine. According to Mr. Harding, the Russian attack on the Ukraine was the first true open source example of cyberwarfare.

Mr. Harding also noted that Shanghai Cooperative Organization [Russia, China, Kurdistan, and other Asian countries] reserved the right to shut down the internet in times of state crisis to protect the state, a position that is markedly different from the approach of the United States government.

Dr. Julie Ryan

Professor, George Washington University (Now with the NDU Information Resources Management College)

Dr. Julie Ryan grounded her comments on the new face of warfare by positing that while it is clear we are currently in conflict, determining if a cyber action amounts to a war, a crime or espionage could be a political decision. She noted that in non-cyber conflict, the process of categorizing an action is key to anticipating a structural response. However, for cyber conflict, a structural response is lacking because of many different factors. Some of these factors include: lack of focus on cyber security requirements in all phases of software and systems engineering; a lack of understanding about cyber security and cryptography by those entrusted with custodial care for sensitive information; and on the country level, a void in who is thinking about strategy and

logistics for cyberspace.

Dr. Ryan emphasized that the country faced similar challenges during the rise of air power, and the threat of submarines in World War II. In both instances, the country needed to marshal new techniques and methods, as well as mathematical and technical skills to overcome our adversaries. The same is true of cyber threats. "This is not a computer science problem. This is a systems engineering problem. This is an operations research problem, and until we recognize that and bring all the technical capabilities across the spectrum to bear in solving this problem, the new face of warfare will be scarier than it should be," she said.

Dr. Julie Ryan

Panelists generally agreed that aspects of the Special Operations Forces (SOF) culture could provide useful modeling for the cyber community. Culture is the problem to be solved: SOF has stability, cyber needs stability. However, as Dr. Ryan pointed out, while each unit of Intelligence, Operations, and Law Enforcement is important in its own right, there must be segregation between them in order to avoid conflicts of interests.

The Tallinn Manual and the Law of Armed Conflict

Mr. Wingfield noted that the Tallinn Manual 1.0 provides what is the 90% agreement on cyberspace law by [developed] nation states, with the exception of Russia and China. Tallinn Manual 2.0, due out at the end of this year, addresses the international law governing cyber threats below the threshold of military action. Mr. Wingfield argued against the prevalent view that that law can't keep up with technology. According to him, "regulations have trouble keeping up technology. But, law properly phrased as clear principles that are agreed upon, has no problem adjusting from land warfare to naval warfare, from naval warfare up to air warfare, and now to cyberspace."

Dr. Libicki offered an alternative perspective to the Tallinn model by proposing that the Law of Armed Conflict, which underpins the Tallinn Manual, has less to say about cyber than people thought. His summary of the law of armed conflict is that it applies in two instances: 'things get broken' or 'when people are hurt.' According to him, these two thresholds have been rarely reached in cyber conflict. The exception being Stuxnet and the putatively Russian attack on a German blast furnace, which could be categorized as 'things get broken'. According to him, cyber conflict is primarily about economic loss and the law of armed conflict deals poorly with economic loss.

His second point was that the law of armed conflict does not provide the necessary distinction between various forms of warfare. According to him, distinction should be made between cyber and kinetic warfare to prevent countries from using kinetic warfare as a response to cyber damage.

Mr. Wingfield stated that the law requires no correlation between the type of attack and the type of response; the victim may choose the most effective means of response. However, he pointed that there are constraints on damage and use of force. Victims are only permitted to use a proportionate level of force to prevent or stop an attack, and no more. Additionally, certain types of weapons are prohibited [e.g., chemical, biological, transparent projectiles, small exploding projectiles, and blinding lasers].

Questions or Comments for ADM Rogers

When asked what comments or questions they would pose to ADM Rogers, panel suggestions fell into two general categories: shaping the cyber workforce and shifting organizational culture:

The Cyber Workforce

- Panel members advocated for cyber education for different segments of the population, including: one-days-worth of cyber law for strategic leaders; and a requirement that all high school students complete a comprehensive class on basic cyber hygiene.
- Panelists also offered ideas about recruiting cyber warriors. Mr. Harding noted that disabled veterans possessed skills and expertise, which could be valuable assets in combating cyber adversaries. In particular, he urged DoD to hire veterans to leverage their intelligence-gathering skills.
- What are the career problems with a cyberspace career definition in USG – DOD? Where do you place cyberspace workers? How do you hire them? What do you overlook in recruits [physical, education, etc.]? Do you want a "whole of nation" approach?

Shifting Organizational Culture

- Increase emphasis on accountability. Cyberspace is everybody's business and cybersecurity it is not optional. Everyone from the mailroom to the board room needs to be responsible for cybersecurity.
- Corporations own the internet backbone and thus have power over our lives. How do we address the situation if private companies wage war on United States government?
- Data sharing laws need to be passed by Congress.
- Recognize and leverage the contributions of other agencies on cyberspace. The U.S. Treasury has a great deal of power and played a major role in getting China to reduce its cyberspace operations.
- People "wetware" are the weakest point of the problem. We should not have to rely on unskilled workers or educating teenagers to keep our networks safe. We need to account for the human weakness factor and really focus on building the security into hardware.
- Increase network and sensors to get legally relevant data to come in so we can quickly make decisions. Over the next 3-5 years, we will face something even more difficult. Artificial Intelligence (AI) is more difficult. We need to think through what we need to teach our AI autonomous agents—what can be built in our information systems to enable it to work correctly and reliably at cyber speed.

Session II:
Balance Security and Mission Effectiveness

Chancellor Jan Hamby,
NDU Information Resources Management College
Moderator

RDML Danelle Barrett; Mr. Gregory Touhill; Chancellor Jan Hamby; BG Maria Barrett; CAPT BryerJoyner

Network security brings with it inconveniences and restrictions on the ability to share information across the network and to conduct business and military operations. It also brings a challenge for DoD and the interagency to put the right people on the task – people who have the level of expertise required and the strategic view to understand where mission effectiveness must trump security compliance standards. Should private network security firms with higher technical prowess play a larger role? Should basic assumptions about defense in depth be challenged by new ideas about resilience and recovery? Where does the commander stand in this mix and does he or she understand the tension between security of data and execution of the mission?

Chancellor Jan Hamby opened the Panel II discussion by stating that balancing security and mission effectiveness is a persistent challenge that has faced network operators and commanders alike. Despite its tenacity, this problem requires continued attention and fresh insight. She invited panelists to engage in a discussion about what does and does not work when faced with the common choice to: tighten security and decrease effectiveness, or loosen security and increase effectiveness. In the ensuing discussion, panelists advanced the follow:

Panel members agreed that managing cybersecurity was fundamentally about managing risk.

Captain Susan BryerJoyner

USA, Hopper Information Services Center

CAPT BryerJoyner framed her response by recounting an experience managing what appeared to be a CCMD network hack. During that event, staff had to make critical decisions evaluating the risk and impact on the mission of shutting down or quarantining the network. She noted that mission owners typically make decisions based on their own mission, without understanding the impact on others. However, mission owners need to understand the impact of adding a security issue to the decision.

Mr. Gregory Touhill

Brigadier General (Ret.)

Department of Homeland Security

Mr. Touhill affirmed that cybersecurity is not a technology issue but a risk management problem which should be managed with three guiding principles:

1. Manage risks
2. Manage risk/make the decision about risk at appropriate level
3. Constantly renew, review, and audit risk posture

Accordingly, he advocated for moving risk decisions out of the "Server Room" and into the "Board Room" where it belongs. He noted that one of the key lessons learned from the Office of Personnel Management breach is to take risk management issues seriously. Sharing an example from his own career he recalled how a Commanding Officer had to make an unpopular decision not to open up additional ports on the network so employees could access social media. This decision was made after a risk assessment showed there were credible threats to the mission. The Commanding Officer stood by the decision and sent a message to employees explaining why it was not possible to open ports and why other actions were necessary to harden the network against attacks.

Brigadier General Maria Barrett

USA, U.S. Cyber Command

BG Maria Barrett

BG Maria Barrett, USA, U.S. Cyber Command, cautioned that as networks improve, so will our adversary. To mitigate against this, leaders must continuously reexamine the risk management framework to ensure deterrence. Additionally, she noted leaders need to understand how to defend

against the threats even if risk decisions are made in the "Board Room". This must be a collaborative process to ensure that board room decision makers can understand implications. This collaborative education is especially important for cyberspace because we are familiar with physical world, but not familiar with cyberspace.

Panelists underscored the importance of consistent reassessment of risk using qualitative, quantitative, and hybrid measures. Risk needs to be well defined, consistent and propagated throughout the organization for shared understanding.

Mr. Touhill noted that government must pay more attention on requirements for third party vendors, which the government is heavily reliant on for internet and communications. More private companies must be required to complete audits. Private companies, as provider of the DoD internet/ communication backbone, need to strengthen beyond minimum requirements.

Rear Admiral Danelle Barrett,
USN, U.S. Cyber Command

RDML Danelle Barrett, USN, U.S. Cyber Command, expanded the discussion from risk management to resiliency planning by questioning how long defense organizations from all sectors and services could survive without a working network. After pointing out the obvious reliance on the network in each of her examples shared, she called for more deliberate planning and examination of second and third order effects by operational commanders before there is a crisis.

Other panel members added to these points by calling for more realistic, unplugged and manual exercises which could significantly change calculations of risk.

CAPT BryerJoyner discussed efforts by the United States Navy to include exercise training objectives to ensure its personnel are trained to accomplish the mission despite degraded external connectivity or information systems. She also noted that current examples of network breaches that targeted government systems (e.g. OPM and Joint Staff) have heightened awareness about cybersecurity where past, private sector examples (e.g. Sony) were discounted.

Panelists identified critical challenges facing the Department of Defense and the private sector in balancing security and network security. Some of the highlighted challenges included the current culture of incorrect mindset about the nature of cyber weapons; low accountability for cyber infractions; and low funding and prioritization of cybersecurity and system upkeep. The following section summarizes these concerns, as well as the suggestions and insight for how these challenges can be addressed.

1. RDML Danelle Barrett noted that when people are at home, they are more careful when clicking on links. However, at work, the same people are not so concerned. As a result, she advocated for promoting

ownership of systems and making personnel accountable for their actions.

2. CAPT BryerJoyner identified a major problem in current thought that the communications backbone is secure. Accordingly, she advocated that these communication systems be considered military weapons systems and be made more secure.

3. Mr. Touhill noted that cyber infractions by personnel must be treated with more seriousness and accountability—not just with a "wrist slap". Adding to this idea, he noted that compliance does not bring about best practices, but best practices ensures compliance. According to him, what is needed is a cultural change in the Department; shifting from a checklist mentality to identifying real concerns and changing mindset.

Mr. Gregory Touhill

In addition to poor cybersecurity practices, panel members attributed persistent issues with cybersecurity to systemic underfunding and low prioritization of DoD initiatives (e.g. Joint Information Environment (JIE) and Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)).

BG Maria Barrett recounted a personal experience working with outdated security mechanism to underscore that even basic recommendation and widely understood best practices can take years to be implemented.

CAPT Susan BryerJoyner noted that part of the problem is that commanders are not educated. As such, a critical part of the solution is education. Intelligence reports must be tailored to each commander so he/she understands the risk threats to his/her particular system(s).

RDML Danelle Barrett discussed the critical need to set aside funds (in separate budgets or line items) for cyberspace movement and upgrades. If risk increases, we need to increase the upgrades.

In response to an audience question about creating spaces for experimentation and innovation, panelists acknowledged that these types of programs were needed throughout the federal government. RDML Danelle Barrett offered the example of OSD bug bounty and other open source communities as indicators that innovation was valued in government. However, she cautioned that military culture typically isolates innovation in experimental spaces or "innovation group"

versus integrating innovation within and across the organization.

Mr. Touhill noted that while he is firm believer in innovation, he has observed instances where innovation have shown results and promise for solving an issue, but fell under the funding line. As an alternative, he advocated for building innovative teams modeled on best practices from the private sector.

Other tips to engender innovation in younger staff and throughout the government included:

1. Provide an environment to innovate—provide a safe area to red team before they go out on mission.
2. Do not self-limit—we need to fix resources, address polices, to allow ideas to bubble up. Need to prioritize innovation and workable ideas.
3. Partner with other services (other units—Aberdeen proving ground) that have room to innovate.
4. Teach innovation to the younger generation so they can do innovative work at work
5. Improve the officer corps' and ability of seniors to innovate and implement. Allow people opportunity to fail.
6. Focus on best practices for addressing cybersecurity risk rather than long compliance checklists.

Comments for Secretary of Defense Ash Carter

When asked what comments or questions they would pose to Secretary Carter, panelists noted the following:

1. Clarify the role of Office of the Secretary of Defense (OSD) or Cyber Command (CYBERCOM) in helping private companies respond to a cyberattack. What are the liability, policy and legal implications for assisting the private sector?
2. Foster a team approach for innovation; lots of innovation goes on outside Silicon Valley.
3. Improve the acquisition guide and process—focus in securing attributes --do not buy great systems with a huge hole in the acquisition.
4. When will the Department dedicate resources to solving the security problem?

Keynote

Admiral Michael S. Rogers

U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service

ADM Michael Rogers framed his first day closing keynote address, from his perspective as the Commander of Cyber Command, on the foundational question of "how do we create the future?" He noted that although this focus is relatively new to Cyber Command, it is part of a long-term focus for the department to execute its mission. As the operational commander, his mission is to assure command-and-control and ensure that networks are operating efficiently and effectively without data compromise. In the past, this mission was primarily fulfilled by assessing and securing the network. Current and future challenges require looking beyond network to weapon systems platform and data integrity.

ADM Rogers shared that in considering the future, the following challenges held much of his focus:

1. The increasing number of non-state actors in cyberspace, and the inevitable rise of ISIL-led attacks in cyberspace.
2. Attacks on data integrity. Most penetrations to date have focused on

surveillance, reconnaissance and data extractions, etc. If data is compromised what are the implications for global finance and other key sectors that depend on trust in data? What are the implications for society?

3. Whether the appropriate authorities, policies, laws and rules of engagement about cyberspace are in place to allow leaders to maneuver and execute effectively like the physical world.

4. Prioritizing how to accomplish the mission and identifying mission set – who, what, and how; and executing win – win partnerships.

ADM Rogers noted that Cyberspace is the ultimate team sport—it depends on other team members across government as well as industry, academia, and our allies and partners. Accordingly, he emphasized the need to go beyond DoD to collaborate and collectively act to ensure mission success. In response to a question on whether current restrictions on hiring non-US citizens work against efforts to diversify the cyber workforce, ADM Rogers clarified that this prohibition was not universally applied across the federal government. Federal agencies employ a range of hiring requirements to recruit and retain the workforce. He also reiterated that there are many ways to create partnerships, which includes identifying different talents and expertise across organizations.

In response to a question of who owns the grand strategy for cyberspace in the United States government, ADM Rogers noted that there is already broad strategy in place with multiple parties (e.g. White House and Department of Defense) responsible for different aspects of the plan. The key challenge, to him, is to answer critical questions to operationalize the strategy including: what are the steps needed to make strategy real? Who is responsible for what? What are timelines? Who is accountable?

ADM Rogers noted that the second DoD cyberspace strategy (released in April 2015) intentionally included for the first time (in an unclassified document) reference to deterrence and offensive application of cyberspace capabilities. According to him, like other mission sets and domains, some degree of public dialog of cyber capabilities must be included to deter other nations and groups. As the Director of the National Security Agency, he fully acknowledges the tensions and dangers of revealing too much to adaptive adversaries. However, he believes deterrence can be achieved when specific actions, towards designated adversaries, for specific breaches, is traceable to identified capabilities and the grand strategy.

ADM Rogers responded to several questions related to the cyber mission force by sharing that CYBERCOM is building out, testing, and assessing the results of the teams toward the goal of a fully operational force by September 2018. He noted that out of necessity teams are being deployed before their training is fully complete. This strategy is unusual from other military operations, and is not without a cost to the organization.

He acknowledged that he cannot compete with the private sector on pay or benefits. Thus, his emphasis is on culture, mission and ethos to recruit and retain the team. Junior staff on the Cyber mission force are able to take on significant responsibilities and act on issues in ways unmatched in the private sector. This is especially critical to mitigate disillusionment and attrition that often occurs if workers, especially civilians, are unable to use their training and skills.

When asked "what keeps you awake and what lets you sleep?" ADM Rogers shared that his chief concern was for U.S. critical infrastructure and the inevitable attack. Another area of concern is when non-state actors change their focus from data extraction to data manipulation.

Keynote

Ms. Letitia Long

Chairman of the Board
Intelligence and National Security Alliance (INSA)

In her opening keynote address, Ms. Letitia Long explored conference themes of "Innovation at Risk" and "Workforce of the Future - Man or Machine" by sharing lessons gleaned from her career as an information leader and recognized government innovator. In particular, she focused on events that occurred early in her tenure at NGA to illustrate conditions, which promote and support innovation. She shared that at the onset of her directorship, she found NGA in a very good place. The agency had been well run by her predecessors, and was focused on its combat support mission. She looked forward to keeping the agency on track and saw no mandate for change.

However, after spending the first 90 days visiting with employees and customers, she discovered that both groups shared similar frustrations with navigating NGA to find information and gain access to data. To address this dissatisfaction, she led a vision for agency-wide innovation centered on putting the power of geospatial intelligence in the hands of the customer. Ms. Long noted that undergirding this vision were two simple

goals that everyone could remember and get behind: 1. Provide online on-demand access to information; and 2. Deepen and broaden analytic expertise.

However, as she recalled, the initial message was surprisingly not well received by employees or customers. Employees believed that the initiative was really about reducing the workforce, and they were working themselves out of a job. On the other hand, customers felt that the NGA might inappropriately shift work to them. To regroup from this initial feedback, Ms. Long invited ideas from all segments of the agency on the future vision. This second attempt yielded a widely supported idea for an agency wide contest. Ultimately, the contest was the means for over 500 people, including NGA employees, as well as industry and FVEY intelligence partners working across the globe, in over 25 self-organized teams to contribute innovative ideas to shape the future vision of NGA.

Ms. Long used this experience to lay out key tenents about innovation:

Innovation starts at the top

Ms. Long noted that the central message that she took away from this experience is the importance of leadership and leaders throughout the organization and leadership can't be delegated. Leadership skills and innovation must be promoted throughout the organization at all levels.

Create an environment where all are free to take risks

Promote an understanding that there will be some failures and that's okay. Celebrate failures, as well as successes.

Invest in developing leaders

Ms. Long noted that NGA's Leadership Development program was core to innovation at the agency and a lasting part of her legacy. She stated that NGA increased investment in leader development, even in the midst of declines to agency funding. Seventeen (17) leader attributes were identified for the entire workforce. However, for senior leaders the focus was on five: motivating others; peer relations; timely decision making; integrity and trust; and courage.

These attributes were infused into the organizational culture and used across the spectrum of decision-making including in recruitment, defining position descriptions, selecting war college attendees, promotions and succession planning. The agency also encouraged and invested in lifelong learning.

Ms. Long explored the workforce of the future – "man and machine" by focusing primarily on the fundamental skills needed by future workers. According to her, the soft skills of critical thinking, structured analysis, and communication are just as important as having technical expertise. These basic skills underpin why technology and/or artificial intelligence cannot replace "the human in the loop." She noted that present and future demands require leaders with the ability to think critically and have strong writing and research skills. Additionally, constant changes to the threat environment require a person in the loop to understand and effectively communicate information at all levels.

Ms. Long noted that there are currently 500,000 unfilled cyber-related jobs, with projected increases to over 1 million in 2020. According to her, some of the reasons for this gap include lack of awareness/exposure to cyber careers in US schools and a gender gap in cyber-related fields. She advanced the following strategies to address the shortfall:

1. Encourage early exposure to STEM and cyber opportunities. For girls in middle school, where the drop-off in STEM confidence is greatest, reinforce that it is cool to be a "geek", encourage participation and show role models of other women in STEM fields.

2. Advocate for equipping classrooms K-12 with technology.

3. Invest in personal organizations and networks.

4. Call on Congress to fund comprehensive K-12 Computer Science education.

Session III:

Innovation at Risk

Mr. Christopher Zember

Director Center for Technology and National Security Policy (CTNSP)

Panel Moderator

Mr. Terry Halvorsen; Mr. Mark Thompson; Mr. Christopher Zember; Dr. Camron Gorguinpour; Mr. Jere Simpson

Resource requirements for sustaining the operations and security of our technology-based systems typically exceed the amount provided for in organizational budgets. As a result innovative ideas and efforts are routinely sacrificed in order to 'keep the lights turned on'. Can we balance the need to maintain operations under a constrained budget while providing an opportunity for creative initiatives and adoption of new technologies that could be the key to future success?

Mr. Zember began the panel by raising what he believed to be values of National Defense University (NDU) that were salient to the discussion on innovation and solutions focused on national security problems. In particular, he noted that NDU provides faculty, staff and students the intellectual time, space and freedom to act, think and do differently and speak truthfully. According to Mr. Zember this type of environment is especially critical in times of constrained budgets and resources. Mr. Zember also advocated for a broader definition of innovation that expands beyond technology

to improving operations, business processes, human capital, and organizational culture. According to him, the true challenge is not just coming up with ideas, but innovating at scale—incorporating ideas into operations and scaling them back into the organization.

Mr. Terry Halvorsen

Chief Information Officer, U.S. Department of Defense

Mr. Halvorsen began his remarks by offering a hypothetical scenario to illustrate how innovation in the Department of Defense is often limited by the perceptions of what is and is not permissible. He stated that the true limits of innovation in DoD is not with current laws or rules, but in DoD culture based on current thinking and perception of risk; as well as the inability of the department to leverage its influence. According to Mr. Halvorsen, advancing innovation throughout the department is less about technology, and more about cultural change. In particular, he stressed the need for the department to reconsider how technology is bought, applied and used.

According to Mr. Halvorsen, leaders in operations and acquisition have to begin thinking differently to innovate. He urged operators to ban the word "requirements" and shift to thinking about capabilities. Likewise, he urged leaders in the acquisition field to view regulations as guidelines that can and should be changed as needed.

Mr. Halvorsen's second point promoted an enterprise perspective of DoD as the largest logistics company in the world, the second biggest food distributor, with an information technology and cyber budget topping $38 Billion. According to him, the Department can influence the market without having to be the exclusive source of innovation. Until the 1960s, DoD was probably the leading innovator in technical area. However, although we are no longer leading in innovation because of its sheer size and scope, the Department has the power to be a major influencer of innovation. However, he notes we don't use our buying power as well as we should. That takes cultural change.

Mr. Halvorsen noted that in addition to DoD's influence in innovation, he is pursuing innovation as a collaborative venture with DoD partners. In recent weeks, he will convene a trip to Silicon Valley where he will be accompanied by DoD strategic partners including: NATO, Japan, New Zealand, Australia, United Kingdom, and Canada. Together the group amounts to 60% of the world economy. That sends a strong message to industry. Additionally, he used the recent decision to discontinue of the Common Access Card (CAC) to highlight how innovation can be spurred through work with partners. In addition to the cards not being sustainable or always usable in every environment (war time), the United States is the only FVEY nation using CAC extensively. Instead, when the US agreed to discontinue the CAC, coalition members all agreed to common identity standards and management approaches that will safeguard the network

and allow shared information among members of our coalition.

He also advocated for spending more time with industry. According to Mr. Halvorsen, law is not preventing time with industry. Rather, it is our interpretation and failure to lean forward in dialogue with industry that is preventing collaboration. He pointed to Information Technology Exchange Program (ITEP) as a recent example of successful work with industry. According to him, this year individuals from industry are now imbedded in the DoD and for the first time civilians are now in industry (military have always been immersed in industry). Lastly, he ended with an admonition to leaders on the importance of reading the law and gaining an understanding of what is law and what isn't.

Mr. Mark Thompson

Cyber Technology Executive

Mr. Thompson offered an industry perspective on innovation by noting that we are presently living through some of the most exciting and creative times in the cyber-security industry. According to him, the cyber market is in a very dynamic and "frothy" period of time. The market is at the same time both consolidating--in terms of companies being acquired, and growing--in terms of the amount of money companies and governments are investing in cyber-security technologies. This in turn has led to peculiar challenges for investors, business owners, and governments. For example, on the technical side, the last three years have produced rapid advancements, particularly through innovations in the fields of machine learning and artificial intelligence. While many of these technologies are relatively young on the maturity curve, customers are experiencing much greater levels of protection from them and are as a result, driving very robust demand for these technologies.

But all sectors of the cyber technology sector are not experiencing break-neck growth. In the market for threat intelligence—companies that promise to provide you with deep insight into the cyber attack, the actual number of threat intelligence companies has far outstripped the demand for this type technology. As a result this sector has experienced consolidation and some high profile business exits, in an otherwise overall booming market for cyber security technologies. This is a healthy and natural market development, as customers have aggressively shifted their investments from threat intelligence technologies to security technologies that actually prevent the attack from occurring. This is a big and positive development for consumers, businesses, and governments a like as customers no longer want to simply know how they're being attacked, they want their security technologies to prevent the attack from occurring.

At the same time there is robust business and government demand for cyber-security technologies, investors and venture capital funds are at the point of their investment cycle where their portfolios are engorged with an abundance of cyber tech investments. So

naturally, it has gotten significantly more challenging for a new cyber technology company to attract outside investment. Put another way, a startup company has to have a very special technology idea in order to attract outsider investors. This too is a natural cycle of technology investing and over the next few years we're likely to see cyber-security tech companies rush to premature consolidation—the tech equivalent of a shotgun wedding, go public through an IPO, or be purchased by larger companies acting as consolidator. Evidence of these is already apparent as within the last year, cyber mergers and acquisition (M&A) has reached approximately $30 Billion; an increase of roughly three times from the previous year.

Dr. Camron Gorguinpour

Director of Transformational Innovation for the United States Air Force, Office of the Assistant Secretary (Acquisitions)

Dr. Gorguinpour discussed the concepts of innovation by highlighting the unique responsibility of his office to innovate around the Air Force acquisition system. His ten person team takes on tasks that normal bureaucracies are unable to solve because of constraints related to executing daily business operations. They create the concepts, structure and understanding for others to use. In addition to solve issues related the Federal Acquisitions Regulations (FAR), the Office of AF Transformational Innovation is tasked with finding solutions for over twenty diverse problems throughout the service. Dr. Gorguinpour highlighted a few examples including:

Bending the Cost Curve initiative, which is an approach tackling acquisition reform in collaboration with industry. According to Dr. Gorguinpour, the historical method used throughout the Air Force is to reform in isolation without talking to companies. He noted that the prevalent perception is that government is spending more and getting less compared to 20-30 years ago. However, there is no credible metric to really determine whether or not this is accurate. Dr. Gorguinpour noted, that what we do know is that the Department moves too slow relative to the commercial industry and is likely paying more than it ought if innovative business concepts were being used. Additionally, we tend to look over narrow time bands, e.g. 4-5 years in the future for Program Objective Memorandum (POM) submissions and a few years back when what is needed is longitudinal analysis which takes into account cost trends that span decades.

Cognitive computing uses artificial intelligence to create a computing tool (IBM Watson and another platform) to assist leaders in navigating bureaucracy, laws, rules and regulations related to the FAR process. The Office of AF Transformational Innovation collaborated with two small businesses to develop beta-versions of the tool which is expected to be available at the end of 2016.

Modular Open System Acquisition (MOSA) is a business model for acquisition that is not based on the FAR. MOSA projects leverage other transaction authorities

which allow prototype systems to not be constrained by FAR rules and regulations to construct a business case applicable to a prototype instance. The MOSA projects uses simulations and virtual space to allow vendor to plug in to demonstrate interoperability and test capability. The system is designed to evaluate and make an award within three weeks. The system currently has $5 million in projects, with $4 million additionally planned for the FY 16-17.

Mr. Jere Simpson

Kitewire, Inc.

Mr. Simpson began his remarks by sharing how two experiences that occurred early in his life shape his belief and professional practices on innovation. His first story chronicled how a preeminent defense research and development agency failed to identify innovation and talent in Sean Parker who is widely credited as the driving force for digital music and media. He recounted that he and Sean Parker met at a special government program meant to recruit young talent. Mr. Simpson had circumvented the rules by untruthfully increasing his age from 15 to 18 in order to qualify for the program. While there, he met Sean Parker, another underage student, who was eager to share his cloud-like architecture model to government leadership. After trying unsuccessfully to promote his ideas within Federal government, a disillusioned Sean left the agency to strike out on his own. Sean created Napster music using the same basic model that was overlooked by government; served as the first president of Facebook; and has been involved with many other prominent technology startups. In addition to Sean's story, Mr. Simpson shared how his own ideas were initially overlooked only to be proven as successful and lucrative ventures in the private sector. According to him, these early examples of rejection and missed opportunities have shaped how he approaches innovation and innovative individuals.

Kitewire, Inc., his current business, is designed to organically design systems so that innovators and innovation can rise to the top. Kitewire provides a bank of "innovation" hours to all employees instead of assigning innovation to a particular group. Employees may use the hours however they wish. Innovation hours can be banked for a large project, used by an individual or team, or donated to others. Innovations are presented annually to the president of the company. The rewards for innovation include autonomy, sabbaticals, fast track career, etc.

Mr. Simpson's commitment to innovative talent is reflected in his hiring practices. Kitewire hires autistic adults with highly technical skills and persons with underdeveloped social or professional competencies. According to him, organizations must figure out how to put a system in place to organically identify innovation, since the true source value is not the technology itself, but the people behind the technology. Mr. Simpson gave the example of an innovative but socially-challenged employee to underscore the

importance of tapping into what motivates employees, pairing up individuals with different strengths and modeling similar organizations that exemplify excellence and do things well.

Panel Themes

One of the prominent themes of the panel involved the role of Silicon Valley in supporting or inspiring innovation in the government, especially the Department of Defense. Panelists explained that although there is widespread interest in forging partnerships with Silicon Valley companies, Silicon Valley represents an ideal or concept, rather than the sole source for innovative practices. Silicon Valley and industry in general, provides diversity of thought and allows for engagement in broad conversations with different organizations. Panel members agreed that these conversations helps everyone: organizations and people alike to foster innovation. According to Mr. Thompson the private sector provides government with a model for thinking about innovation since a main focus for private industry is on the customer—identifying customer problems and getting them to buy your solution.

Mr. Halvorsen, answering a related audience question, challenged the notion that competition and contests, innovation incentives often found in industry, could not be leveraged in the Department of Defense. According to him, the Department needs to implement diverse tools and options where it makes sense, based on the need and desired outcomes. He also advocated for government to learn from industry and to understand motivators at the individual and the corporate levels. Other panelists offered examples of innovation found throughout government including: the America COMPETES act and reauthorization, DARPA, and various agency prize competitions.

Session IV:

Workplace of the Future: Man or Machine?

Captain Angie Holcombe Walker

USN, Director Center for Applied Strategic Learning (CASL), NDU

Panel Moderator

Cathryn Downes; Dr. Kathryn Hume; CAPT Angie Walker; Dr. Tod Levitt; Dr. Jeff McNeil; Dr. Eric Daimler

The increasing presence of artificial intelligence and machine assisted technology in the workplace carries with it an impact on how we develop our workforce. If machines are doing the majority of the work, will the role of workers as "the human in the loop" drive a need for greater judgment and critical thinking? And what about the understanding of fundamental concepts? Do we still need to teach basic skills?

Dr. Cathryn Downes

Professor, NDU Information Resources Management College

Dr. Downes opened her remarks with a categorization of Artificial Intelligence (AI) into three strands of technological evolution: Automation, Humanoid Robots and Transhumans. Manufacturing Automation, catalyzed by the coincidence of technology advances in software applications capable of transactional processing and complementing business process improvement practices, is characterized by the replacement of humans

with increasingly automated "intelligent" software/hardware systems. Humanoid robots are machines equipped with humanoid and beyond capabilities (e.g. increased intelligence, strength, and environmental tolerances). Transhumanism describes human beings augmented with machine-like capabilities of memory, sensing, storage, strength. It also captures the transition from humans wearing mobile devices to the physical incorporation of sensors and processing capabilities.

Dr. Downes pointed to the current intertwining, mutually-catalyzing trends in nano, bio-genetic, robotics and information advances that are generating exponential rates and scales of changes in human capabilities, referencing the work of the key researcher and thought-leader, Dr. Ray Kurzweil. Each trend is linked, and has an impact on the other trends; such that advances in one area, can lead to rapid change in one or more of the others. Dr. Downes reflected that these rapid changes have implications for multiple areas, including: policy, the civilian workforce, the development of autonomous weapons, and military workforce. With regard to policy, Dr. Downes noted that the distance and time between science fiction and fact is narrowing quickly. Failure to recognize the effects of technology advances occurring at exponential rather than linear rates of progress can lead to inaccurate predictive assessment of how long it will take for breakthroughs to occur and therefore how long a time period is available for policy formulation and consensus to be achieved. This is particularly the case with contentious ethical policy issues. She advocated for a greater urgency in identifying, working and gaining consensus on national and international policy frameworks, objectives, and approved policies surrounding advancing research agendas, uses, legal frameworks, etc. of AI systems.

Dr. Downes approached the implications for the civilian future workforce by first summarizing a recent study by McKinsey 2015- 2017. This study posited that jobs that have been substantially unaffected by previous industrial technology waves, or were created by those waves, are now vulnerable to replacement by increasingly intelligent automated systems. Based on these trends, Dr. Downes has concluded:

- Universities are currently preparing students for jobs that are increasingly at risk for elimination, and are less vested in preparing students to be able to continuously adapt and learn.
- Greater research is needed in foreshadowing "jobs of the future" to guide both the evolution of higher education institutions and students in assuming responsibility for their own career selection and strategies for employment.

Lastly, Dr. Downes explored the positive and negative implications for AI across the workforce and also in terms of the application of artificial intelligence to the next evolutions of autonomous weapons systems:

Positive:

1. Reduce the requirement for expensive, less predictable, restrictive human workforce;
2. Reduce the requirement to expose human beings to dangerous situations and conditions.
3. Support, enable, human thinking, reasoning, knowledge access and decision-making
4. Improve response times to time-critical situations.

Negative:

1. Some decision-making cycles particularly in military operations can be reduced to seconds, rather than hours or days, reducing the time available for de-escalation options
2. Vulnerability to hacking, hijacking, and forced employment for illegal purposes

Dr. Kathryn Hume

Fast Forward Labs

Dr. Hume began her remarks by noting that she considered the audience to be educators who are responsible for teaching others how to engage with computers in the future. According to her, the dominant rhetoric about AI typically falls into two camps: those that believe that jobs will be replaced by AI in the next ten years, and those who believe that AI is unknown and the jobs and skills needed to address it are also unknown. According to her, both camps offer flawed, unrealistic perspectives on AI and its impact on the workforce. As such, she focused her remarks on near-term civil liability issues that must be overcome.

Dr. Hume explained that most popular accounts of machine learning we read about in the press fall under the subdomain of supervised learning, and unsupervised learning (finding patterns in data) is an active area of research. In supervised learning, humans are a key part of the process to train and supervise the work of the machine. According to her, there are many human factor/judgement implications that must be addressed before AI can be adopted in most fields. She noted that many activities that seem appropriate for machines to administer are constrained by social and regulatory requirements. According to her, even the process for training machines to perform classifications, which machine learning can do very well, can have the potential for gender bias. A reality of using humans to train machines is that machines will be trained based on human biases. These biases will be adopted and perpetuated by the machine. Additionally, current AI systems lack the ability to interpret and make judgement.

Her recommendation is to analyze the "do" (e.g. pattern matching based on previously taught parameters) aspects of a jobs and assign those to AI. Interpretation and analysis should be left to humans. As an example she lifted the potential for collaboration between an AI and human in the legal field. An AI system could be trained over time to help a legal assistant find

a pattern(s) in document discovery that the human would be responsible for interpreting.

In discussing implications of AI in the future, Dr. Hume advocated for significant changes to current educational models. In particular, she noted that students need knowledge of:

1. Liberal arts education, noting that liberal arts education may become more important than STEM as computers increasingly automate technical jobs.
2. Higher math and basic statistics to work with AI.
3. Knowledge of models and how to test them – the scientific method and how to test it.
4. Probabilistic decision making (down to the high school level).
5. Critical thinking—teaching students to read primary sources.

Dr. Tod Levitt

George Mason University

Dr. Levitt noted that the future of Artificial Intelligence was tied to the future of the Department of Defense 3rd offset strategy. In particular, the emphasis on autonomy and human machine teaming are core capabilities for critical application and training. Dr. Levitt raised two primary questions to capture the end goal characteristic of AI systems:

1. Can the AI interact in a natural way that humans understand?
2. Can the system learn during operations?

According to Dr. Levitt, current systems are far from meeting these important benchmarks although advances are being made. Dr. Levitt also discussed the critical need to identify new methods to test, evaluate, and identify trustworthiness. As he explained, the factors of trustworthiness, include the ability of the AI to: explain its actions while performing them; deal with threats that are not pre-programmed (i.e. have/use common sense); and know its performance boundaries (i.e. it knows the limits of its competencies).

Dr. Jeff McNeil

USMCR, NDU, Center for Applied Strategic Learning (CASL)

Dr. Jeff McNeil raised critical questions about AI systems based on his current and previous research. In particular, he noted a previous assessment of AI systems and their potential ability to predict the intentions or actions of adversaries. Similarly, what factors need to go into a predictive model, how can it be automated? And, what are its implications? According to Dr. McNeil, the fear behind autonomy is that we'll create an autonomous system that will "go off" in unexpected ways through emergent behavior. Dr. McNeil concluded that the future of AI in the workforce is primarily an issue of trust, defined by two critical questions:

1. Are we willing to accept an AI system going off script?
2. Could you take orders from a machine?

Dr. Eric Daimler

White House Presidential Innovation Fellows

Dr. Eric Daimler noted that many of the fears and concerns about AI systems are largely myths perpetuated by Hollywood. According to him, AI systems do not spontaneously learn new content or make huge advances in capabilities. However, he agreed with previous panelists that autonomous systems have the potential for perpetuating biases. He noted that while they are legitimate concerns that the AI will impact the workplace, history has shown that technological advances not only eliminate jobs but expand and transform the job market. According to him, since we don't know how jobs will be transformed, the workforce must:

1. Encourage lifelong learning- to teach how to be "newbies" regularly, because the half-life of jobs is 3-5 years.
2. Teach students/workers how to deal with ambiguity and to persevere.

In closing, he offered a new definition of robots as "anything that can sense, plan, and learn from its own experience". According to him, this includes everything from a home thermostat to more advanced forms of AI systems. Given the ubiquity of these systems, Dr. Daimler predicts that instead of a dystopian or a utopian transformation, the future will change slowly, based on the day-today evolution of robots.

Q & A

In the question and answer session, panelists articulated a commitment to the promise of education in shaping the future of AI and the workplace. When asked how to teach and educate beyond the scope of what is owned or known, panelists provided a variety of approaches. However, there was general agreement that most systems cannot be secured and the future cannot be controlled. As such panel members noted that students can be taught to use a different set of standards to evaluate trustworthiness of a system; learn to augment processes of how we sense, plan and react; and learn via repeated real world gaming.

Similarly in answer to the question, "What keeps you up at night?" panelists focused on concerns about education, with direct references to senior leader education; educating the next generation; helping students develop digital literacies; and how to include creativity and open thinking in education. The panel highlighted the utility of alternative futures analysis and wargaming. Referencing the historical example of Project Solarium which took one entire National War College class circa 1953 to review and provide alternatives to the national strategy of containment, Dr. McNeil asked "Where is the Project Solarium for our Cyber Strategy?"

Executive Sessions

Dr. Paul Shapiro
National Defense University, Information Resources Management College
Facilitator

Mr. Hyong Lee
National Defense University, Center for Applied Strategic Learning
Facilitator

The Cyber Beacon III Executive Sessions used opportunities each afternoon of the conference to engage participants in small group, facilitator-led exercises to explore the future of cyberspace and the implications for cyberspace policy and education.

Day I:

Reframing the debate - Identifying the indicators or conditions that would lead to future outcomes

The Day 1 exercise used a scenario analysis framework to guide participants in considering the policy implications of four different alternative futures scenarios. The alternate futures were represented by four quadrants as depicted in Figure 1. Each quadrant is defined by two variables: Handling Effects and Dominants Actors. Handling Effects represented two extreme positions regarding how to handle cyber threats: Deterrence/Defense and Resilience/ Recovery. Likewise, the Dominant Actors category represented the positions of: National Governments and Individuals/ Private Sector.

Participants were assigned to one of four quadrant groups (A, B, C, or D) and tasked with exploring the characteristics and policy implications for their scenario 10 years in the future. For example, participants

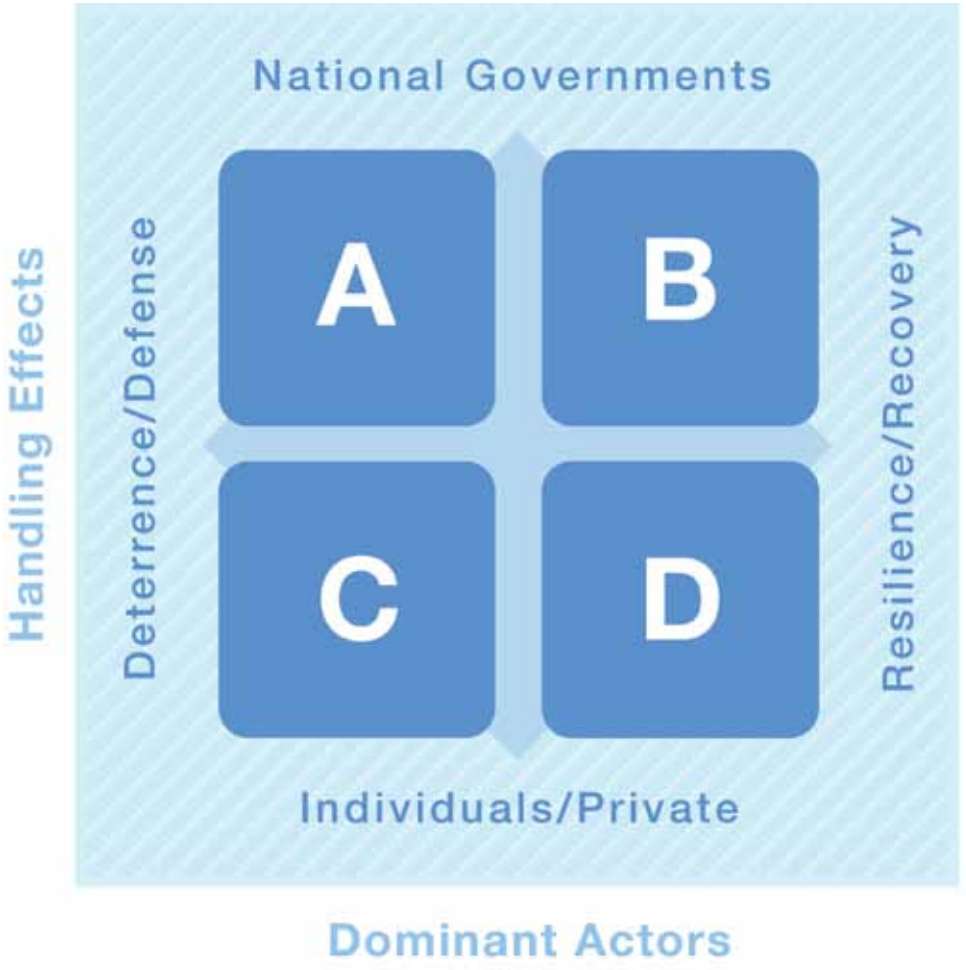

Figure 1: Alternate Futures Scenario Analysis Exercise

assigned to quadrant A examined a future in which the National Governments (dominant actor) operated from a posture of deterrence and defense (handling effects). Groups were asked to consider the dominant characteristics of this future in terms of systemic features or critical technologies, and, how these features may be different from technologies present today. They were also asked to explore the motivations and innovations that drove events to this future, and their impact on individuals, governments, and societies. Lastly, they examined the critical policy and legal issues that exposed gaps from our present system.

Each group presented their findings to the larger audience. The exercise concluded with a collective vote from all participants on the scenario most likely to be reality in the next ten years.

Results of the Day One Executive Session

In answer to the question "Where are we heading?" 40% of participants voted that we are heading to reality most like Quadrant A: Government States and Deterrence/Defense.

Quandrant A
According to participants, the dominant characteristics of life in this future include: deluge of data; "internet of everything"; increased connectedness with the internet as a far-reaching "global blanket"; and increased use of Artificial Intelligence. Governance and regulation in this quadrant are driven by security, and the impact on society and individuals include: individual losing trust in government; rising cyber crime; increase in societal fear; and increased innovation by individuals.

However, 56% percent of participants believe we should be heading a future most like Quadrant D: Individual/Private Sector and Resilience/Recovery.

Quandrant D
Quadrant D is imagined to be characterized by networks run by non-human/Artificial Intelligence (AI); explosion of users on peer-peer networks that are self-policed to avoid government oversight; increase in AI, personal cloaking and enhanced biometrics; emphasis on insurance markets to protect against individual liability; bottom up, open sourced architecture; and cyber communities that transcend geography. Implications of these characteristics on daily societal life include: communities that develop their own solutions to attacks/disruptions; government with less power; and individual empowerment. Negative potential impacts include: nation states using force to resist de-centralization and cyber criminals that are harder to track.

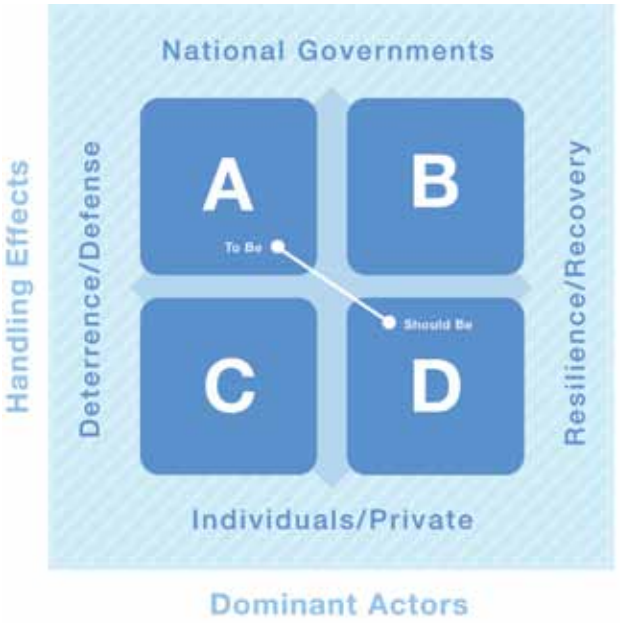

Figure 2: Day I: Collective vote on the most likely future

Day 2:
Formulating For Action – Identifying threats and opportunities, based on an envisioned future (Day 1)

The Day 2 Executive Session engaged participants in an exercise to create an educational offering to positively impact the futures scenario: Quandrant D: Individual/ Private Sector and Resilience/Recovery that was selected in the Day one vote. Participants responded to framing questions to design the educational offering:

1. What is the rationale or justification for this course?
2. Who is the target audience for your course? In other words, who is your typical ideal student?
3. What is the delivery method for this course? (e.g., face-to-face, hybrid, online, MOOC) [What is the course size?]
4. How would you describe this course? (Write a brief course description).
5. What are the expected outcomes?
6. What is the title of your course?

Day 2 Results

Participants worked in seven different small groups to design their educational offering. Each group presented its design to the larger gathering. Five groups identified the target audience as leaders in government, industry, the community or a combination of multiple sectors. Two groups designed the course to broadly impact the general population: from early learners in grade school to leaders in government and industry.

Most groups indicated that diverse and tailored delivery methods should be used to educate target audience, including case studies, simulations-based, hybrid, online, and face to face courses. Three of the four groups targeting leaders proposed a hybrid course that leveraged both online and face to face capabilities. One group that designed a course for government leaders and critical infrastructure providers advocated for exclusively face to face delivery.

The learning outcomes for the two general population courses centered on developing creative and responsible, digital/cyber users, with emphasis on the ability of students to understand their roles and responsibilities in the digital age. However, each of these courses also introduced different instructional content. One course underscored the need to teach students how to think and gain competence in technology and business. The second course noted the importance of developing shared cyber values including: ethics, integrity, courtesy, and safety/security.

Groups focused on developing leaders advocated for offerings that would educate and empower leaders to change culture; instill accountability; and address deficiencies of current systems. These groups targeted learning outcomes that would enable students to leverage practical and strategic knowledge to understand the nature of threats, define objectives and strategically respond.

Implications

Exploration of the future of cyberspace often gives rise to more unanswered questions and critical challenges in need of collective action and solutions. Cyber Beacon III broke from this mold by advancing specific implications for policy and practice. Over the course of the conference, the perspectives of panelists, speakers, and executive session participants converged to advocate for a future of cyberspace hallmarked by:

Awareness and accountability across the organization on cyber threats and critical cyber issues. Informed leaders with personal knowledge of cyber issues and mature understanding of cyber strategy and logistics. Organizational cultures that support holding employees, from leaders to lower level staff, accountable for actions which put the organization at risk.

Risk management frameworks that are prioritized, integrated and well defined across the enterprise.

Cross-pollination and collaboration at every level of government, and between all sectors (e.g. government agencies, services, and the private sector).

Deliberate investment in targeted cyber education that balances technical proficiency with critical thinking and problem solving for all segments of society.

Support for innovation in people, ideas, and technology.

Implications for Graduate Cyber Education

The below student learning outcomes are drawn primarily from the Day Two executive session, and represent participant recommendations of critical elements that must be included in the cyber education for senior leaders.

1. Understand the current availability of tools and limitations of technology.
2. Evaluate approaches to mitigate or circumvent deficiencies, including consideration of doctrine, legal and policy constraints and potential changes to advance.
3. Understand strategic focus and how to develop and integrate grand strategies.
4. Demonstrate critical thinking in proposing unique solutions to evolving cyber-related challenges.
5. Understand cyber threats and vulnerabilities.
6. Understand risk assessment methodology.
7. Create a cyber resiliency plan.
8. Develop plans to build coalitions and shared understanding in adaptive organizational networks.

Possible Topics for Future Cyber Beacon Conferences Include:

- Cyber "Project Solarium"
- Cyber Resiliency: Exploring Resilient Systems and Life without Cyber Capabilities
- Law Enforcement in Cyberspace
- Risk Management in the Cyber Context
- National Cybersecurity Policy
- Cyber Norms and Ethics
- Cyber Sovereignty

End of Cyber Beacon III Conference Summary

Speaker Bios

Rear Admiral Danelle Barrett

USCYBERCOM

Rear Admiral Danelle Barrett is the Deputy Director of Current Operations at U.S. Cyber Command. She graduated from Boston University in 1989 with a BA in History where she received her commission from the Naval Reserve Officer Training Corps in a ceremony aboard the USS Constitution. Her operational assignments include tours at U.S. Naval Forces Central Command/Fifth Fleet; Commander, Second Fleet, Carrier Strike Group Two, Multi-National Forces Iraq, Carrier Strike Group Twelve which included deployments in support of Operations Enduring Freedom in Afghanistan and Unified Response in Haiti; and Standing Joint Force Headquarters United States Pacific Command.

Shore assignments included tours at Naval Computer and Telecommunications Stations in Jacksonville, Cecil Field and Puerto Rico; Senior Navy Fellow at the Armed Forces Communications and Electronics Association; Allied Commander Atlantic Systems Support Center Norfolk, Naval Personnel Command, Chief of Naval Operations Task Force Web, Commanding Officer, Naval Computer and Telecommunications Area Master Station Atlantic; and Chief of Staff, Navy Information Dominance Forces Command.

She holds Masters of Arts degrees in Management, National Security/Strategic Studies, Human Resources Development, and a Master's of Science in Information Management. She has published 25 articles. Her personal awards include: Legion of Merit and other military decorations, Copernicus Awards 1998, 2000, and 2005; Naval Institute C4 writing award; DoD Chief Information Officer Award First Place Individual Category 2006; Federal 100 Winner 2010; AFCEA Women in Leadership Award 2014.

Brigadier General Maria B. Barrett

United States Army Cyber Command (ARCYBER)

BG Maria B. Barrett serves as the Deputy Commanding General for the Joint Force Headquarters – Cyber (JFHQ-C), United States Army Cyber Command (ARCYBER). Under the leadership of a three-star commander, JFHQ-C plans, coordinates, integrates, synchronizes, directs and conducts cyberspace operations to ensure freedom of action in cyberspace, and to deny the same to our adversaries in support of Combatant Commands.

BG Barrett, a Massachusetts native, graduated from Tufts University with a Bachelor of Arts Degree in International Relations and was commissioned through the Army ROTC program as a Second Lieutenant in 1988.

BG Barrett's past assignments are: Deputy Commander (Operations) for the Cyber National Mission Force, United States Cyber Command; Executive Officer to the Chief Information Officer/G-6, United States Army, Office of the Secretary of the Army, Washington, DC; Chief Information Officer/Director, J-6, United States Southern Command, Doral, FL; Commander, 160th Signal Brigade, Third United States Army, OPERATIONS NEW DAWN/ ENDURING FREEDOM, Kuwait; Commander, 307th Integrated Theater Signal Battalion, Schofield Barracks, HI; Director, J-3, White House Communications Agency, Washington, DC; Operations Officer, 41st Signal Battalion, 1st Signal Brigade, 311th Signal Command (Theater), Camp Coiner, Korea; Chief, Strategic Operations, 1st Signal Brigade, 311th Signal Command (Theater), Yongsan, Korea; Secretary to the General Staff, and Aide-de-Camp to the Commanding General, United States Army Signal Center and Fort Gordon, Georgia; Commander, D Company, 16th Signal Battalion, 3d Signal Brigade, III Corps, Fort Hood, Texas; Radio Officer and Frequency Manager, III Corps G6, Fort Hood, Texas; Operations Officer, 51st Signal Battalion, 22nd Signal Brigade, V Corps, United States Army Europe and Seventh Army, Germany; and Executive Officer and Platoon Leader, C Company, 26th Signal Battalion, 93d Signal Brigade, VII Corps, United States Army Europe and Seventh Army, Germany and OPERATIONS DESERT SHIELD/DESERT STORM, Saudi Arabia.

BG Barrett's awards and decorations include the Defense Superior Service Medal, Legion of Merit, Bronze Star Medal, Defense Meritorious Service Medal with one oak leaf cluster, Meritorious Service Medal with three oak leaf clusters, Army Commendation Medal with one oak leaf cluster, Joint Service Achievement Medal, Army Achievement Medal, the Joint Meritorious Unit Award, the Parachutist Badge and the Signal Regiment's Bronze Order of Mercury.

BG Barrett is a graduate of the United States Army Command and General Staff College, the Information Systems Staff Officer Course, the Signal Officer Advanced Course, the Brigade and Below Signal Officer Course, and the Signal Officer Basic Course. She holds a Master of Science Degree in National Resource Strategy from the Industrial College of the Armed Forces, and a Master of Arts Degree in Telecommunications Management from Webster University.

She is married to LTC (Ret) B Brian T. Barrett, a former Signal Corps Officer and fellow Massachusetts native.

Captain Susan BryerJoyner

Hopper Information Services Center

Captain BryerJoyner assumed command of the Hopper Information Services Center in January 2016.

CAPT BryerJoyner was commissioned in 1991 through the Naval Reserve training Corps (ROTC) at Rensselaer Polytechnic Institute, where she earned a Bachelor of Science in Materials Engineering.

Her diverse tours of duty include deployments in the Mediterranean and Arabian Seas, the Western and South Pacific Ocean, and Iraq in support of Operation *Enduring Freedom*, Operation *Iraqi Freedom*, and Operation *Tomodachi.*

CAPT BryerJoyner's shore assignments include the Naval Computer and Telecommunications Area Master Station, and the Naval Computer and Telecommunications Station, Far East. She served as Flag Aide to the Director, Space and Information Warfare, Command and Control Directorate on the staff of the Chief of Naval Operations (CNO), and Flag Aide to the first Commander, Naval Network Warfare Command. Her joint tours include the U.S. Pacific Command, the Joint Warfare Analysis Center. Multi-national Force-Iraq, and U.S.Cyber Command.

CAPT BryerJoyner's fleet assignments include Carrier Strike Group B embarked on USS *George Washington* (CVN 73), the USS *Blue Ridge* (LCC 19), Commander, U.S. 7th Fleet in Yokosuka Japan.

She hold a Master of Science degree in Computer Science from the Naval Postgraduate School and a Master of Science degree in Government Information Leadership from the National Defense University.

CAPT BryerJoyner's awards and decorations include the Defense Superior Service Medal, Legion of Merit, Bronze Star, two Defense Meritorious Service Medals, and three Navy Meritorious Service Medals. In 2001 and 2005, she received the Copernicus Award, and is a proud Plank Owner of the Information Professional Community and the Naval Network Warfare Command.

Dr. Alex Crowther

NDU, Center for Technology and National Security Policy

Areas of Expertise: Middle East; Western Hemisphere; Cyber Security & Information Technology; Humanitarian Assistance & Disaster Relief; Insurgency/Irregular Warfare; Stabilization and Reconstruction

Glenn Alexander Crowther grew up in Ethiopia, Brazil, Bolivia and Indonesia where his father worked as a civil engineer. He has extensive government service, including a decade each in the Cold War, the post-Cold War era and the post 9/11 era. He has worked as a Western Hemisphere specialist, a strategist and a political advisor. He served overseas eight times: three times in Latin America, twice in Korea, twice in Iraq and once in Belgium. He has a variety of awards from the Departments of Defense and State as well as the Canadian government. His work at the strategic level includes tours at the Army Staff, the Joint Staff J5 (Strategic Plans & Policies), and as a Research Professor at Strategic Studies Institute (the US Army's think tank). He was personally selected to be a Counterterrorism Advisor for the US Ambassador to Iraq, a Political Advisor for the MNC-I Commander and a Special Assistant for the Supreme Allied Commander, Europe.

He is currently a Cyber Policy specialist in the Expert Consultant program at the Center for Technology and National Security Policy (CTNSP) at the National Defense University in Washington, DC. He is also an adjunct Senior Political Scientist at the RAND Corporation and an adjunct Research Professor of National Security Studies at the Strategic Studies Institute. Alex has a BA in International Relations from Tufts University, an MS in International Relations from Troy State University, and a Ph.D. in International Development from Tulane University. He was also an International Security Studies Fellow at the Fletcher School of Law & Diplomacy. He has professional fluency in Spanish and specializes in strategy; Western Hemisphere issues; cyber policy issues; international development; insurgency/counterinsurgency; Joint, Interagency, Intergovernmental and Multinational (JIIM) issues and the Comprehensive Approach.

Dr. Eric Daimler

Office of Science and Technology Policy

Dr. Daimler is currently a White House Presidential Innovation Fellow at the Office of Science and Technology Policy. Eric Daimler is creating the robotics revolution. Mr. Daimler has 20+ years' experience building companies. Principal in two Investment Firms (HgAnalytics, CDO Ventures) championing early-stage investments in household firms such as Hotmail (NASDAQ: MSFT) and TiVo (NASDAQ: TIVO) while producing superior returns to investors. Agent in two financial firms (Morgan Stanley, Merrill Lynch) in quantitative, and emerging markets, finance. Experience as an Executive, Investor, and Advisor to many

information-technology companies, including six as founder.

Studying Computer Science early, starting at the University of Washington, continuing to Carnegie Mellon University, and later Stanford University. Academic career culminated in time spent at Carnegie Mellon as Assistant Professor of Software Engineering Practice and finally Assistant Dean.

Dr. Cathryn Downes

NDU, Information Resources Management College

Dr. Downes served thirteen years as a member of the New Zealand Defence Force, completing service as SES-1 as the Military Policy Development Adviser to the Chief of the Defence Force. In her academic career, she served twelve years as a research academic scholar, with appointments at Harvard University's Center for International Affairs, the University of Melbourne Australia, and the Strategic and Defense Studies Center, Australian National University.

Dr. Downes has published and presented widely during her academic career. Her research and recent publications have focused inter-agency collaboration at the strategic level, clarifying the concepts and space of strategic thinking and decision-making, unintentional militarism and civil-military relations in complex, national security wicked problems, innovations in E-Learning 2.0 for graduate-level education.

Dr. Camron Gorguinpour

USAF, Office of the Assistant Secretary (Acquisition)

Dr. Goguinpour serves as the Director of Transformational Innovation for the United States Air Force, Office of the Assistant Secretary (Acquisitions).

In this role, Camron solicits, advocates for, and executes innovative concepts with the potential for broad-ranging and rapid improvements to Air Force acquisition processes and systems. Camron also serves as Executive Director for the Department of Defense Plug-In Electric Vehicle (PEV) Program. He is responsible for designing and executing a large-scale, multi-year effort to integrate PEV's into the Defense Department's non-tactical vehicle fleet.

Prior to arriving at the Pentagon, Camron served as Executive Director for Scientists & Engineers for America a 501c-3 nonprofit, non-partisan organization dedicated to engaging scientists and engineers in public policy and political activities. Camron also served for

six years as Co-Founder and Executive Director for Space Science Outreach and Research (SSOAR) a 501c-3 nonprofit organization dedicated to promoting science and education. Through SSOAR, Camron executed numerous programs, including the creation of two public charter schools in collaboration with NASA, the University of California at Berkeley, and the Cesar E. Chavez Foundation.

Camron served for four years as a lecturer and part-time faculty member in the Bioengineering Department of the University of California, Berkeley. In this role, he created and taught courses in the field of Bioastronautics (i.e. human physiology in space). Camron received his doctorate from the University of California, Berkeley/University of California, San Francisco Joint Graduate Program in Bioengineering. His area of emphasis was Bioastronautics, with a focus on the health impacts of space-borne radiation. Camron also holds a bachelor's degree in Astrophysics and Physics from the University of California, Berkeley.

Mr. Joel Harding

Cyber and Information Warfare Consultant

Joel is a consultant for cyber warfare, information operations, and information warfare, working closely with government, corporate and academic seniors. Joel spent over 35 years working national security issues. Joel was enlisted US Army Special Forces (18D and 18E), graduated from the University of Pittsburgh, commissioned as an infantry officer and later became a military intelligence officer. As a Military Intelligence officer, he worked for years in Information Operations before retiring. Since then he has worked in the Department of Defense, in the corporate world and then as an IO subject matter expert at the Association of Old Crows. While at the AOC, he was the Director of the IO Institute, the editor of the IO Journal, and the organizer of InfowarCon. He has lectured, taught and worked in Russia, China, Canada and the UK on information warfare and cyberwar. Mr. Harding works with NATO and the EU regarding Russian Information Warfare. Joel is working closely with the Ukraine Rada on a Ukraine National Information Strategy for the Minister of Information Policy.

He also writes and publishes a blog: To Inform Is To Influence.

Mr. Terry Halvorsen

Department of Defense

Terry Halvorsen assumed the duties as the Department of Defense Chief Information Officer effective March 8, 2015. He previously served as the Acting Department of Defense Chief Information Officer. Prior to that, he was the Department of the Navy Chief Information Officer.

As DoD CIO, Mr. Halvorsen is the principal advisor to the Secretary of Defense for Information Management / Information Technology and Information Assurance as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications. He provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions.

Before serving as the Department of the Navy CIO, Mr. Halvorsen was the deputy commander, Navy Cyber Forces. He began serving in that position in January 2010 as part of the Navy Cyber reorganization. Previous to that, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for over 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 globally dispersed computer network users. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management.

Mr. Halvorsen served as an Army intelligence officer in a variety of assignments, including Operations Just Cause and Desert Storm. He holds a bachelor's degree in history from Widener University, and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.

Rear Admiral (Ret.) Janice Hamby

NDU, Information Resources Management College

Janice Hamby, RADM, USN (Ret.) began serving as the Chancellor of the Information Resources Management College in October 2014. She previously served on the staff of the Secretary of Defense (OSD) as the Deputy Chief Information Officer for Command, Control,

Communications and Computers (C4) and Information Infrastructure Capabilities (DCIO for C4IIC).

A native of Medina, Ohio, Hamby was commissioned from the University of North Carolina at Chapel Hill Navy Reserve Officers Training Corps program in 1980. Early assignments included duty at Naval Regional Data Automation Center, Washington; commander, Naval Base Pearl Harbor; and plans and project management department head at the Data Processing Service Center, Pearl Harbor. She attended Boston University earning a Master of Science in Information Systems Management and a Master of Business Administration, graduating from both programs with highest honors. She was subsequently assigned as assistant professor of Computer Sciences at the U.S. Military Academy and then served as deputy director of the Communications Operations Directorate at Naval Computer and Telecommunication Station Washington. In 1994, she reported to USS Dwight D. Eisenhower (CVN 69) as part of the initial assignment of women to naval combatants. She participated in Eisenhower's deployment to Haiti in support of Operation Uphold Democracy, completing her surface warfare qualification during Eisenhower's 1994 Mediterranean deployment. In August 1995, she transferred to USS George Washington (CVN 73) to serve as the first afloat combat systems officer to combine information systems management, combat systems maintenance and telecommunications systems management in one department.

Dr. Kathryn Hume

Fast Forward Labs

Kathryn Hume leads sales and operations for Fast Forward Labs, an artificial intelligence research and advising company. She helps large enterprises apply data and machine learning technologies to modify business processes and build new revenue streams. Kathryn is also a visiting professor at the University of Calgary, where she teaches innovative courses on law and technology featuring guest speakers from law firms and technology companies.

Before joining Fast Forward Labs, Kathryn advised international law firms on data privacy and security (ISO 27001 and NIST 800-53) and managed Intapp's Risk Roundtable, a seminar program focused on cybersecurity and risk management.

Kathryn is a recognized writer and speaker on the practical applications of machine learning. Holding a PhD in comparative literature from Stanford, she speaks eight languages and brings a humanistic, interdisciplinary perspective to technology and data science.

Dr. Tod S. Levitt

George Mason University

Dr. Levitt is an acknowledged leader in development of advanced capabilities for evidential reasoning in large-scale, high dimensional model analysis including operations applications in multisensor fusion, SAR, IR, and EO image understanding, ground robot vision, air to ground surveillance systems and C4ISR systems supporting multiple military intelligence, planning and command and control applications.

He has led the development of a diverse family of advanced information software systems built to handle real world data under complex operating conditions. These systems include a fully automated middle-Eastern armor unit detector for the U.S. Army that was evaluated to perform at expert imagery analyst levels on wide-area, low resolution Desert Storm SAR, and a system for automated diagnostic measurement from digital x-rays of the hand that was employed in clinical care at the San Francisco Veterans Administration Medical Center.

From 1978-1991, Dr. Levitt worked for the Honeywell Signal and Image Processing Division, in the Image Understanding Division at Advanced Information Systems and as a Senior Research Associate in the Stanford University Robotic Laboratory before founding IET, Inc. in 1991. Dr. Levitt led IET for sixteen years, producing numerous R&D breakthroughs and generating the Quiddity*Suite commercial software package for building complex, probabilistic reasoning applications.

In October 2007 Dr. Levitt joined the George Mason University C4I & Cyber Center as a Research Professor where he has performed counter-insurgency and counter- improvised explosive device (C-IED) research, developed forward-looking, net-centric, evolutionary persistent ISR algorithms for plug-and-play surveillance assets, and made innovative contributions to the emergent field of multi-modeling with applications to nuclear deterrence.

Dr. Levitt is a co-founder and 18 year member of the Board of Directors of the Association for Uncertainty in Artificial Intelligence. His Ph.D. in mathematics is from the University of Minnesota.

Dr. Martin Libicki

RAND Corporation

Martin Libicki (Ph.D., U.C. Berkeley 1978) has been a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and

national security. In addition he is a Distinguished Visiting Professor at the U.S. Naval Academy and has been an adjunct at Columbia University and Georgetown University. He wrote two commercially published books, Conquest in Cyberspace: National Security and Information Warfare, and Information Technology Standards: Quest for the Common Byte and has a cyberwar textbook (Cyberspace in War and Peace) at the publisher's (U.S. Naval Institute Press). He is also the author of numerous RAND monographs, notably Defender's Dilemma, Brandishing Cyberattack Capabilities, Crisis and Escalation in Cyberspace, Global Demographic Change and its Implications for Military Power, Cyberdeterrence and Cyberwar, How Insurgencies End (with Ben Connable), and How Terrorist Groups End (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

Ms. Letitia Long

Intelligence and National Security Alliance (INSA)

Letitia A Long served as the fifth Director of the National Geospatial-Intelligence Agency (NGA), and was the first woman to lead a major US intelligence agency. This appointment culminated a career that spanned all aspects of organizational leadership, business functions, and global operations. She led the NGA during a critical period of transition and has deep experience in strategic planning, policy development, leading change in complex organizations, executive development and succession planning with an emphasis on diversity operations, budget planning and execution, and innovation and risk management.

Starting her career in Naval Intelligence, Ms Long went on to serve as the Deputy Director of Naval Intelligence, and then the first Deputy Undersecretary of Defense for Intelligence (Policy, Requirements and Resources), the first Chief Information Officer at the Defense Intelligence Agency as well as the Deputy Director of the Defense Intelligence Agency.

Ms. Long is the recipient of numerous awards to include the Presidential Rank Award of Distinguished Executive, two Presidential Rank Awards of Meritorious Executive, two DoD Medals for Distinguished Service and three National Intelligence Distinguished Service Medals. She has been decorated with the Medal of Merit by the King of Norway, appointed to the rank of Chevalier in the National Order of the Legion of Honor of France and awarded the Commander's Cross of the Order of Merit of the Republic of Poland.

Ms Long currently sits on the boards of Raytheon Company, Urthecast Corporation and

Noblis, Inc. She is the Chairman of the Board of the Intelligence And National Security Alliance and on the boards of the Virginia Tech School of Public and International Affairs and the United States Geospatial Intelligence Foundation. She is also an Executive in Residence with Brookings Executive Education.

Ms Long earned a Bachelor of Science in Electrical Engineering from Virginia Tech, a Master of Science in Mechanical Engineering from the Catholic University of America and was awarded an honorary Doctorate of Strategic Intelligence by the National Intelligence University.

Dr. Jeff McNeil

NDU, Center for Applied Strategic Learning

Col Jeff McNeil, USMCR, Ph.D., recently joined the NDU CASL faculty in June, 2016. An artillery and intelligence officer, Col McNeil's recent assignments have included Cyberspace Plans Officer for USPACOM, USSTRATCOM and USCYBERCOM; USJFCOM Deputy Director for International Engagement, and Intelligence Plans and Operations Officer for Marine Forces Central and Pacific Commands. In his civilian position as a full Professor for Clemson University, he is presently dedicated to full-time research supporting OUSD(AT&L) to develop and manage the nations cyber ranges. Prior to assuming his current position, Dr. McNeil spent 15 years in industry as a Principal Investigator conducting analysis and evaluation across a broad range of defense programs, operations and weapons systems. He also taught a variety of international relations and US foreign policy courses for the University of Nebraska.

Major General Frederick M. Padilla

National Defense University

Major General Padilla was born in April 1959 in Torrejon, Spain, to a career Air Force officer. He is a 1982 graduate of East Carolina University and was commissioned in 1983.

Major General Padilla's assignments in the operating forces include Platoon Commander, Company Commander and Battalion Adjutant, 3d Battalion, 6th Marine Regiment; Rifle and Weapons Company Commander, 3d Battalion, 9th Marine Regiment; Inspector-Instructor, Weapons Company, 2d Battalion, 23rd Marine Regiment; G-3 Operations Officer, 1st Marine Division; Commanding officer, 1st Battalion, 5th Marines and Commanding General, 3d Marine Division.

Other assignments include Command Adjutant, Marine Aircraft Group-42, Detachment A, 4th Marine Aircraft Wing; Commanding Officer, Marine Detachment, USS CANOPUS (AS-34); Commanding Officer, School of Infantry-West; and Chief of Staff, Marine Corps Combat Development Command. His joint assignments include Plans Officer, J3/5 and Secretary of the Joint Staff, Joint Task Force Six; and Branch Chief for the Joint Requirements Oversight Council (J8) on the Joint Staff in the Pentagon. Major General Padilla's first General Officer assignment was as the Commanding General Marine Corps Recruit Depot, Eastern Recruiting Region, Parris Island, South Carolina.

Major General Padilla was promoted to his present rank in July 2013 and before coming to NDU as 15th President was the Director of Operations with Plans, Policies and Operations, Headquarters Marine Corps.

Major General Padilla is a graduate of the Marine Corps Amphibious Warfare School, Air Command and Staff College, Armed Forces Staff College and Naval War College. He has a B.A. in Geography and an M.A. in National Security and Strategic Studies.

His personal decorations include the Legion of Merit (with Combat V and two gold stars), Defense Meritorious Service Medal (with oak leaf), the Meritorious Service Medal, the Joint Service Commendation Medal, the Navy and Marine Corps.

Mr. Ken Robinson

NDU Foundation

An internationally recognized expert in intelligence, terrorism, and national security – with 30 years of experience in Special Forces, Special Mission Units, and the US Intelligence Community. Having helped design the nations National Exercise Program, detailed experience in crisis and consequence management, including reconstituting a government after a national emergency. Heavily invested in cyber, all-source intelligence, science and technology, and green technologies – with a focus on sustainability, survivability, and cutting edge innovation. Has unique capabilities to provide secure, independent 3G/4GLTE broadband solutions, and management consulting experience solving complex issues for governments and NGOs in the most dangerous places on earth. Ken provided distance learning training tools, and Serious Gaming, which supports the Joint Improvised Explosive Device Defeat Organization (JIEDDO). This support included battlefield visualization, as well as creating, writing, and executive producing virtual and reality-based interactive software solutions for the Military Intelligence Community. Ken was nominated to serve on the President's Intelligence Advisory Board (PIAB), which exercises oversight responsibilities of the United States Intelligence

Community. He provides objective advice to solve some of the most complex international problems. His approach is to remain technology and vendor agnostic – providing objective solutions for the world's challenges. Ken does not "predict," rather he "anticipates," the possibilities of the markets and sets his goals and objectives accordingly. His professional services have a single standard of excellence, which is offered equally to clients, vendors, stakeholders, and investors alike – accomplishing the mission, on time and on budget.

Admiral Michael S. Rogers

Commander, U.S. Cyber Command and Director,
National Security Agency/Chief, Central Security Service

Adm. Rogers is a native of Chicago and attended Auburn University, graduating in 1981 and receiving his commission via the Naval Reserve Officers Training Corps. Originally a surface warfare officer (SWO), he was selected for re-designation to cryptology (now Information Warfare) in 1986.

He assumed his present duties as Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service in April 2014.

Since becoming a flag officer in 2007, Rogers has also served as the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, and most recently as Commander, U.S. Fleet Cyber Command/U.S. TENTH Fleet.

Duties afloat have included service at the unit level as a SWO aboard USS Caron (DD 970); at the strike group level as the senior cryptologist on the staff of Commander, Carrier Group Two/John F. Kennedy Carrier Strike Group; and, at the numbered fleet level on the staff of Commander, U.S. 6th Fleet embarked in USS Lasalle (AGF 3) as the fleet information operations (IO) officer and fleet cryptologist. He has also led cryptologic direct support missions aboard U.S. submarines and surface units in the Arabian Gulf and Mediterranean.

Ashore, Rogers commanded Naval Security Group Activity Winter Harbor, Maine (1998-2000); and has served at Naval Security Group Department, NAVCOMSTA Rota, Spain, Naval Military Personnel Command, Commander in Chief, U.S. Atlantic Fleet, the Bureau of Personnel as the cryptologic junior officer detailer, and Commander, Naval Security Group Command as aide and executive assistant (EA) to the commander.

Rogers' joint service both afloat and ashore has been extensive and, prior to becoming a flag

officer, he served at U.S. Atlantic Command, CJTF 120 Operation Support Democracy (Haiti), Joint Force Maritime Component Commander, Europe, and the Joint Staff. His Joint Staff duties (2003-2007) included leadership of the J3 Computer Network Attack/Defense and IO Operations shops, EA to the J3, EA to two Directors of the Joint Staff, special assistant to the Chairman of the Joint Chiefs of Staff, director of the Chairman's Action Group, and a leader of the JCS Joint Strategic Working Group.

Rogers is a distinguished graduate of the National War College and a graduate of highest distinction from the Naval War College. He is also a Massachusetts Institute of Technology Seminar XXI fellow, Harvard Senior Executive in National Security alum, and holds a Master of Science in National Security Strategy.

Brigadier General (Ret.) Gregory Touhill

Office of Cybersecurity and Communications (CS&C), DHS

Brigadier General (retired) Gregory J. Touhill is the Deputy Assistant Secretary for Cybersecurity and Communications (CS&C) within the National Protections and Programs Directorate (NPPD) of the Department of Homeland Security (DHS), where he focuses on the development and implementation of operational programs designed to protect our government networks and critical infrastructure systems.

General Touhill retired from the United States Air Force in July 2013 after a distinguished career culminating as the Chief Information Officer and Director of Command, Control, Communications, and Cyber Systems at U.S. Transportation Command—one of the nation's 10 combatant commands. As the Senior Cyberspace Operations officer, he led the command's cyberspace defense mission and oversaw a $500 million information technology portfolio.

General Touhill is a highly experienced combat leader who commanded at the wing, group, and squadron level. Prior to his assignment at United States Transportation Command, he was the United States Defense Attaché to Kuwait, where he coordinated a new long-term bilateral defense agreement that enabled U.S. forces to withdraw from Iraq through Kuwait. As commander of the 81st Training Wing, he established the Air Force's Cyberspace Operations training programs and led the $1 billion rebuilding of Keesler AFB, Miss. after Hurricane Katrina. The Air Force's only three-time winner of the Communications-Computer System Professional Achievement Award, General Touhill was the recipient of the 2006 Air Force Science and Engineering Achievement Award for his work leading the team that created the life-saving Radio-Over-Internet Protocol Network (RIPRNET) supporting convoy operations in Iraq, for which he was also awarded the Bronze Star medal.

General Touhill is a distinguished graduate of the Squadron Officer School, Air Command and Staff College, and the Advanced Communications Officer Training school, where he received the Webb Award as the top graduate. He also is a graduate of the Air War College, the Armed Forces Staff College, the Harvard University John F. Kennedy School of Government Senior Executive Fellows program, and the University of North Carolina's Logistics and Technology Program for Executives.

General Touhill was previously an adjunct instructor and staff member of Washington University in the St. Louis College of Engineering and Applied Science graduate program in Cybersecurity and Information Systems Management. He is the co-author of Commercialization of Innovative Technologies, Bringing Good Ideas to the Marketplace and Cybersecurity for Executives, A Practical Guide (John A. Wiley & Sons). He maintains the Certified Information Systems Security Professional (CISSP), Certified Acquisition Professional in Information Technology and Program Management, and the American College of Corporate Directors Master Professional Director certifications.

Captain Angie Holcombe Walker

NDU, Center for Applied Strategic Learning

Captain Angie Walker is a native of Cumming, GA. She graduated from the University of Florida with a Bachelor of Science in Mathematics and received her commission through the Naval Reserve Officer Training Corps Scholarship Program. She holds a Master of Science in Meteorology and Physical Oceanography from the Naval Postgraduate School and is completing her dissertation as a Doctoral Candidate in the University of Southern Mississippi's Human Capital Development Executive Program.

At sea, she served as the First Division Officer and Boilers Officer in USS Shenandoah (AD-44) qualifying as a Surface Warfare Officer and Engineering Officer of the Watch (Steam). While in USS Stump (DD-978), she served as the Navigation/ Administration Department Head and Strike Warfare Officer during a Middle East Force deployment. Re-designated as a Special Duty Officer (Oceanography), she reported to the Mobile Environmental Team (MET) in Jacksonville, FL as the Assistant Department Head and Fleet Liaison Officer supporting multiple ships' independent operations and exercises as an embarked MET. She assumed dual responsibility as Staff Oceanographer for Commanders, Carrier Strike Group Six and Fourteen. She served as the Joint METOC Officer in support of Combined Joint Task Force – Horn of Africa at Camp Lemonier, Djibouti where she also earned her Flight Meteorologist qualification.

Ashore, she served as the Operations Officer and then the Regional Operations/Plans Officer at the Naval Atlantic Meteorology and Oceanography Facility Jacksonville, FL. It is in this capacity which she coordinated all hurricane issues for Commander, Navy Region Southeast, which included all naval installations from North Carolina south to Puerto Rico and west to Mississippi. In January 2005, she reported as a Plank Owner to Naval Meteorology and Oceanography Professional Development Detachment South in Gulfport, MS and served as Officer-in-Charge until she assumed Executive Officer of Naval Meteorology and Oceanography Professional Development Center, Gulfport, MS. She served as Plans Division Head of the Strategic Plans and Policy Department and later Deputy Assistant Chief of Staff for Operations for Commander, Naval Meteorology and Oceanography Command, Stennis Space Center, MS. She commanded the Center for Naval Aviation Technical Training Unit Keesler in Biloxi, MS, where her command won several Regional and CNO Flagship awards each year.

She most recently served on the Operational Navy Staff as the Navy's Arctic Affairs Officer in support of Task Force Climate Change (OPNAV N2N6E) and as the Section Head for Battlespace Awareness in Assessment Division of the Information Dominance Branch (OPNAV N81). She is currently the Director of the Center for Applied Strategic Learning (CASL) at the National Defense University.

Captain Walker's personal awards include the Meritorious Service Medal (3), the Joint Service Commendation Medal, the Navy and Marine Corps Commendation Medal (4), the Navy and Marine Corps Achievement Medal (3), and various other individual, campaign, and unit awards.

Mr. Thomas Wingfield

NDU, Information Resources Management College

Thomas C. Wingfield is Professor of Cyber Law at the Information Resources Management College of the National Defense University in Washington, DC. He holds a B.A. in History and Russian Language (summa cum laude) from Georgia State University, and a Doctor of Laws (J.D.) and a Master of Laws (LL.M., with distinction, International and Comparative Law) from the Georgetown University Law Center.

Beginning his career as a naval officer, he served as Squadron Intelligence Officer with an F/A-18 strike fighter squadron aboard USS Midway, based in Yokosuka, Japan. Following deployments in the Western Pacific, the Indian Ocean, and the Northern Arabian Sea, he was

assigned to back-to-back tours in Washington, DC: first as a Desk Officer at Headquarters, Office of Naval Intelligence, and then as Intelligence Liaison Officer at the Center for Naval Analyses, the Navy's principal think tank. While in Washington, he served as a White House Social Aide and completed his law degrees at Georgetown.

Upon passing the Georgia bar exam, Mr. Wingfield transitioned to the naval reserve and took a position with a defense consulting firm to advise military and intelligence community clients in the areas of treaty compliance, use of force in cyberspace, and space law. In 2003, he became a Research Fellow of the Potomac Institute for Policy Studies, providing analysis to Congress and the Administration on the legal and policy aspects of emergent national security issues.

Appointed an Associate Professor at the US Army Command and General Staff College at Fort Belvoir, Virginia, Mr. Wingfield served in the Department of Joint, Interagency, and Multinational Operations. Professor Wingfield then deployed to Afghanistan in 2009-10 as Rule of Law Advisor for COMISAF's Counterinsurgency Advisory and Assistance Team.

He served as Professor of International Law at the George C. Marshall European Center for Strategy Studies, where he directed the Program on Applied Security Studies, and, most recently, was Professor of Law and Strategy at the newly-established United Arab Emirates National Defense College in Abu Dhabi, UAE. He was appointed to his current position at the US National Defense University in December of 2015.

A former Chair of the American Bar Association's Committee on International Criminal Law, he is a member of the State Bar of Georgia, the District of Columbia Bar, and, since 2006, the Bar of the United States Supreme Court. He lectures widely and writes extensively on cyber conflict, rule of law, and lawful uses of force. He is the author of THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE and one of the drafters of the TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Cambridge, 2013). His wife Kim is a Professor of Renaissance Art History, but neither their son John Percival (age 8) nor daughter Katharine Isla (age 4) has yet chosen a professional track. Mr. Wingfield may be reached at thomas.wingfield@ndu.edu.

Mr. Christopher Zember

NDU, Center for Technology and National Security

Mr. Christopher Zember is currently serving as co-director of the Center for Technology and National Security Policy (CTNSP), at the National Defense University. CTNSP is a DOD

research center focused on the intersection of technology and national security policy. As both a government organization and a university, CTNSP is uniquely positioned to help DOD expand outreach and access to academia and global technology markets,

Prior to this assignment, Mr. Zember served as the Director of the Department of Defense Information Analysis Centers (IACs), under oversight of the Assistant Secretary of Defense for Research and Engineering. In this position, he was responsible for operational management and policy guidance for 10 IACs, which annually conducted nearly $2 billion in technical research and analysis. With more than 7,000 scientists and engineers in 49 states, IACs provide strategic studies and build communities of interest in areas of critical importance to the DOD, including cyber operations, weapon systems, and homeland defense.

In Spring 2014, Mr. Zember launched the Technology Domain Awareness (TDA) initiative, which focuses on effectively understanding the technology landscape as it relates to current and future defense needs, in order to expand DoD's access to global technology innovation. The DoD TDA efforts seek to expand awareness and application of commercial and non-government investments to enable better, cheaper, and faster Defense capability development.

Prior to this, Mr. Zember led the Strategy and Operations practice for a consulting firm. His teams supported various offices in the Department of Homeland Security, the Intelligence Community, Defense Research and Engineering, and across the Joint Staff. Mr. Zember also served as a member of the core research team in a congressionally chartered effort to rewrite the National Security Act, enhancing collaboration and information sharing at the interagency and multinational levels.

Mr. Zember has served in several liaison positions, including leading a liaison office for the National Security Agency. In this capacity, he played a key role in overcoming organizational barriers across the Intelligence Community, including fostering cooperation with foreign allies. His efforts made significant progress in enhancing information sharing, moving from the mentality of "need to know" to a culture embracing the "need to share."

Mr. Zember holds a Master of Public Administration from American University, and is DAWIA Level III certified in program management.

Registered Participants

Mr. James Adams
Joint Service Agency
Participant

Mr. Anthony Allard
U.S. Army War College
Participant

Mrs. Anne Bader
Bader Resources LLC
Participant

Mr. Sean Baggott
JSOU
Participant

Ms. Yegana Baghirova
World Bank / George Mason University
Participant

Rear Admiral Danelle Barrett
U.S. Cyber Command
Speaker

Brigadier General Maria Barrett
Cyber National Mission Forces
Speaker

Dr. Chuck Barry
INSS, NDU
Participant

Brigadier General James Begley
National Guard Bureau (NGB)
Participant

Dr. W. Stan Boddie
NDU, Information Resources Management College
Group Facilitator

Maj Geoff Bowman
NDU, Center for Applied Strategic Learning
Group Facilitator

Mr. Calvin Brown
NDU
Participant

Captain Susan BryerJoyner
HOPPER Information Services Center
Participant

Dr. William Butler
Critical Infrastructures and Cyber Protection Center
Participant

CW4 Joe Cardenas
USASOC HQ
Participant

CPT Joseph Casey
781st Military Intelligence BN
Participant

Dr. John Christian
NDU, Information Resources Management College
Participant

Mr. John Cidila
Army Cyber Command and Second Army
Participant

Ms. Patricia Coopersmith
NDU, Information Resources Management College
Staff

Lt Col Lauren Courchaine
USEUCOM Joint Cyber Center
Participant

Dr. Alex Crowther
NDU, Center for Technology and National Security Policy
Panel Moderator

Dr. Eric Daimler
White House Presidential Innovation Fellows
Speaker

Mr. Ross Dakin
White House Presidential Innovation Fellows
Participant

Dr. Cathy Downes
NDU, Information Resources Management College
Speaker

COL Patrick Duggan
Strategic Landpower Task Force
Participant

Mr. Mark Duke
NDU, Information Resources Management College
Participant

Dr. Roxanne Everetts
NDU, Information Resources Management College
Group Facilitator

Ms. Adrienne Ferguson
NDU, Information Resources Management College
Group Facilitator

Ms. Lisa Fowlkes
Public Safety & Homeland Security Bureau/ FCC
Participant

Dr. Camron Gorguinpour, PhD
United States Air Force, Office of the Assistant Secretary (Acquisitions)
Speaker

Mr. Brian Hajost
SteelCloud LLC
Participant

Mr. Terry Halvorsen
DOD/CIO
Speaker

Chancellor Jan Hamby, RADM (Ret), USN
NDU, Information Resources Management College
Panel Moderator & Speaker

Mr. Joel Harding
Independent Consultant
Speaker

Brig Gen Patrick Higby
SAF/CIO A6
Participant

Ms. Theresa Hitchens
Center for International and Security Studies at Maryland
Participant

Maj Hans Hogan
ARCYBER & 2A
Participant

Dr. Carl Horn
NDU, Information Resources Management College
Participant

Dr. Kathryn Hume
Fast Forward Labs
Speaker

Dr. John Hurley
NDU, Information Resources Management College
Group Facilitator

Ms. Beth Ibish
NDU, Center for Applied Strategic Learning (CASL)
Participant

Dr. Marwan Jamal
NDU, Information Resources Management College
Participant

Mr. Ken Kligge
Center for Applied Strategic Learning (CASL)
Participant

Mr. Marc Kolenko
Information Innovators Inc.
Participant

RADM Kevin Kovacich
USCYBERCOM
Participant

Mr. Alex Kreilein
SecureSet
Participant

Mr. Hyong Lee
NDU, Center for Applied Strategic Learning (CASL)
Participant

RADM (ret) William Leigher
Raytheon
Participant

Mr. Erren Lester
General Services Administration
Participant

Dr. Tod Levitt
George Mason University
Speaker

Dr. Cassandra Lewis
NDU, Information Resources Management College
Organizer

Dr. Martin Libicki
RAND
Speaker

Ms. Letitia Long
Intelligence and National Security Alliance (INSA)
Keynote Speaker

Ms. Mekisha Marshall
National Maritime Intelligence-Integration Office (NMIO)
Participant

Dr. Russ Mattern
NDU, Information Resources Management College
Group Facilitator

Dr. Fernando Maymi
Army Cyber Institute
Participant

Dr. Mary McCully
NDU, Information Resources Management College
Participant

COL Jeff McNeil
NDU
Participant

Ms. Allene (Lainey) Mikrut
NGA/NWC
Participant

Dr. Robert Mills
Air Force Institute of Technology
Participant

Mr. John O'Brien
NDU, Information Resources Management College
Participant

Mr. Robert James Orr
NDU, National War College
Participant

MajGen Frederick Padilla
NDU
Speaker

LTC (Retired) USA Lance Paoli
Red Hat
Participant

LCDR Jonathan Parker
NMIO
Participant

BrigGen US Army (retired) Jack Pellicci
National Defense University Foundation
Participant

Ms. Donna Powers
NDU, Information Resources Management College
Staff

Mr. Russ Quirici
NDU, Information Resources Management College
Participant

COL Kenneth Rector
U.S. Army Cyber School
Participant

Mr. Bruce Rideout
NAVAIR
Participant

Mr. Ken Robinson
NDU Foundation
Speaker

Admiral Michael Rogers
United States Cyber Command,
National Security Agency/Chief,
Central Security Service
Keynote Speaker

Dr. Sheila Ronis
NDU Foundation
Participant

Professor Dennis Ruth
NDU, Information Resources Management College
Participant

Dr. Julie Ryan
George Washington University
Speaker

Dr. Ron Sanders
Booz Allen Hamilton
Participant

Dr. Geoffery Seaver
NDU, Information Resources Management College
Group Facilitator

CW5/CCWO Heriberto Serrano
USASOC
Participant

Dr. Paul Shapiro
NDU, Information Resources Management College
Organizer

Lt Gen, USMC (Ret.) Robert "Bob" Shea
AFCEA International
Participant

Rear Admiral (Ret.) David Simpson
FCC
Participant

Mr. Jere Simpson
KITEWIRE Inc
Speaker

Mr. Phillip Simpson
Booz Allen Hamilton
Participant

Mr. Mitchell Sipus
White House Presidential Innovation Fellows
Participant

Lt Col James D. Skelton, USAF
NDU, Information Resources Management College
Group Facilitator

Mr. Robert Spring
NDU Foundation
Participant

Amb. Walter Stadtler
NDU Foundation
Participant

Mr. Moon Sulfab
United States Senate
Participant

Mr. Shawn Sullivan
Avantgarde Partners
Participant

COL Max Thibodeaux
Joint Forces Staff College
Participant

Mr. Mark Thompson
Thompson+Billings, LLC
Participant

Captain Paul Tortora
US Naval Academy
Participant

Mr. Gregory Touhill
DHS, DAS
Speaker

Ms. Clara Tsao
White House Presidential Innovation Fellows
Participant

CAPT Angie Holcombe Walker, USN
NDU, Center for Applied Strategic Learning (CASL)
Panel Moderator

CPL Trey Warner
USASOC
Participant

LTC (R) Vern Wendt
NDU, Information Resources Management College
Group Facilitator

Mr. Thomas Wingfield, J.D.
NDU, Information Resources Management College
Speaker

Mr. Robert Zakon
White House Presidential Innovation Fellows
Participant

Mr. Christopher Zember
NDU, Center for Technology and National Security Policy
Panel Moderator

Cyber Beacon III was generously supported by the NDU Foundation

NATIONAL DEFENSE UNIVERSITY
FOUNDATION

The NDU Foundation is a non-profit organization committed to enhancing human security and global stability by investing in the education and leadership development of national security professionals studying at the National Defense University (NDU). Established in 1982 as a nonpartisan philanthropic organization, the Foundation's mission is to raise awareness and support for NDU. The Foundation brings together dedicated individuals, corporations, and NGO's to ensure that the NDU community has the richness of resources necessary to cultivate excellence in the next generation of global security leaders.

CYBER BEACON IV

Save the Date

September 27 - 28, 2017

National Defense University

Cyber Beacon III
Exploring Cyberspace Through Engaging Thought
National Defense University
Fort McNair, Washington DC
cyberbeacon@ndu.edu

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu